TAMPEREEN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma
Tietoliikennetekniikan suuntautumisvaihtoehto

Tuomas Penttilä

WLAN-LANGATTOMAT LÄHIVERKOT

Insinöörityö, joka on jätetty opinnäytteenä tarkastettavaksi insinöörin tutkintoa varten Tampereella 06.02.2007

Työn ohjaaja Ari Rantala

TAMPEREEN AMMATTIKORKEAKOULU INSINÖÖRITYÖN TIIVISTELMÄ

Tekijä:	Tuomas Penttilä
Työn nimi:	WLAN-langattomat lähiverkot
Päivämäärä:	30.01.2007
Sivumäärä:	37 sivua ja 2 liitesivua
Hakusanat:	WLAN, WEP, WPA, 802.11
Koulutusohjelma:	Tietotekniikka
Suuntautumisvaihtoehto:	Tietoliikennetekniikka
Työn valvoja:	Lehtori Ari Rantala

Langattomuus on yleistynyt viime vuosien aikana erittäin paljon, ja nykyään ihmiset käyttävät langattomia yhteyksiä päivittäin. Tutkintotyössä tutustuttiin langattomiin lähiverkkoihin ja niiden tietoturvaan. Langattomissa lähiverkoissa tietoliikenne tapahtuu ilmassa radioteitse. Nykyään langattomia lähiverkkoja käytetään lähes kaikkialla, kodeista ja yrityksistä, sairaaloihin ja julkisiin tiloihin.

Tässä työssä on pyritty antamaan lukijalle käsitys langattomien lähiverkkojen toiminnasta. Työssä on esitelty langattomille lähiverkoille tyypillisimmät standardit ja perehdytty tarkasti verkkojen vaatimaan tekniikkaan. Lisäksi työssä on kerrottu langattomien lähiverkkojen tietoturvallisuudesta. Tietoturva-puutteisiin on pyritty antamaan ratkaisuja ja parannusehdotuksia. Työn lopussa on esitelty elektroniikka-alan yrityksessä oleva langaton lähiverkko.

Tulevaisuudessa langattomat lähiverkot tulevat yleistymään erittäin paljon ja langattomuus valloittaa maailmaa. Uusia standardeja tulee markkinoille, ja tietoturvallisuuteen tulee kiinnittää erityistä huomiota verkkojen lisääntyessä.

TAMPERE POLYTECHNIC **ABSTRACT OF ENGINEERING THESIS**

Author:	Tuomas Penttilä
Name of the thesis:	WLAN-wireless local area network
Date:	30.01.2007
Number of pages:	37 pages and 2 appendixes
Keywords:	WLAN, WEP, WPA, 802.11
Degree programme:	Computer Systems Engineering
Specialisation:	Telecommunication Engineering
Thesis Supervisor:	Lecturer Ari Rantala

Wireless Local Area Network (WLAN) is the linking of two or more computers without using wires. Presently, WLAN is a very popular technique, and it is getting even more popular in the future. Many standards are typical to WLAN. All the most common standards are introduced in this thesis. WLAN uses spread-spectrum technology based on radio waves. WLAN can cover areas ranging in size from a small office to a whole city. Also all the newest security standards are introduced in this thesis.

ALKUSANAT

Tämä tutkintotyö käsittelee langattomia lähiverkkoja. Aiheen valinta oli vaikea. Aiheeseen päädyin kuitenkin lopulta sen nykyaikaisuuden takia ja ajattelin siitä olevan hyötyä itselleni tulevaisuudessa. Tutkintotyön tekeminen oli lopulta suurempi urakka kuin olin koskaan kuvitellut. Olen kirjoittanut tutkintotyötä oman ansiotyön ohessa Helsingin Etelä-Haagassa sijaitsevassa yksiössäni keväästä 2006 tammikuuhun 2007. Työ on tehty suurimmaksi osaksi itsenäisesti. Yhdessä kappaleessa on esitelty työpaikassani Eaton Power Quality Oy:ssä oleva langaton lähiverkko, josta kiitokset Markku Riiheläiselle. Kiitokset annan myös työn valvojalleni Ari Rantalalle. Suurin kiitos kuuluu vanhemmilleni, jotka ovat jaksaneet tukea minua läpi opiskeluaikojeni sekä taloudellisesti että henkisesti hyvinä ja vaikeina aikoina.

Helsingissä 30.01.2007

Tuomas Penttilä

SISÄLLYSLUETTELO

LYHENNELUETTELO

AES	Advanced Encryption Standard, vahva lohkosalausmenetelmä
BSS	Basic Service Set, peruspalveluverkko, WLAN-verkko liitetty langalliseen lähiverkkoon yhdellä tukiasemalla
CCK	Complementary Code Keying, signaalin hajautusmenetelmä
CCMP	Counter Mode Encryption, salausprotokolla
DoS	Denial of Service, palvelunestohyökkäys
DSSS	Direct Sequence Spread Spectrum, suorasekvenssitekniikka
EAP	Extensible Authentication Protocol, käyttäjien tunnistusprotokolla
ESS	Extended Service Set, laajennettu palveluverkko, WLAN-verkko liitetty langalliseen lähiverkkoon useammalla tukiasemalla
ETSI	European Telecommunications Standards Institute, Eurooppalainen telestandardointijärjestö
FHSS	Frequency Hopping Spread Spectrum, taajuushyppelytekniikka
IBSS	Infrastructure Basic Service Set, infrastruktuuriverkko
IEEE	Institute of Electrial and Electronics Engineers, standardointijärjestö
ISO	International Standardization Organisation, kansainvälinen standardointi-organisaatio
LLC	Logical Link Control, siirtokerroksen protokolla
MAC	Medium Access Control, siirtokerroksen alikerros, kaistanvaraus
OFDM	Orthogonal Frequency Division Multiplexing, monitaajuusmodulointitekniikka
OSI	Open Systems Interconnection, tietoliikenteen referenssimalli
PBCC	Packet Binary Convolution Coding, modulointimenetelmä
PLCP	Physical Layer Convergence Protocol, fyysisen tason konvergenssikerros
PMD	Physical Media Dependent, mediasta riippuva fyysinen kerros
PPDU	Physical Protocol Data Unit, fyysisen tason tietosähke

SSID	Service Set Identification, langattomalle verkolle annettu käyttäjäkohtainen nimi
TKIP	Temporal Key Integrity Protocol, parannuksia WEP:n tietoturvaan
VPN	Virtual Private Network, virtuaaliverkko, joka kehitetty parantamaan tietoturvaa
WEP	Wired Equivalent Protocol, langatonta tietoliikennettä suojaamaan kehitetty salausmenetelmä
WPA	Wireless Fidelity Protected Access, langattoman tietoliikenteen salausmenetelmä

1 JOHDANTO

Langattomuus on nykyään erittäin yleistä ja nykyään ihmiset käyttävät langattomia yhteyksiä päivittäin. Esimerkiksi lähes jokaisella suomalaisella on käytössään kännykkä, joka toimii langattomasti. Muita jokapäiväisessä elämässä esiintyviä langattomia laitteita ovat mm. kannettavat tietokoneet, pöytäkoneet, viivakoodin lukijat, uusien autojen keskuslukitukset ja langaton GPS-satelliitti-paikannus (*Global Positioning System*), jonka avulla nykyään mm. taksit suunnistavat. Langattomuus on yleistynyt viime vuosien aikana erittäin paljon kehittyneen tekniikan ja kasvavien tarpeiden johdosta. Nykyään puhelimissa, pelikonsoleissa, digikameroissa ja monissa muissa laitteissa on valmiiksi asennettu langaton verkkovalmius. WLAN (*Wireless Local Area Network*) eli langaton lähiverkko on kehitetty palvelemaan näitä tarpeita. WLAN-tekniikan avulla käyttäjä pystyy esimerkiksi ottamaan yhteyden Internetiin radioteitse, jolloin käyttäjä ei tarvitse kaapeleita. WLAN-tekniikassa onkin omat hyötynsä ja haittansa. Hyödyistä mainittakoon juuri tämä kaapelittomuus, joka avaa useita eri mahdollisuuksia verkon rakentamiseen ja käyttämiseen. Esimerkiksi monissa yrityksissä on langaton lähiverkko, jolloin työntekijät voivat liikkua vapaasti ja pääsevät silti kannettavan päätelaitteensa avulla yrityksen verkkoon. Mainittakoon yhtenä esimerkkinä sairaala, jossa lääkäri voi hakea potilastiedot verkon kautta potilaan luona. Langaton lähiverkko voidaan myös rakentaa paikkaan, jossa kaapelointi olisi mahdotonta, kuten esimerkiksi vanhoihin rakennuksiin. WLAN-tekniikkaa käytetään myös tilapäisissä ratkaisuissa, kuten messuilla ja urheilukilpailuissa. Langattomat lähiverkot ovat lisäksi kokonaiskustannuksiltaan usein halvempia ratkaisuja kuin perinteiset lähiverkot. Kuitenkin myös haittapuolia löytyy, niistä mainittakoon esimerkiksi radiotiestä ja WLAN-standardien puutteista johtuva tietoturva.

Tässä tutkintotyössä perehdytään WLAN-tekniikkaan ja pyritään antamaan syventävä käsitys siitä miten langaton lähiverkko itse asiassa toimii. Lisäksi perehdytään WLAN-tekniikan eri standardeihin, arkkitehtuureihin ja tieto-turvallisuuteen. Tutkintotyön lopussa esitellään myös elektroniikka-alan yrityksessä oleva langaton lähiverkko.

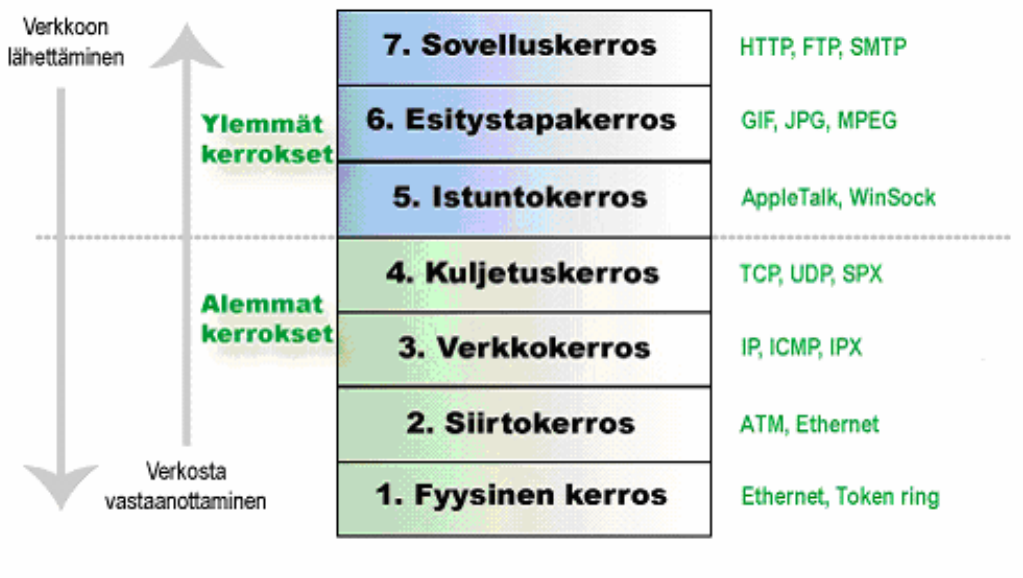
2 WLAN–STANDARDIT

WLAN-tekniikalle ovat tyypillisiä erilaiset standardit. Standardeja on kertynyt useita, langattomien lähiverkkojen lyhyestä historiasta huolimatta. Tällä hetkellä vallitsevin standardi on IEEE:n (*Institute of Electronic and Electrical Engineers*) kehittämä 802.11-standardi, tästäkin standardista on kehitetty monta eri versiota. IEEE on yhdysvaltalainen sähkö-, tietokone- ja tietoliikenne-insinöörien yhdistys, joka on kehittänyt monia alaansa liittyviä standardeja /31/. IEEE:ssä toimii standardointikomitea LMSG (*LAN/MAN Standardization Group*), joka on erikoistunut lähi- ja alueverkkojen standardointiin eli 802-standardiin. Myös ETSI:llä (*European Telecommunications Standard Insitute*) on omat HiperLAN- (*High-Performance Radio Local Area Network*) ja HiperLAN/2-standardinsa. Nämä HiperLAN-standardit eivät kuitenkaan ole menestyneet läheskään yhtä hyvin kuin IEEE:n kehittämät 802.11-standardit. Usein langattomien lähiverkkojen yhteydessä näkee myös Wi-Fi-sertifikaatin (*Wireless Fidelity*). Wi-Fi:stä puhutaan, kun WLAN on tarkoitettu yleisön Internet-yhteyksiä varten. Nykyään erilaisissa julkisissa paikoissa, esimerkiksi ravintoloissa, voikin törmätä tähän Wi-Fi-logoon, se tarkoittaa, että halutessaan asiakkaalla on mahdollisuus käyttää Internetiä omalla päätteellään joko maksua vastaan tai ilmaiseksi.

WLAN-standardit toimivat 2,4 GHz:n ja 5 GHz:n taajuusalueilla. Uusimmat standardit voivat nykyään saavuttaa teoriassa jopa 125 Mbit/s:n bittinopeuden. Tutkintotyössä vertaillaan myös IEEE 802.11 -standardia IEEE 802.16 -standardiin, jota kutsutaan nimellä WiMAX (*Worldwide Interoperability for Microwave Access*). WiMAX on tarkoitettu laajemmalle alueelle kuin WLAN.

2.1 IEEE 802.11 -standardit

Nykyään suurin osa langattomista lähiverkoista noudattaa IEEE:n 802.11-standardia. 802.11-standardit kattavat OSI-mallin (*Open Systems Interconnection*) kaksi alinta kerrosta eli fyysisen kerroksen ja siirtokerroksen (kuva 1).

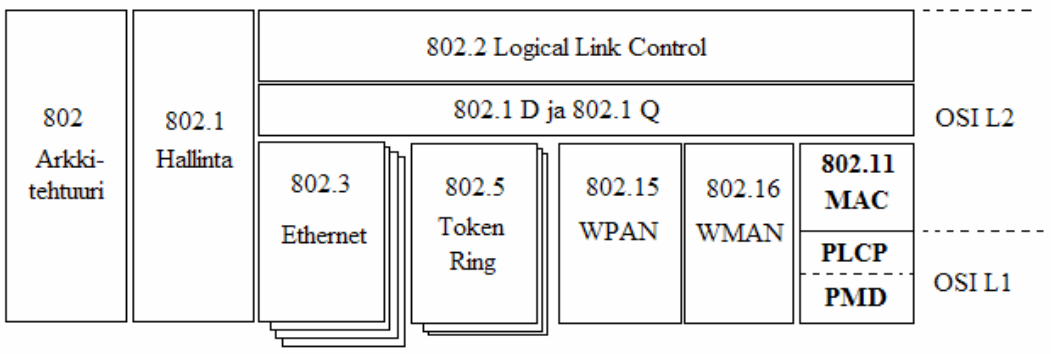


Kuva 1 OSI-mallin 7 eri kerrosta /33/

OSI-malli on ISO:n (*International Standardization Organization*) standardoima malli, jonka perusteella eri tietoliikennejärjestelmät tulisi suunnitella. OSI-mallissa ylempi kerros käyttää hyväkseen alempia kerroksia eli siirryttäessä ylöspäin pyramidia pitkin vaaditaan aina kehittyneempää tekniikkaa. Tässä tutkintotyössä keskitytään kuitenkin tarkasti vain 802.11-standardin käyttämiin siirtokerrokseen ja fyysiseen kerrokseen. Sekä fyysinen kerros että siirtokerros jaetaan vielä kahteen eri osaan. /33/

Nimensä mukaisesti fyysinen kerros siirtää bittivirran fyysisesti paikasta toiseen. Fyysinen kerros jaetaan konvergenssikerrokseksi ja mediasta riippuvaksi kerrokseksi. Konvergenssikerros sovittaa eri bittinopeudet ja fyysiset siirtotiet yhtenäiseksi palveluksi ja käyttää PPDU-kehystä (*Physical Protocol Data Unit*). PPDU-kehys on fyysisen tason tietosähke, joka sisältää mm. tiedon käytetystä bittinopeudesta ja sekoittimen alustuksen. Mediasta riippuva kerros määrittelee modulaation, hajaspektritekniikan ja kanavointi-tavan. Konvergenssikerroksesta käytetään lyhennettä PLCP (*Physical Layer Convergence Procedure*) ja mediasta riippuvasta kerroksesta lyhennettä PMD (*Physical Media Dependent*). /6, s.25/

Siirtokerros käsittelee fyysisen kerroksen sille välittämän datan kehyksinä. Siirtokerroksen tehtävänä on mm. luoda yhteys, korjata virheet ja purkaa yhteys. Siirtokerros jaetaan kahteen alikerrokseen, jotka ovat MAC-alikerros (*Medium Access Control*) ja LLC-alikerros (*Logical Link Control*). MAC-kehys vastaa vuoron varauksesta ja lisäksi se sisältää ohjaustiedot, sekvenssitiedot, tarkistussumman ja radiotiellä käytettävät osoitteet. LLC-kehys sisältää puolestaan protokollan tunnukset ja ohjauskentän. LLC-kehys määritellään 802.2-standardissa ja se muodostaa yhtenäisen rajapinnan kaikille 802-verkoille. /6, s.26/



Kuva 2 802-standardiperhe /6, s.26/

Kuvassa 2 on esitelty yhteenvetona 802.x-standardit. Kuvassa on siis OSI-mallin kaksi alinta kerrosta, OSI L1 vastaa fyysistä kerrosta ja OSI L2 siirtokerrosta. 802.11-standardi on kuvassa lihavoituna ja siihen kuuluvat siis MAC-alikerros ja fyysisen kerroksen PLCP ja PMD. IEEE 802.11 -standardit on vielä erikseen jaettu eri versioihin, joita ovat esimerkiksi 802.11, 802.11a, 802.11b, 802.11g. Tällä hetkellä suosituin standardi on 802.11g. /6; 33/

2.1.1 IEEE 802.11

IEEE esitteli ensimmäisen WLAN-standardinsa vuonna 1990. Ensimmäinen virallinen standardi julkaistiin kuitenkin vasta 7 vuotta myöhemmin heinäkuussa 1997, standardi sai nimekseen IEEE 802.11. IEEE 802.11-standardi oli kuitenkin melko hidas, se kykeni vain 1 ja 2 Mbit/s:n siirtonopeuteen, tästä syystä IEEE aloittikin hyvin nopeasti uuden standardin kehityksen. 802.11 toimii 2,4 GHz:n taajuudella ja se keskittyy OSI-mallin fyysiseen kerrokseen ja

MAC-kerrokseen. 802.11-standardissa määritellään välitystekniikoiksi infrapuna- ja radiotaajuustekniikka. Radiotaajuustekniikoista ovat käytössä suorasekvenssihajaspektri- ja taajuushyppelyhajaspektritekniikka. Suorasekvenssihajaspektritekniikasta käytetään lyhennettä DSSS (*Direct Sequence Spread Spectrum*) ja taajuushyppelyhajaspektritekniikasta lyhennettä FHSS (*Frequency Hopping Spread Spectrum*). 802.11-standardi käyttää kahta eri verkkotopologiaa, toinen niistä on AdHoc-verkko, jossa päätelaitteet ovat yhteydessä suoraan toisiinsa. Toinen standardin käyttämä verkkotopologia on ns. infrastruktuuri, jossa päätelaitteet ovat toisiinsa yhteydessä tukiaseman välityksellä. Verkkotopologioista ja radiotaajuustekniikoista kerrotaan vielä tarkemmin tutkintotyön luvussa 3. IEEE 802.11 -standardissa ilmeni nopeasti erilaisia puutteita, hitauden lisäksi ongelmia tuottivat myös yhteensopivuus-ongelmat ja käytettyyn taajuuskaistaan liittyvät käyttölupaongelmat. /19; 23/

2.1.2 IEEE 802.11b

Seuraava IEEE:n julkaisema WLAN-standardi ei ollutkaan 802.11a vaan 802.11b, joka julkaistiin vuonna 1999. 802.11a-standardi julkaistiin saman vuoden syksynä. 802.11b-standardi nosti nopeudet 11 Mbit/s:iin, mikä on huomattavasti edeltäjäänsä enemmän. Lisäksi 802.11b-standardi tarjoaa myös 1, 2 ja 5,5 Mbit/s:n siirtonopeudet. Kyseinen standardi toimii vapaalla 2,4 GHz:n taajuusalueella ja määrittelee ainoaksi välitystekniikakseen radiotaajuus-tekniikan eli standardissa on luovuttu infrapunatekniikasta. Radiotaajuus-tekniikoista 802.11b-standardi käyttää vain suorasekvenssihajaspektritekniikkaa (*DSSS*), ja 802.11-standardin käyttämästä taajuushyppelyhajaspektritekniikasta (*FHSS*) on myös luovuttu. 802.11b-standardin tuotteet ovat kuitenkin yhteensopivia 802.11-standardiin. Bittinopeuden mukaan 802.11b-verkossa käytetään joko Barker- tai CCK-hajautusta (*Complementary Code Keying*). CCK-tekniikassa tieto lähetetään 64:n 8-bittisen koodisanan sarjoina. Jokaisella sarjamuodossa olevalla koodisanalla on matemaattinen merkityksensä. Toinen vaihtoehto 802.11b-standardin tiedonsiirrossa on PBCC-tekniikka (*Packet Binary Convutional Coding*). 802.11b-standardista on myös olemassa versio 802.11b+, jonka nopeudeksi nostettiin 22 Mbit/s. Siirtonopeus onkin ainoa asia,

joka erottaa standardit toisistaan. 802.11b+-standardi ei kuitenkaan saavuttanut 802.11b-standardin saavuttamaa suosiota. /6, s.15; 19; 23/

2.1.3 IEEE 802.11a

Toinen IEEE:n vuonna 1999 julkaisema WLAN-standardi oli nimeltään 802.11a, se koki 802.11-standardiin verrattuna paljon suurempia muutoksia kuin 802.11b-standardi. 802.11a-standardi nosti teoreettiset nopeudet jopa 54 Mbit/s:iin käyttäen 5 GHz:n U-NII-taajuuksia (*Unlicenced National Information Infrastructure*). 802.11a-standardin merkittävimmäksi alueeksi jäivät Yhdysvallat ja Kanada, koska useissa muissa maissa 5 GHz:n taajuusalueet on varattu muuhun käyttöön. Suuremman taajuuden vuoksi 802.11a-standardin kantomatka on huomattavasti lyhempi kuin esimerkiksi 802.11b-standardin. Lisäksi ongelmia aiheutti laitteiden korkea hinta. Näiden ongelmien takia 802.11a- standardia ei ole juuri markkinoilla nähty. 802.11a-standardissa esiteltiin ensimmäistä kertaa OFDM-monitaajuusmodulointitekniikka (*Orthogonal Frequency Division Multiplexing*), joka perustuu signaalin jakamiseen pienempiin alasignaaleihin, joita käytetään rinnakkain. /6; 19/

2.1.4 IEEE 802.11g

IEEE:n 802.11g-standardi hyväksyttiin kesäkuussa 2003 ja se on nykyään yleisin käytetty WLAN-standardi. Nykyisin on myynnissä jopa 125 Mbit/s:n teoreettisen bittinopeuden tarjoavia WLAN-tukiasemia, jotka noudattavat 802.11g-standardia. Käytännössä nopeudet jäävät kuitenkin paljon alhaisemmiksi. 802.11g-standardi on yhteensopiva 802.11b-standardin mukaisten laitteiden kanssa. Standardi käyttää vapaassa käytössä olevaa 2,400-2,485 GHz:n ISM-taajuutta (*Industrial, Scientific, Medical*), joka jaetaan 13:een eri kanavaan. 802.11g käyttää samaa OFDM-modulointitekniikkaa kuin Pohjois-Amerikassa käytettävä 802.11a-standardi. 802.11g-standardi sisältää myös CCK-koodauksen yhteensopivuussyistä. /6/

2.1.5 IEEE 802.11n

IEEE 802.11n-standardin odotetaan valmistuvan vuoden 2007 lopulla, ensimmäinen luonnos siitä hyväksyttiin tammikuussa 2006. 802.11n-standardilla päästään teoriassa jopa 540 Mbit/s:n tiedonsiirtonopeuteen, mutta käytännössä tyypillinen nopeus on n. 200 Mbit/s. 802.11n-standardista pyritään tekemään yhteensopiva kaikkien aikaisemmin julkistettujen 802.11-standardien kanssa ja yhteensopivuuteen pyritään myös eri toimittajien välisissä laitteissa. Näin ollen uuden standardin tulee toimia sekä 2,4 GHz:n, että 5 GHz:n taajuusalueella. 802.11n-standardi mahdollistaa signaalin, joka kantaa 300 metriä. /23; 18/

2.1.6 Muut 802.11-standardit

IEEE on julkaissut 802.11-standardeista myös lisäominaisuuksia sisältäviä standardeja, joista kerron seuraavassa lyhyesti. 802.11e on kehitetty parantamaan WLAN-verkon soveltuvuutta multimediapalveluihin. 802.11f-standardi pyrkii parantamaan WLAN-verkoissa eri valmistajien välistä yhteensopivuutta. Se määrittelee liikenteen liityntäpisteiden välissä. 802.11h-standardi puolestaan sisältää lisämääritykset 5GHz:n taajuusalueen käytölle Euroopassa. 802.11i-standardi on kehitetty parantamaan tietoturvaa ja 802.11j sisältää Japania koskevat laajennukset. 802.11d-standardi on kehitetty, jotta 802.11-standardin mukaisia laitteita voitaisiin käyttää maissa, joissa niitä ei saa käyttää. 802.11k on puolestaan parannus WLAN-systeemin hallintaan ja 802.11x on lähiverkkojen pääsyn valvontastandardi. /6, s.47; 23/

2.1.8 Tiivistelmä 802.11-standardeista

IEEE:n ratifioimat 802.11-standardit ovat siis käytetyimpiä WLAN-standardeja. Ilman käyttölupaa Suomessa saa käyttää 802.11-, 802.11b-, 802.11a- ja 802.11g-standardeja. 802.11a-standardi toimii 5 GHz:n taajuusalueella, kaikki muut tämän hetken 802.11-standardit toimivat 2,4 GHz:n taajuusalueella. 802.11g on tällä hetkellä käytetyin standardi, sillä päästään

teoriassa jopa 125 Mbit/s:n siirtonopeuteen. Suomessa 802.11-standardeille on määritelty myös suurimmat sallitut EIRP-tehot (*Effective Isotropic Radiation Power*) eli radiolähettimien lähetystehot. Suurimmat sallitut EIRP-tehot 5 GHz:n taajuusalueella ovat 200mW ja 2,4 GHz:n taajuusalueella 100mW. Taulukossa 1 on vielä vertailtu eri 802.11-standardien ominaisuuksia. /6, s.46/

Taulukko 1 802.11-standardien ominaisuuksia /6, s. 46/

Standardi	802.11	802.11b	802.11a	802.11g	802.11n
Julkaistu	1997	1999	1999	2003	2007(arvio)
Taajuusalue	2,4 GHz	2,4 GHz	5 GHz	2,4 GHz	2,4 ja 5 GHz
Teoreettinen siirtonopeus	1 Mbit/s 2Mbit/s	11 Mbit/s	54 Mbit/s	1-125 Mbit/s	~300 Mbit/s
Yhteensopivuus		802.11g 802.11n	802.11n	802.11b 802.11n	802.11a 802.11b 802.11g
Hajaspektitekniikat	FHHS, DSSS	DSSS	OFDM	OFDM	
Mediat	IF, RF	RF	RF	RF	RF
Kanavia yht.	14 (DSSS)	14	12	12	
Ei päällekkäisiä kanavia	3	3	12	3	
Kavavat (Suomessa)	1-13	1-13	36, 40, 44, 48	52, 56, 60, 64	
EIRP- teho	100 mW	100 mW	200 mW	100 mW	
Käyttökohteet (Suomessa)	sisä- ja ulkotiloissa	sisä- ja ulkotiloissa	vain sisätiloissa	sisä- ja ulkotiloissa	

2.2 HiperLAN

HiperLAN-standardit (*High Performance Radio Local Area Networks*) ovat eurooppalaisen telealan standardoimisjärjestön ETSI:n standardoimia. HiperLAN-standardeista on kaksi eri versiota: HiperLAN/1 ja HiperLAN/2. Molemmat versiot toimivat 5 GHz:n taajuusalueella. HiperLAN-standardit toimivat 802.11-standardien tavoin OSI-mallin kahdella alimalla kerroksella eli siirtokerroksessa ja fyysisessä kerroksessa. HiperLAN-standardit toimivat silloin, kun kiinteätä yhteyttä ei ole saatavissa yhteyden missään osassa.

2.2.1 HiperLAN/1

HiperLAN/1-standardi julkaistiin vuonna 1998. Standardille on määritelty tiedonsiirtonopeudeksi 20 Mbit/s ja sen kantama on vain n. 50 metriä. Tiedonsiirtoon HiperLAN/1 käyttää viittä eri kanavaa taajuuksilla 5,15-5,35 GHz. Tiedonsiirto tapahtuu datapurskeissa, jotka tapahtuvat erilaisilla taajuusmuunnoksilla. /29/

2.2.2 HiperLAN/2

HiperLAN/2-standardi julkaistiin vuonna 2000. Sen teoreettinen tiedonsiirtonopeus on 54 Mbit/s. HiperLAN/2 toimii myös 5 GHz:n taajuusalueella ja käyttää OFDM-modulaatiota. Tiedonsiirtomenetelmänä se käyttää yhteydellistä protokollaa ja aikajakokanavointia. Menetelmä on tehokas multimediasovelluksissa. /1/

2.3 Bluetooth

Bluetooth-tekniikka syntyi muun muassa Ericssonin, IBM:n, Intelin, Nokian ja Toshiban yhteistyön tuloksena vuonna 1998. Se ei ole standardi vaan ainoastaan spesifikaatio. Se on tarkoitettu lyhyehköihin etäisyyksiin päätelaitteiden liittämiseksi, siksi sen virrankulutus onkin pieni. Sitä pidetään hyvänä ratkaisuna pienellä alueella työskentelevän yksittäisen henkilön pienlaitteiden yhdistämiseen. Bluetooth-tekniikkaa esiintyykin esimerkiksi kännyköissä.

Bluetooth-tekniikka toimii 2,4 GHz:n taajuusalueella ja sen tiedonsiirtonopeus on 1 Mbit/s. Alhaisen tehon Bluetooth-laitteiden kantama on vain n. 10 metriä, kun taas suuren tehon Bluetooth-laitteilla ylletään jopa 100 metrin kantamaan. Nykyisin käytössä on lähinnä vain alhaisen tehon Bluetooth-laitteita. Bluetooth käyttää taajuushyppelytekniikkaa. Nykyään tekniikkaa käytetään lähinnä pienlaitteiden yhdistämiseen. Esimerkiksi kännykällä otettuja valokuvia voidaan siirtää Bluetooth-tekniikan avulla tietokoneelle. /1, s.96/

2.4 WiMAX

Tällä hetkellä kehityksen alaisena oleva WiMAX-standardi (*Worldwide Interoper-ability for Microwave Access*) perustuu IEEE 802 -sarjan avoimeen 802.16-standardiin. Se julkaistiin keväällä vuonna 2002, minkä jälkeen siitä on julkaistu monia uudempia versioita. Sen kehityksestä vastaa yli 200 yrityksestä koostuva WiMAX-foorumi, johon kuuluu esimerkiksi Nokia. /30/

WiMAX:n kantama on huomattavasti suurempi kuin WLAN-verkkojen, sillä voidaan optimaalisissa olosuhteissa saavuttaa jopa 50 kilometriä. Käytännössä kuitenkin 20 kilometrin kantamat ovat todennäköisempiä. WiMAX on myös tiedonsiirtonopeudeltaan WLAN:ia parempi. Se pystyy tarjoamaan nopeudeltaan kaapelimodeemi ja DSL-yhteyksiä vastaavia langattomia yhteyksiä. Sen toimintaa voidaankin hyvin pitkälti verrata WLAN:in toimintaan. /30/

WiMAX-systeemi koostuu koostuu kahdesta eri osasta: WiMAX-tukiasemasta ja WiMAX-vastaanottimesta. Tukiasema muistuttaa radiomastoa, jonka avulla se on yhteydessä operaattoriin kaapeliyhteyden avulla tai mikroaaltolinkillä toisen maston kautta. Yksi tukiasema pystyy tarjoamaan DSL-tasoisen yhteyden sadoille kodeille. WiMAX-verkkoja onkin rakennettu syrjäseuduille, esimerkiksi kesämökkien verkottamiseksi. WiMAX tarjoaa sekä näköyhteydellisen että näköyhteydettömän langattoman palvelun. WiMAX toimii Yhdysvalloissa 2,5 GHz:n ja 5,8 GHz:n taajuusalueilla ja Euroopassa 3,5 GHz:n taajuusalueella. 802.16-standardi kattaa kuitenkin 2-11 GHz:n taajuusalueet. WiMAX-tekniikkaa käytetään 802.11-standardien kanssa. WiMAX ei siis korvaa WLAN:ia, vaan täydentää niitä langattomana laajakaistana. /30; 6,s.48/

Tutkimusyhtiö InStat pohtii WiMAX:n tulevaisuutta Tietokonelehden Internet-sivuilla. Yhtiö uskoo, että ensimmäiset mobiiliin WiMAX-laajakaistatekniikkaan perustuvat päätelaitteet tulevat markkinoille vuoden 2007 lopussa, mutta ei usko niiden uhkaavan kolmannen sukupolven matkapuhelinverkkoja ainakaan tällä vuosikymmenellä. /16/

2.5 WLAN-standardien tulevaisuus

Tulevaisuuden tavoite langattomissa lähiverkoissa on rakentaa koko maailman kaupungit ja taajamat kattava langaton verkko. Pieni espanjalainen IT-yritys, Fon, onkin jo aloittanut tällaisen verkon kehityksen. Fonin idea on yksinkertainen: käyttäjät jakavat Internet-operaattorin signaalin pienellä ikkunan ääreen sijoitetulla langattomalla lähettimellä. Siis jakamalla oman verkkonsa saa tunnuksen myös toisten WLAN-verkkoihin. Jos lähettimiä on tiuhassa, saadaan kattava verkko. Tulossa oleva 802.11n-tekniikka mahdollistaa signaalin, jonka kantosäde on n. 300m. Näin ollen jopa muutama lähetin kattaisi koko korttelin. Operaattorit eivät kuitenkaan välttämättä tykkää ajatuksesta, että niiden verkkoja jaetaan yleiseen käyttöön vain yhden maksaessa palvelusta. It-alan mediassa onkin ollut epäilyjä, että operaattorit saattavat nostaa syytteitä Fonia vastaan sääntöjen rikkomisesta, yhtään syytettä ei ole kuitenkaan toistaiseksi tullut. Fonin 48-vuotias argentiinalainen toimitusjohtaja Martin Varsavsky /7/ vakuuttaakin, että ”puhelinyhtiöt ja muut Internet-palveluja toimittavat operaattorit vihaavat Fonia nyt, mutta ne alkavat sietää sitä ensi vuonna. Vuonna 2008 ne jo rakastavat Fonia, koska se ei tuota heille tappiota vaan tuloja”. Tällä hetkellä kuitenkin esimerkiksi suomalaiset operaattorit kieltävät yleensä sopimusehdoissaan WLAN-verkon jakamisen kotitalouden ulkopuolelle. Varsavsky kuitenkin uskoo rakentaneensa Fonin siten, että siitä hyötyvät kaikki osapuolet. Hänen mukaansa kyse on yhtä hyvin kansanliikkeestä kuin liiketoiminnasta. /7; 15/

Fon on jakanut käyttäjänsä kolmeen ryhmään, jotka ovat linus, bill ja alien. Linus-käyttäjäryhmä on saanut nimensä Linus Torvaldsin mukaan. Linus-käyttäjät maksavat Internet-operaattorille normaalisti, mutta jakavat signaalinsa toisten linus-käyttäjien kanssa. Näin ollen linus-käyttäjillä on verkko käytössään kaikkialla samalla perusmaksulla. Bill-käyttäjäryhmä on puolestaan saanut nimensä Microsoftin perustajan Bill Gatesin mukaan. Myös bill-käyttäjät maksavat normaalisti Internet-operaattorille. Bill-käyttäjät voivat kuitenkin myydä verkkoyhteyttään eteenpäin kahden euron päivähintaan satunnaisille käyttäjille eli alien-käyttäjille. Alien-käyttäjä voi olla esimerkiksi ihminen,

jonka tulee soittaa ulkomaanpuhelu WiFi-kelpoisella kännykällään. GSM-yhteyttä paljon halvemmaksi tulee käyttää Internet-yhteyttä puhelussaan, jolloin voi ostaa bill-käyttäjältä puheluun tarvittavan verkkoyhteyden. Juuri nämä alien-käyttäjät rahoittavat maksuillaan Fonin toiminnan. Kun bill-käyttäjä myy yhteyksiänsä, hän saa puolet rahasta ja puolet menee Internet-operaattorille. Näin ollen myös operaattorit hyötyvät, koska bill-käyttäjät toimivat niiden myyntimiehinä. Lisäksi operaattorit saavat linus-käyttäjiltä ja bill-käyttäjiltä normaalit tilausmaksut nettiyhteyksistä. /7; 15/

Fon-verkko eroaa täysin avoimista WLAN-verkoista, koska Fon-verkossa tukiasemaan asennetaan ohjelma, joka eristää jaetun ja julkisen WLAN-verkon käyttäjän omasta kotiverkosta. Verkkoon saadaan käyttäjätunnukset jakamalla oma verkko. Fonin tietokoneohjelma huolehtii myös automaattisesti yhteyksistä ja maksuliikenteestä. Fonin ohjelmisto toimii kuitenkin tällä hetkellä vain harvojen tukiasemien kanssa. Linksysin mallit WRT54G, WRT54GS, WRT54GL ovat tällä hetkellä ainoita tukiasemia, jotka ovat yhteensopivia Fon-ohjelmistojen kanssa. Tällä hetkellä maailmassa on noin 20 000 Fon-käyttäjää, joista 5000 on Espanjassa ja saman verran Yhdysvalloissa. Loput käyttäjät ovat jakautuneet eri Euroopan maihin. Esimerkiksi ruotsalainen Internet-operaattori Glocalnet on tehnyt sopimuksen Fonin kanssa ensimmäisenä nettipalvelun toimittajana. Lisäksi toimitusjohtaja Varsavsky sanoo Fonin käyvän neuvotteluja 15 muun suuren eurooppalaisen operaattorin kanssa. Fon on saapumassa myös Suomeen. Varsavsky nimesi Nokialla työskentelevän Marko Ahtisaaren Suomen Fon-lähettiläälksi. Ahtisaari /15/ kertookin innokkaana odottavansa tuodakseen Fonin Suomeen ja muuttaaksen Helsingin ja muut kaupungit Suomessa jaettujen WLAN-verkkojen alueiksi. Aika näyttää, kuinka alkujaan pienen espanjalaisyrityksen yritys rakentaa koko maailman kattava langaton verkko tulee onnistuu.

3 WLAN-tekniikkaa

WLAN-tekniikan avulla pystytään rakentamaan langattomia lähiverkkoja rajatulle alueelle. Käytettäessä langattomia lähiverkkoja ei tarvita mitään erillistä siirtotietä sillä data liikkuu sähkömagneettisina aaltoina tukiasemien välillä. Tukiasemat voivat esimerkiksi olla liitettyinä perinteiseen Ethernet-verkkoon. Tukiasemat vastaanottavat, puskuroivat ja lähettävät dataa langallisen ja langattoman lähiverkon välillä. Jotta työasemalla pääsisi WLAN-verkkoon, tulee siinä olla WLAN-adapteri. WLAN-adapteri voi olla kiinteä tietokoneeseen liitetty kortti tai valmiiksi emolevyyn integroitu ominaisuus. Korteissa on lähetin ja vastaanotin, joiden avulla voidaan toteuttaa radioyhteys toiseen laitteeseen. Lähes kaikissa uusissa tietokoneissa on nykyään valmiina WLAN-ominaisuus. Nykyään on myös mahdollista liittää tietokoneen USB-porttiin WLAN-adapteri. WLAN-adapterissa on lähetin ja vastaanotin, joiden avulla voidaan toteuttaa yhteys toisesta tietokoneesta toiseen tukiaseman välityksellä. WLAN-tekniikka perustuu luvussa 2 esiteltyyn IEEE:n 802.11-standardi-perheeseen. Tällä hetkellä käytetyin siirtotekniikka langattomissa lähiverkoissa ovat radioaallot. Radioaaltojen lisäksi voidaan käyttää infrapunatekniikkaa, lasertekniikkaa tai mikroaaltotekniikkaa. Nykyisin käytössä olevat standardit tosin toimivat ainoastaan käyttämällä radiolähetystä. Radioaaltojen etuna muihin on se, että niissä ei tarvita näköyhteyttä päätteen ja lähettimen välille. Infrapunayhteydessä vaaditaan joko suoraa tai heijastettua näköyhteyttä lähettimen ja päätteen välille, koska infrapunavalo ei pysty läpäisemään läpinäkymätöntä estettä. Infrapunatekniikalla pystytään saavuttamaan vain 1-2 Mbit/s:n tiedonsiirtonopeuksia ja se sopii parhaitein paikkoihin, joissa ei ole esteitä ja välimatkat ovat lyhyitä. Lasertekniikassa käytetään nimensä mukaisesti tiedonsiirtoon laservaloa. Lasertekniikka vaatii myös suoraa näköyhteyttä, eikä tekniikka ole saavuttanut suurta suosiota. Mikroaalto-tekniikka on myös harvinainen ja sitä käytetään lähinnä vain Yhdysvalloissa. Tässä tutkintotyössä perehdytään tarkasti vain radioaaltotekniikkaan. /3,9/

Vaikka radioaaltotekniikka ei vaadikkaan näköyhteyttä päätteen ja lähettimen välille, fyysiset esteet, kuten esimerkiksi seinät, ihmiset, ovet ja puut

heikentävät signaalin etenemistä. Lisäksi radioaaltojen etenemiseen vaikuttavat vaimennus, heijastukset, monitie-eteneminen, taipuminen ja sironta. Radioaaltotekniikoita on kahta eri lajia, kapeakaistatekniikka ja hajaspektritekniikka. Näistä tekniikoista hajaspektritekniikka jaetaan vielä kahteen alalajiin, suorasekvenssi- ja taajuushyppelytekniikkaan. Suorasekvenssitekniikasta käytetään yleisesti lyhennettä DSSS (*Direct Sequence Spread System*) ja taajuushyppelytekniikasta lyhennettä FHSS (*Frequency Hopping Spread System*). Kapeakaistatekniikka ei salli kuin yhden palvelun käytön kerrallaan ja se onkin poistunut käytöstä jo lähes kokonaan. Tässä tutkintotyössä keskitytäänkin tarkasti vain hajaspektritekniikkoihin. /13/

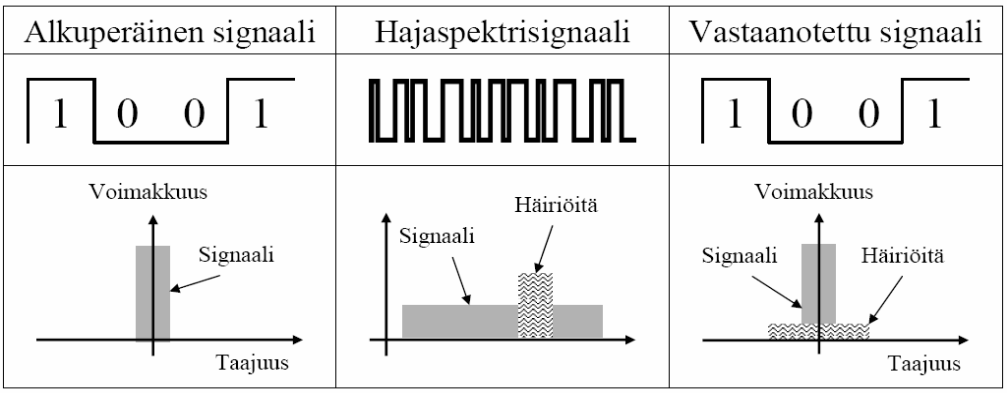
3.1 Hajaspektritekniikat

Hajaspektritekniikat jaetaan siis kahteen osaan, suorasekvenssitekniikkaan (*DSSS*) ja taajuushyppelytekniikkaan (*FHSS*). Hajaspektritekniikat kehitettiin alun perin sotilaskäyttöön, koska ne ovat luotettavia ja niillä on laajahko peittoalue, lisäksi niillä on hyvä häiriönsietokyky. Hajaspektritekniikassa taajuusalue jaetaan koodin avulla joukkoon alitaajuuksia, joilla tietoa lähetetään samanaikaisesti. Radiolähetys on hajautettu molemmille puolille kantoaaltoa laajemmalle alueelle kuin bittinopeuden vuoksi olisi tarpeellista. Tämän tarkoituksena on poistaa häiriöitä. Standardeista 802.11 ja 802.11b käyttävät hajaspektritekniikoita. 802.11a ja 802.11g puolestaan käyttävät OFDM-moni-kantoaaltomodulointia. DSSS ja FHSS sijoittuvat OSI-mallin fyysiseen kerrokseen. /9/

3.1.1 DSSS, suorasekvenssitekniikka

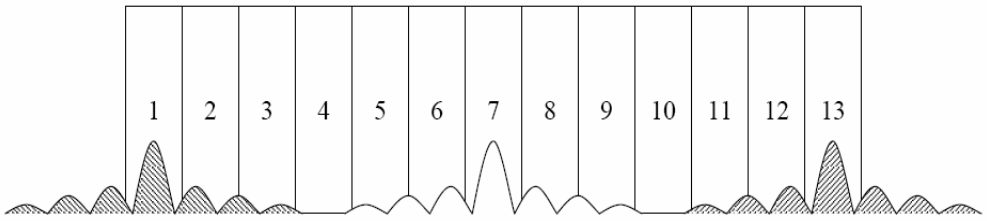
Suorasekvenssitekniikkaa (*DSSS*) käytetään standardeissa 802.11 ja 802.11b. DSSS käyttää jatkuvasti 22 MHz:n kaistanleveyttä taajuusalueella 2,4 – 2,4835 GHz . Kaikkia taajuusalueen alitaajuuksia käytetään rinnakkain ja bittijono hajautetaan entistä laajemmalle taajuusalueelle. 802.11b-standardissa hajautus-menetelmiä on kaksi erilaista. Alemmilla bittinopeuksilla käytössä on Barker-

hajautus ja yli 2 Mbit/s:n bittinopeuksilla käytössä on CCK-hajautus (*Complementary Code Keying*).



Kuva 3 DSSS:n toiminta Barker-hajautusta käyttäen /14, s.45/

Barker-hajautuksessa yksi bitti levitetään 11 bitiksi eli silloin sen taajuusalueeksi tulee 22-kertainen alkuperäiseen dataan verrattuna. Kuvassa 3 on havainnollistettu Barker-hajautusta, lähetin levittää alkuperäisestä bittijonosta yhden bitin 11 bitiksi, kun taas vastaanotin muuttaa hajaspektrisignaalin takaisin alkuperäiseksi signaaliksi. Bittijonon hajautus ja demodulointi tapahtuu PN-koodin (*Pseudo Noise*) avulla. Kuvasta 3 voidaan myös lisäksi havaita, että hajaspektrisignaali on alkuperäistä signaalia heikompi ja leveämpi. Lisäksi tekniikka sietää hyvin häiriöitä.



Kuva 4 Euroopassa käytettävät DSSS-kanavat /14, s. 46/

Standardin 802.11b DSSS:n käyttämä taajuusalue jaetaan osittain päällekkäisiksi kanaviksi. Suurimassa osassa Eurooppaa taajuusalue on jaettu 13:een eri kanavaan, joista 1 ja 13 ovat täysin erilliset. Kuitenkin jo kanavat 1 ja 7 ovat riittävän etäällä toisistaan, jotta niitä voidaan käyttää toisiaan lähellä sijaitsevissa tukiasemissa. Kanavat toimivat taajuusalueella 2,4-2,485 GHz ja ne on jaettu 5 MHz:n välein. Kuvassa 4 on esitelty kanavat. Kuvasta havaitaan, että kanavat ovat osittain päällekkäin, joten vierekkäisiltä kanavilta voi johtua

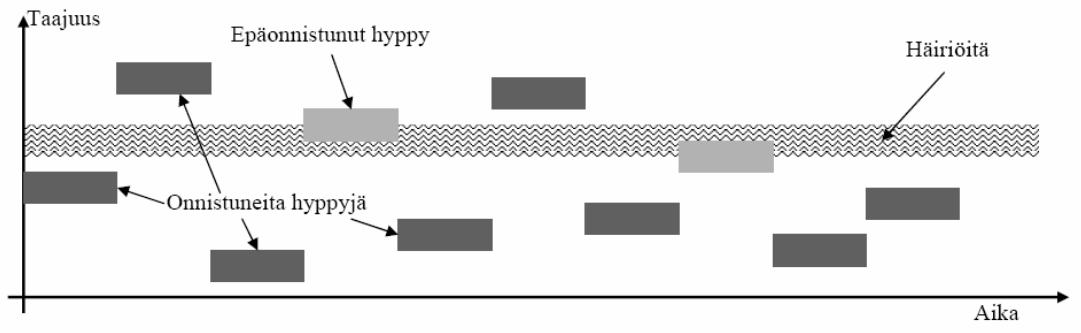
häiriöitä signaaliin. Juuri tästä syystä vierekkäisissä soluissa ei saa käyttää vierekkäisiä tai toisiaan lähellä olevia kanavia. Vaan tulee käyttää ns. ei-päällekkäisiä kanavia, joita Euroopassa ovat 1, 7 ja 13. Myös 1, 6 ja 13 sekä 1, 8 ja 13 ovat ei-päälekkäisiä kanavia. Ei-päälekkäisissä kanavissa keskitaajuudet eroavat enemmän kuin kanavanleveys. /14, s. 42-48/

Barker-hajautusta käytetään siis alle 2 Mbit/s:n siirtonopeuksissa. Yli 2 Mbit/s:n siirtonopeuksilla käytetään CCK-hajautusta. CCK-hajutusta käytetään yhdessä QPSK-modulaation kanssa. CCK-hajautuksessa 11-bitin hajautuksen jälkeen ryhmitellään alkiobitit kahdeksan alkion koodisanoiksi. Tämän jälkeen alkiovirrasta erotellaan lohkoja, joista osa koodataan vaihe-eroa käyttäen ja loput sopivasti valituilla koodisanoilla. Esimerkiksi 5,5 Mbit/s siirtonopeudella alkiovirrasta erotetaan neljän bitin lohkoja, joista kaksi koodataan nelitasoisella vaihe-erolla ja loput kaksi bittiä sopivasti valituilla kahdeksan bitin koodisanoilla. /6, s.36-39; 14, s. 42-48/

3.1.2 FHSS, taajuushyppelytekniikka

FHSS (*Frequency Hopping Spread System*) eli taajuushyppelytekniikka on toinen langattomissa lähiverkoissa käytetty hajaspektritekniikka. FHSS tekniikkaa on käytetty vain standardissa 802.11 ja tekniikka salliikin korkeintaan 2 Mbit/s siirtonopeuden. Myös FHSS:n taajuusalue on tyypillisesti 2,4-2,485 GHz:a, se on kuitenkin jaettu peräti 79 eri kanavaan eli yhden kanavan kaistanleveys on 1 MHz. Lähetettävä signaali pilkotaan pieniin osiin ja jokainen osa lähetetään aikavälein kullakin kapealla kanavalla. Myös vastaanottimen tulee tietää millä tietyllä taajuudella signaalia lähetetään. Taajushyppelytekniikassa signaalia lähetetään ja vastaanotetaan yhdellä taajuudella, jonka jälkeen hypitään edestakaisin kaikkien taajuuksien välillä. Yhtä taajuutta käytetään yleensä 100 ms. Taajuutta vaihdellaan tietyn algoritmin mukaan, jonka vain lähettäjä ja vastaanottaja tietävät. FHSS käyttää FSK-modulaatiota (*Frequency Shift Keying*), siinä digitaalisen tiedon nollat vastaavat yhdellä taajuudella lähetettyä pulssia ja ykköset puolestaan vastaavat toisella taajuudella lähetettyä pulssia /27/. Taajuushyppely voi olla joko hidasta tai

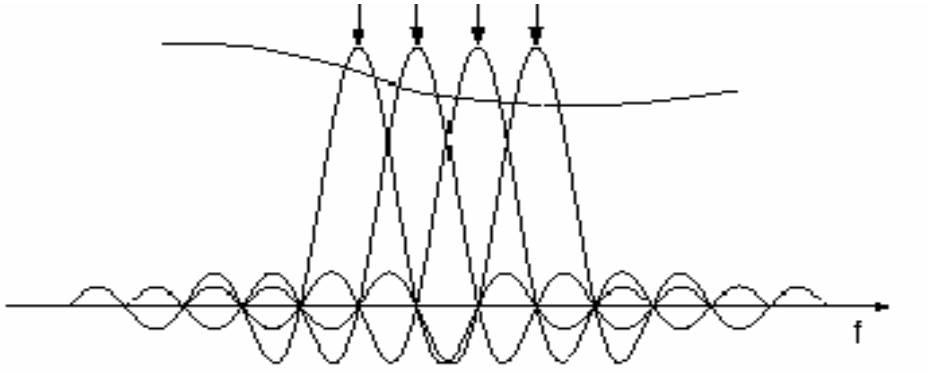
nopeata. Hitaassa taajuushyppelyssä lähetetään yksi bitti yhdessä aikavälissä, kun taas nopeassa lähetetään yksi bitti useammalla aikavälillä. Kuvassa 5 on esitelty FHSS:n toimintaa, epäonnistuneet hypyt lähetetään uudelleen toista taajuuskanavaa pitkin ja häiriölliset kanavat otetaan pois käytöstä. /27; 32; 11/



Kuva 5 FHSS:n toiminta, jossa epäonnistuneet hypyt osuvat häitiölliselle taajuuskaistalle /14, s. 50/

3.2 OFDM-monikantoaaltomodulointi

802.11a- ja 802.11g-standardit käyttävät tiedonsiirtotekniikkanaan OFDM-monikantoaaltomodulointia (*Orthogonal Frequency Division Multiplexing*). OFDM-tekniikassa siirrettävä data on jaettu eli multipleksoitu eri taajuuksisiin alikanaviin, joita käytetään rinnakkain. Alikanavat ovat kaistaltaan kapeita ja niiden keskifrekvenssit ovat toisiinsa nähden ortogonaalisia. Ortogonaalisuudella tarkoitetaan sitä, että yhden kantoaallon taajuuden ollessa keskikohdassaan on muiden aaltojen amplitudi nollassa. Tästä syystä eivät kantoaallot häiritse toisiaan. Kuvassa 6 on esitelty neljä signaalia monikantoaaltomoduloituna, jolloin jokaisen signaalin huipussa muut signaalit ovat nollassa. Ortogonaalisuudesta johtuen alikanavien spektrit ovat toisistaan riippumattomia.



Kuva 6 OFDM kanavien ortogonaaliset taajuusspektrit /20/

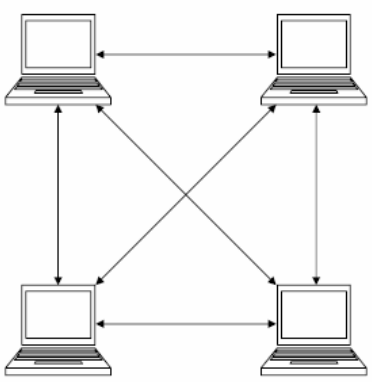
Käytännössä OFDM toimii siten, että lähetin päässä multipleksaaja välittää datavirrat lähettimen modulaattoriin. Lähetin muodostaa lähetettävän signaalin osakanavista käyttämällä käänteistä nopeaa Fourier-muunnosta ja pelkästään lähetyssignaalin spektrillä on merkitystä. Puolestaan vastaanottavassa päässä demodulaattori ja demultiplekseri muuttavat tulevat analogiset signaalit alkuperäiseen muotoonsa. Vastaanotin laskee myös amplitudit alikanavien taajuusspektristä käyttämällä Fourier-muunnosta. /6, s. 40-41/

3.3 Verkkotopologiat

Verkkotopologialla tarkoitetaan sitä, miten laitteet on kytketty toisiinsa. WLAN-verkoissa noudatetaan kolmea eri verkkotopologiaa, jotka ovat: IBSS (*Independent Basic Service Set*), BSS (*Basic Service Set*) ja ESS (*Extended Service Set*). Jokainen topologia perustuu soluarkkitehtuuriin, jossa jokaista solua valvoo tukiasema.

3.3.1 IBSS (*Independent Basic Service Set*)

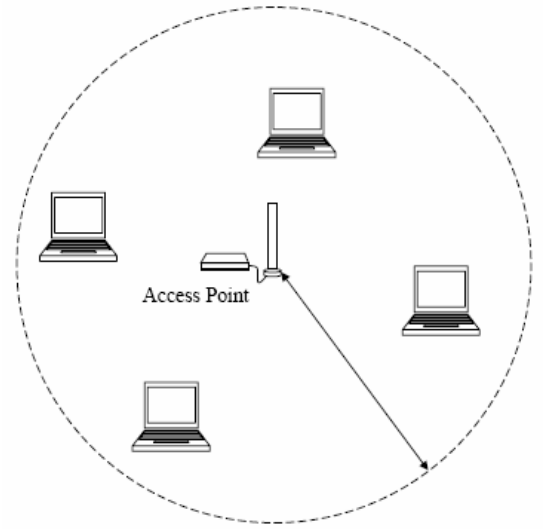
IBSS-verkoissa langaton verkko ei ole yhteydessä kiinteään verkkoon. IBSS-verkosta käytetään myös nimeä AdHoc-verkko. AdHoc-verkot poikkeavat muista topologioista siten, että sillä ei ole lainkaan tukiasemia. Päätelaitteet ovat yhteyksissä suoraan toisiin päätelaitteisiin radioyhteyden avulla, lähettiminä ja vastaanottimina toimivat langattomat verkkokortit. AdHoc-verkot ovat pieniä ja paikallisia verkkoja ja ne ovatkin hyvin verrattavissa Bluetooth-verkkoihin /14, s. 27/. AdHoc-verkoissa päätelaitteet voivat lähettää tiedon suoraan toiselle samassa verkossa olevalle päätelaitteelle, ilman, että tiedon tarvitsisi kulkea useamman laitteen kautta, jolloin verkkoa ei turhaan rasiteta. AdHoc-verkko soveltuukin parhaiten pieniin tiloihin kuten esimerkiksi kokouksiin, jossa osallistujat tuovat mukanaan omia laitteita ja keskustelevat niiden välityksellä toistensa kanssa. AdHoc-verkot ovat siis melko yksikertaisia ja niillä ei pääse Internetiin, siksi tietoturva onkin AdHoc-verkoissa helppo toteuttaa. Lisäksi AdHoc-verkko on melko yksinkertainen ja nopea rakentaa. /6, s.132; 9, luku 2/



Kuva 7 AdHoc-verkoissa päätelaitteet ovat suorissa yhteyksissä toisiinsa ilman tukiasemaa /14 s. 27/

3.3.2 BSS (*Basic Service Set*)

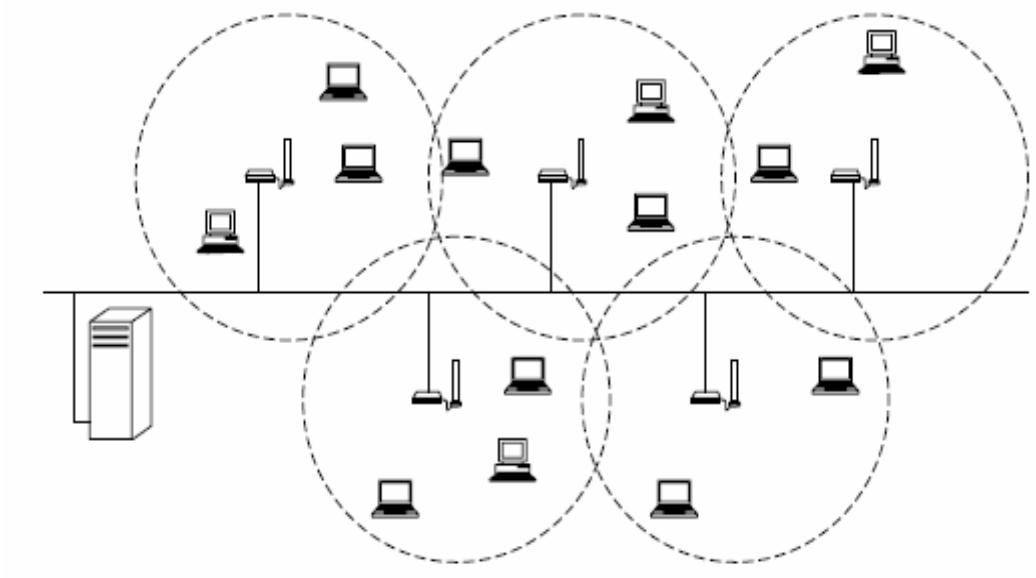
BSS-verkot kuuluvat infrastruktuurisiin verkkoihin. Infrastruktuuriset verkot on liitetty vähintään yhdellä tukiasemalla langalliseen lähiverkkoon, joiden välityksellä pääsee Internetiin. BSS:n tapauksessa verkko on liitetty langalliseen lähiverkkoon yhdellä tukiasemalla. IBSS-verkkoon verrattuna BSS-verkko käyttääkin kaksinkertaisen kapasiteetin tiedonsiirtoon laitteelta toiselle, koska data on ensin siirettävä ainoalle tukiasemalle ja vasta tämän jälkeen vastaanottajalle. BSS-verkoissa kaikki liikenne kulkeekin yhden tukiaseman kautta, jolloin tämä tukiasema joutuukin kovalle rasitukselle. Tukiaseman kaatuessa kaatuu koko verkko. BSS soveltuu hyvin koteihin ja toimistoihin. /2, s.232; 9/



Kuva 8 BSS-verkoissa päätelaitteet ovat yhteydessä langalliseen lähiverkkoon yhden tukiaseman kautta /14, s.28/

3.3.3 ESS (*Extended Service Set*)

ESS on myös infrastruktuuriverkko, kuten BSS, mutta se on yhteydessä langalliseen lähiverkkoon useamman tukiaseman välityksellä. Kaikki suuremmat WLAN-kokonaisuudet ovatkin yleensä ESS-tyyppisiä. Käytännössä ESS-verkot koostuvat useista BSS-verkoista. Kuvassa 9 on esitelty viidestä tukiasemasta koostuva ESS-verkko. Yhdelle tukiasemalle suositellaan 20-60 päätelaitetta, vaikka yhdellä tukiasemalla voi teoriassa olla jopa useampi sata päätelaitetta. Mitä enemmän yhdellä tukiasemalla on päätelaitteita sitä enemmän verkko kuormittuu. ESS-verkoissa yhden tukiaseman kattamaa aluetta kutsutaan mikrosoluksi. Samaa kanavaa käyttävillä mikrosoluilla tulee olla tarpeeksi etäisyyttä toisiinsa jotteivat ne sotkeutuisi keskenään. Mikrosolujen peittämät voidaan rakentaa osittain päällekkäisiksi, jolloin käyttäjät eivät huomaa siirtymistä mikrosolusta toiseen. /2, s.233; 9/



Kuva 9 ESS-verkko, joka on yhdistetty runkoverkkoon viidellä tukiasemalla /14, s.29/

4 TIETOTURVA WLAN-VERKOISSA

Langattomissa lähiverkoissa on kiinnitettävä erityistä huomiota tietoturvallisuuteen, koska viestisignaalit ovat avoimesti tavoitettavissa niiden liikkuessa ilmassa. Langattoman lähiverkon käyttäjän tulee olla tietoinen mahdollisista ongelmista ja niihin soveltuvista vastatoimenpiteistä. Tietoturvaa pidetään yhtenä suurimpana ongelmana langattomissa verkoissa ja usein syy tähän on verkon omistajassa. Vielä nykyäänkin löytyy huolestuttavan paljon langattomia verkkoja täysin vailla tietoturvaa. Oikeilla toiminnoilla ja asetuksilla saadaan langattomasta lähiverkostakin turvallinen. Tässä luvussa käsitellään tietoturvauhkia ja tapoja, joilla langattoman verkon tietoturvaa voidaan parantaa.

4.1 Tietoturvan tavoitteet /6 s.70/

IETF (*Internet Engineering Task Force*) on järjestö, joka on määritellyt tietoturvallisuudelle tietyt tavoitteet. Nämä tavoitteet sopivat hyvin myös langattomien lähiverkkojen tietoturvallisuuden tavoitteiksi. Tavoitteita on kaikkiaan kuusi ja ne ovat: tiedon luottamuksellisuus, tiedon eheys, todennus, kiistämättömyys, pääsynvalvonta ja käytettävyys.

Tiedon luottamuksellisuudella tarkoitetaan sitä, että vain käyttöoikeuden omaavat henkilöt pääsevät selaamaan, lukemaan ja välittämään elektronista tietoa. Turvaluokituksissa määritellään etukäteen henkilöt, joilla on oikeus tietoon.

Tiedon eheydellä puolestaan tarkoitetaan sitä, että etukäteen on määritelty henkilö, joka voi muuttaa tai poistaa tietoa. Eheysvaatimuksiin kuuluvat tiedonsyöttö, tallennus, käsittely ja tiedonsiirto.

Todennuksella tarkoitetaan nimensä mukaisesti sitä, että jälkeenpäin voidaan kaikki tehdyt toimenpiteet kiistatta todentaa.

Kiistämättömyydellä varmistetaan tiedon, henkilöiden ja toimenpiteiden aitous.

Pääsynvalvonnalla varmistetaan se, että vain oikeuden omaavat henkilöt pääsevät käsiksi tietoon.

Käytettävyydellä tarkoitetaan sitä, että tieto on saatavilla ja käytettävissä käyttöoikeuden omaaville henkilöille sovittuun aikaan kaikissa olosuhteissa.

4.2 Tietoturvariskit ja uhat

Langattomiin verkkoihin kohdistuu monenlaisia uhkia. Esimerkiksi hakkerit voivat käyttää hyväkseen langattomia verkkoja hankkimalla luvattoman pääsyn sovelluksiin ja varastaa täten tietoja esimerkiksi yrityksiltä. Myös yksityisen käyttäjän tulee huolehtia langattoman verkkonsa tietoturvasta hyvin. Vuonna 2005 tapahtui ensimmäistä kertaa rikos, joka oli tehty käyttämällä naapurin suojaamatonta nettiyhteyttä. Kyseisessä tapauksessa rikoksen tehneet henkilöt ottivat yhteyden naapurinsa suojaamattomaan verkkoon ja käyttivät sitä hyväkseen tietomurron yhteydessä. Aluksi mikään ei todistanut verkon omistajan syyttömyyttä. Lopulta kuitenkin langattoman tukiaseman loki-tiedostoista saatiin todistettua, että verkkoa oli käyttänyt myös joku ulko-puolinen ja rikos selvisi. Tältäkin tapaukselta olisi vältytty, jos langattoman verkon omistaja olisi kiinnittänyt paremapaa huomiota tietoturvaan ja salannut yhteytensä asianmukaisesti. Vielä nykyäänkin valitettavan usea käyttää langatonta yhteyttään täysin salaamattomana. Esimerkiksi kerrostaloasunnoissa törmää usein langattomiin verkkoihin, joita naapuri ei ole salannut. Periaatteessa tällöin ilkikurinen käyttäjä saattaa käyttää naapurinsa verkkoa ilmaiseksi hankimatta itse Internet-yhteyttä. Hakkereiden keskuudessa on nykyään suosittu harrastus ns. *war-driving*, jossa autolla ajaen etsitään avoimia langattomia verkkoja. Erityisesti yritysten tulee olla tarkkana tietoturvan kanssa, jotta salaisia tietoja ei pystyttäisi varastamaan. Salakuuntelu on erittäin vaikeasti estettävissä ja mahdotonta havaita, joten siihen tulee varautua. /9/

Langattomiin lähiverkkoihin kohdistuvat tietoturvauhat voidaan jakaa monella eri tapaa. Monesti puhutaan aktiivisista ja passiivisista uhista. Aktiivisessa tapauksessa verkkoon tunkeutuja lähettää kohdeverkkoon dataa tai signaalia.

Passiivisessa tapauksessa puolestaan salakuunnellaan tietoliikennettä. Lisäksi murtautumisyritykset langattomaan verkkoon voidaan jakaa viiteen eri ryhmään: Fyysisiin hyökkäyksiin, imitointiin, eheyden säilyttäviin hyökkäyksiin, kuunteluhyökkäyksiin ja palvelunestohyökkäyksiin. /5/

Fyysisen hyökkäyksen tavoitteena on hankkia tietoa tietoturva-aukoista käyttäen hyväksi laitteen fyysisiä ominaisuuksia kuten hajasäteilyä. Esimerkiksi hyökkääjä saattaa ottaa haltuunsa WLAN-verkon salaisen avaimen ja pääsee tällöin käyttämään verkkoa. Hyökkääjä voi olla esimerkiksi pysäköidyssä autossa ja murtautua yrityksen tiloissa olevaan langattomaan tukiasemaan. Verkon vierasta käyttäjää on hyvin vaikea havaita. /5/

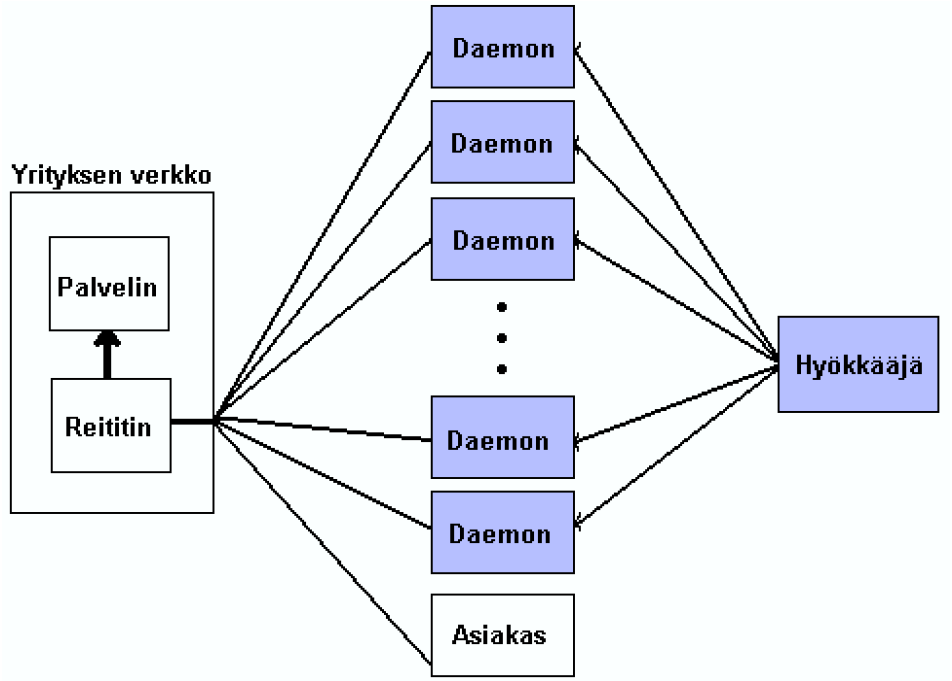
Imitoinnissa salakuunnellaan langatonta tietoliikennettä. Imitoija väittää olevansa toinen, verkkoon käyttöoikeudet omaava henkilö ja saattaa estää oikeiden käyttöoikeuksien omistavia henkilöitä pääsemästä verkkoon. /5/

Eheyden säilyttävässä hyökkäyksessä hyökkääjän tavoitteena on muuttaa langattomassa verkossa liikkuvaa tietoa omien etujensa mukaisesti niin, että muut käyttäjät eivät huomaa tätä. /5/

Kuunteluhyökkäyksessä nimensä mukaisesti salakuunnellaan langattoman verkon liikennettä. Yleensä salakuuntelun tavoitteena on saada selville tietoja, joiden avulla verkkoon pääsee murtautumaan. Salakuuntelua on mahdotonta havaita ja sitä on myös erittäin vaikea estää.

Palvelunestohyökkäksestä käytetään yleisesti lyhennettä DoS (*Denial of Service*). Palvelunestohyökkäyksissä pyritään häiritsemään langatonta verkkoa esimerkiksi kuormittamalla sitä, jos verkon liikenne kasvaa järjestelmän käytettävyys huononee. Palvelunestohyökkäys voi tukkeuttaa tai jopa kokonaan kaataa langattoman verkon. Ulkopuolisen tahon on mahdollista kuormittaa koko langattoman lähiverkon taajuusalue, koska langattomat lähiverkot toimivat vapaalla taajuusalueella. Verkko voidaan ylikuormittaa myös jatkuvilla tarpeettomilla palvelupyynnöillä. Palveluestohyökkäys saattaa aiheuttaa

suuriakin taloudellisia tappioita, esimerkiksi, jos hakkeri lamauttaa yrityksen langattoman varastonhallintajärjestelmän. Kuvassa 10 on havainnollistettu hajautettua palvelunestohyökkäystä (*DDoS, Distributed Denial of Service*), joka on edistyneempi versio normaalista palvelunestohyökkäyksestä. Hyökkäykseen osallistuu useita koneita, jotka ovat hajautettu verkon yli. Koska koneita on useita, on hyökkäys vaikeammin torjuttavissa. /1/



Kuva 10 Hajautettu palvelunestohyökkäys, DDoS /8/

4.3 Ratkaisuja tietoturvaongelmiin

Tietoturvan kehittämiseksi on kehitetty monia eri menetelmiä. Tärkeintä langattomien verkkojen tietoturvassa on se, että käyttäjä tunnistaa olemassa olevat uhat ja osaa varautua niihin oikein menetelmin. Täydelliseen tietoturvaan tuskin koskaan päästään mutta oikein menetelmin voidaan päästä riittävän hyvään tietoturvatasoon ja välttyä ikäviltä väärinkäytöiltä. Tietoturvan parantamiseksi kehitettyjä ratkaisumenetelmiä ovat esimerkiksi WEP-salaus, WPA, VPN, 802.11i-standardi ja 802.1x sekä SSID- ja MAC-tunnistus.

4.3.1 SSID-tunnistus ja MAC-osoitetunnistus

Langatonta lähiverkkoa käyttöönotettaessa tulee aina aluksi asettaa tietoturva-asetukset kuntoon. Yleensä WLAN-palvelun tarjoajalla on kattavat ohjeet tietoturva-asetuksien määrittämisille. Esimerkiksi perus kotikäyttöön otettavassa WLAN-verkossa yhteyden turvaaminen alkaa tukiaseman konfiguroinnilla. Langaton tukiasema liitetään kiinteästi verkkojohdolla tietokoneeseen. Tämän jälkeen otetaan tukiasemaan yhteyttä www-selaimen avulla, josta tukiaseman asetuksia voidaan muuttaa. Palveluntarjoajan ohjeissa on mainittu osoite, jolla tukiasemaan saadaan yhteys. Osoite on yleensä kerrottu ip-osoitteena. Uuden tukiaseman asetukset ovat yleensä ns. tehdasasetuksissa ja tarvittavat salasanat löytyvät palveluntarjoajan ohjekirjoista. Tästä syystä onkin tärkeää muistaa asettaa henkilökohtaiset salasanat, koska tehdasasetuksien salasanat ovat kaikkien saatavilla. /9/

Tukiaseman oletussalasanan jälkeen annetaan omalle langattomalle verkolle nimi, eli SSID (*Service Set Identification*). SSID-tunnistus sisältää monia heikkouksia. SSID-tunnus on paras nimetä siten, että sitä ei voida mitenkään yhdistää käyttäjäänsä tai käyttäjän osoitteeseen. Tällöin tukiaseman sijaintia on vaikeampi päätellä. Usein kuitenkin käyttäjä unohtaa vaihtaa SSID-tunnuksensa oletusasetuksista ja usein oletusasetuksena on tunnus ANY tai verkon nimeä ei ole ollenkaan nimetty eli tunnus on tyhjä. Tällöin ulkopuolisen on helppo päästä vaihtamaan tukiaseman asetuksia. SSID-tunnukset ovat määriteltävä jokaisessa yhteyspisteessä ja WLAN-asemassa erikseen. SSID-tunnus näkyy kaikille kantoalueella oleville WLAN-yhteyden omaaville päätteille, ellei se ole piilotettu. Tukiasema lähettää SSID-tunnuksen majakkasanomissa ja liittymissanomat sisältävät tunnuksen selväkielisenä, ellei käytetä salausta. /6, s. 72-73; 9/

Kaikilla verkkokorttisilla tietokoneilla on olemassa oma yksilöllinen MAC-osoite (*Media Access Control*). MAC-osoitteen avulla laite tunnistetaan verkossa. MAC-osoitetunnistus kehitettiin korvaamaan SSID-tunnistuksen puutteita. Tunnistuksessa tukiasema määrittelee listan niiden työasemien MAC-

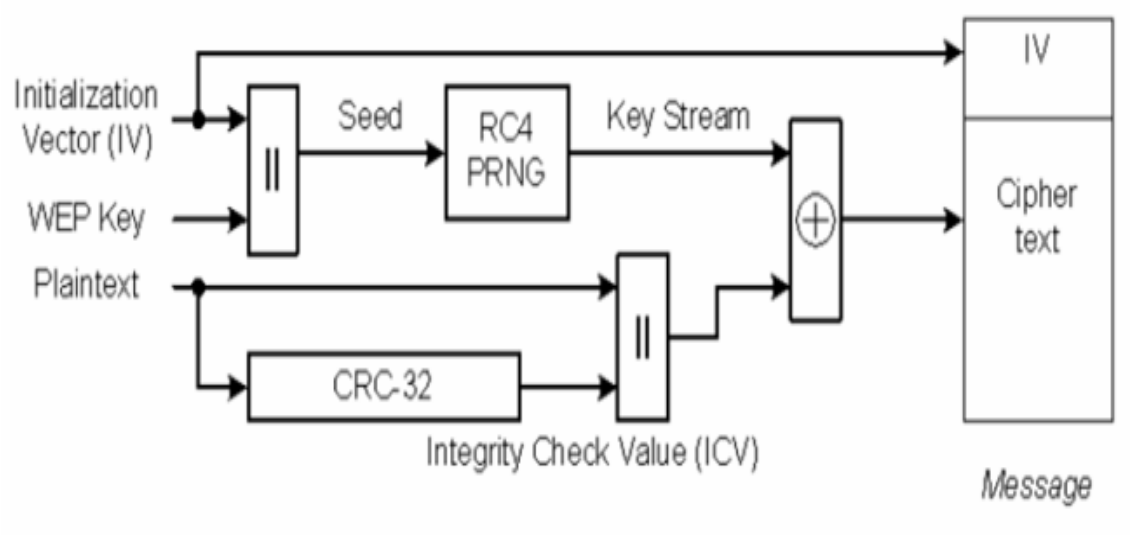
osoitteista, joilla on lupa liittyä verkkoon. MAC-osoitetunnistusta käytetään pääosin kotiverkoisssa, jolloin verkon ylläpitäjä syöttää kaikkien haluamiensa verkkolaitteiden MAC-osoitteet langattoman tukiaseman osoitelistaan. Suodatuksen ollessa päällä pääsevät vain osoitelistasta löytyvät päätteet ottamaan yhteyden tukiasemaan. Pelkkä MAC-suodatus ei kuitenkaan tee verkkoa turvalliseksi, koska MAC-osoite pystytään väärentämään ja se on muutettavissa. /6, s.73; 9/

4.3.2 WEP-salaus

Kun salasanat on saatu asetettua ja verkko piilotettua, tulee keskittyä tietoliikenteen varsinaiseen salaukseen eli kryptaukseen. WEP-salaus (*Wired Equivalence Privacy*) on ensimmäinen salausmenetelmä, jota langattomien verkkojen salauksessa on käytetty. WEP-salauksen tavoitteena on suojata verkkoa salakuuntelulta ja estää asiattomien pääsy verkkoon. WEP-salaus toimii vain 802.11-standardeissa ja sitä käytetään usein rinnakkain MAC-osoitetunnistuksen kanssa. Nykyään WEP-salaus on jo hieman vanhentunut järjestelmä, mutta kuitenkin sitä esiintyy vielä käytössä. WEP-salaus tarjoaa perusturvaa, mutta salaus on kuitenkin melko helposti murrettavissa salauksesta löytyneiden aukkojen vuoksi. Uudempi WPA-salaus (*Wireless Fidelity Protected Access*) on nykyään lähes kokonaan korvannut WEP-salauksen. WEP-salausta suositellaankin käytettävän vain silloin kun langaton tukiasema ei ole WPA-yhteensopiva.

WEP-salaus sisältää salausalgoritmin, jaetun salaisen avaimen ja alustusvektorin, IV (*Initilization Vector*). WEP käyttää salauksessaan symmetristä jonoalgoritmiä RC4, jonka käytössä on havaittu puutteita. Lisäksi WEP-salauksen haittapuolena ovat lyhyt alustusvektori, joka lähetetään salaamattomana jokaisen kehyksen alussa. Alustusvektorin pituus on 24 bittiä, joka mahdollistaa noin 17 miljoonan erilaisen bittijonon käytön. Salausavain on pituudeltaan 64 tai 128 bittiä, mutta käytännössä siitä vähennetään alustusvektorin pituus. Yksi WEP-salauksen haittapuolista on se, että salausavain on koko verkolle sama. Kuvassa 11 on havainnollistettu WEP-salauksen logiikkaa. Salainen avain saadaan, kun se XOR:ataan alustusvektorin

kanssa. Salattua avainta käytetään puolestaan syötteenä random-luku generaattorille, joka luo istuntoavaimen. Salattu viesti saadaan puolestaan, kun istuntoavain XOR:ataan varsinaisen viestin kanssa. Vastaanottava tukiasema purkaa salauksen. Salaus toimii vain 802.11-laitteiden välillä, kun kehys siirtyy langallisen verkon puolelle ei salaus enää toimi. Mikäli tukiasema vastaanottaa datan, jota ei ole salattu asian mukaisella tavalla, data häviää eikä sitä toimiteta kohteeseensa. /1, s.181; 6, s.74; 4/



Kuva 11 WEP-salauksen logiikka /21/

Nykyään hakkerit purkavat WEP-salauksen helposti ja sitä pidetäänkin melko alkeellisena. WEP-salaukseen on kehitelty parempia versioita esimerkiksi TKIP (*Temporal Key Integrity Protocol*) ja WEPplus- tekniikka, joissa tietoturva-aukkoja on pyritty paikkaamaan. Tänäpäivänä WEP-tekniikan ongelmien takia kehitetty WPA-salaustekniikka on syrjäyttämässä WEP-salauksen.

4.3.3 WPA-salaus

Wi-Fi järjestön kehittämä WPA-salaus (*Wireless Fidelity Protected Access*) on huomattavasti tehokkaampi kuin, WEP-salaus, siinä vaihdellaan jatkuvasti salausavainta ja paketttikohtaiset salausavaimet ovat käytössä. Tämä tekee salauksen murtamisen vaikeammaksi. WPA:n huonona puolena on kuitenkin sen alttius palvelunestohyökkäyksille. WPA-salaus on yleinen standardi, joka tarjoaa kaksisuuntaisen todennuksen. Nykyisin useimmat laitteiden valmistajat

tukevat WPA-standardia. WPA-standardi tarjoaa tietoturvaa sekä koteihin, että suuryrityksiin. WPA-standardista on olemassa eri versioita, kuten WPA-PSK (*Pre-Shared Key*) ja WPA. Lisäksi on uusi WPA2-standardi, joka tunnetaan myös 802.11i-standardina. /1, s.184/

WPA-standardissa on käytössä TKIP-kryptaus (*Temporal Key Integrity Protocol*) tai AES-kryptaus (*Advanced Encryption Standard*). Näistä kahdesta AES-kryptaus on uudempi ja kehittyneempi. AES-kryptausta käytetään uudessa WPA2-standardissa ja siitä enemmän kappaleessa 4.3.5. TKIP on algoritmijoukko, joka sisältää parannuksia WEP-salauksen tietoturvaan. TKIP-kryptaus käyttää myös RC4-algoritmiä ja sisältää 128-bittisen pakettikohtaisen salausavaimen ja laajennetun 48-bitin alustustusvektorin. TKIP-protokollassa on korjattu WEP-salauksessa esiintyneet tietoturvaongelmat. Salausavainta vaihdellaan n. 10 000:nen paketin välein ja vaihto tapahtuu dynaamisesti. TKIP-protokolla sisältää myös sanoman eheyden tarkistamisen eli MIC:n (*Message Integrity Check*), joka paljastaa datan väärennysyritykset. MIC laskee MAC-otsikosta, sekvenssinumerosta, hyötykuormasta ja siemenluvusta 64-bitin sormenjäljen. Kehykset hylätään, jos vastaanotettu MIC-sormenjälki ei täsmää. /6, s.82-83; 17; 24/

Liitteessä 1 on esitelty TKIP-kehys. Salaus aloitetaan yhdistämällä 128-bittinen aloitusavain, työaseman MAC-osoite ja kehyksen järjestysnumeron neljä eniten merkitsevää bittiä. Tämän jälkeen saadaan väliaikainen avain. Kun järjestynumeron kaksi alinta bittiä yhdistetään väliaikaisen avaimen kanssa, saadaan kehyskohtainen avain. Avain vaihtuu jokaiselle lähetetylle kehykselle ja jokainen asema käyttää eri salausavainta. Myös alustusvektorit (*IV*) salataan. TKIP-kehyksen lopussa on ICV-tiiviste (Integrity Check Value) ja FCS (Frame Check Sequence). ICV turvaa kehyksen eheyden ja FCS on virheenhavaitsemistoteutus. /6, s.82-83; 17; 24/

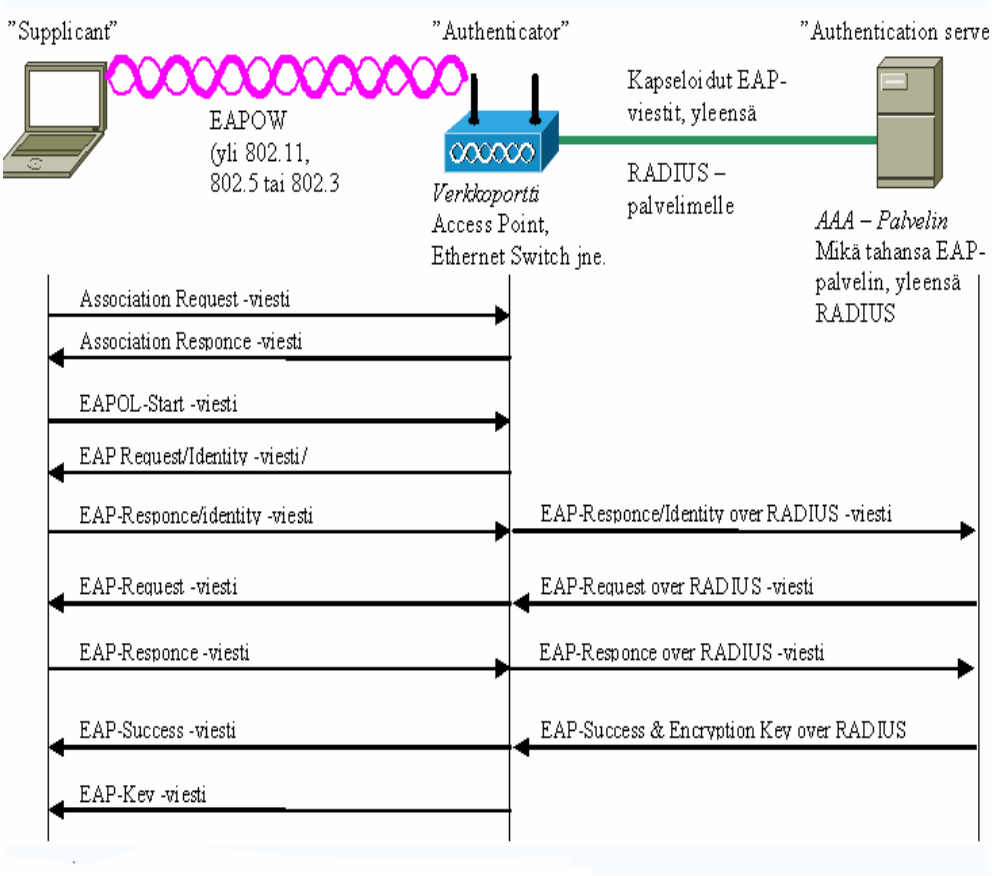
WPA:ssa on mahdollista käyttää kahta eri kirjautumismenetelmää: WPA ja WPA-PSK. Näistä jälkimmäinen soveltuu parhaiten kotikäyttöön tai pienyrityksiin. Siinä määritellään yhteinen perussalausavain (*Pre Shared Key*)

jokaiselle tukiasemaan yhteydessä olevalle tietokoneelle. Tukiasema käyttää perussalausavainta, joka annetaan tukiasemalle ja kaikille siihen liitetyille koneille, koneiden tunnistamiseen. Tietokone ei saa yhteyttä tukiasemaan, jos sille ei ole määritelty perussalausavainta. Varsinaiset verkon datapaketit salataan jatkuvasti vaihtuvalla salausavaimella. Tukiasemaan kirjaudutaan salasanaa käyttämällä, jonka jälkeen yhteys käyttäjän ja tukiaseman välillä on suojattu. /17/

Tavallinen WPA on puolestaan tarkoitettu järeämpiin keskitettyihin ratkaisuihin ja sitä käytettäessä salausavain haetaan erilliseltä RADIUS-palvelimelta. Tämä ratkaisu on kuitenkin hyvin kallis.

4.3.4 802.1x

802.1x-standardi julkaistiin vuonna 2001. Sen tarkoituksena on estää luvattoman laitteen kommunikointi lähiverkon liityntäpisteen kautta sekä langallisissa, että langattomissa verkoissa. 802.1x perustuu EAP-protokollaan (*Extensible Authentication Protocol*). EAP on konsepti käyttäjän ja laitteen tunnistukseen, se tukee useita todennusmenetelmiä, kuten Kerberos, token card-tunnistus, kertakäyttöisiä salasanoja, varmenteita ja julkisen avaimen todennusta. EAP koostuu päätelaitteen Supplicant-ohjelmasta, verkon reunalla olevasta tunnistajasta (*Authenticator*) ja tunnistuspalvelimesta. Tunnistuspalvelimelle on tallennettu käyttäjätilit ja salasanatiedot. /6, s. 75-76; 1, s. 188; 26/



Kuva 12 802.1x autentikointi /26/

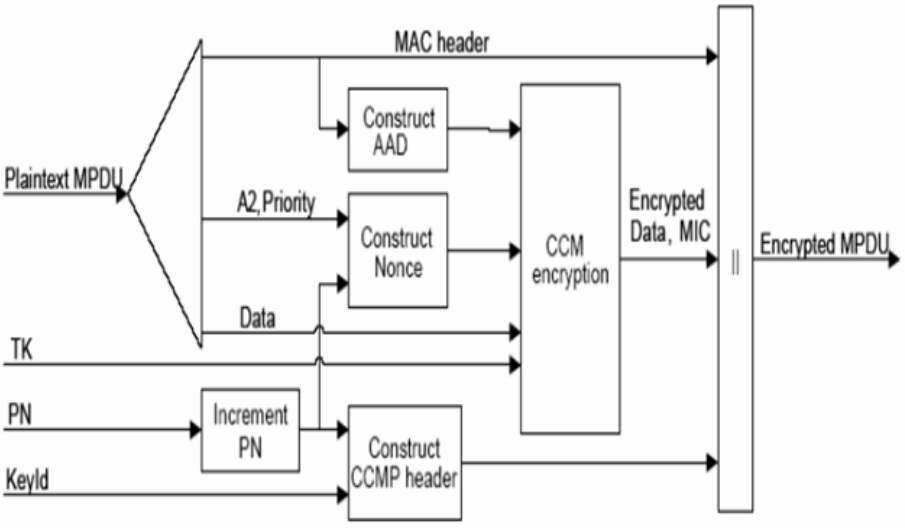
Kuvassa 12 on havainnollistettu 802.1x autentikointia. 802.1x-liikenne käynnistyy, kun todentamaton langaton asiakaslaite, supplicant, yrittää muodostaa yhteyden tukiasemaan, authenticatoriin. Tämän jälkeen tukiasema vastaa avaamalla verkkoportin, jossa sallitaan vain asiakkaalta todennuspalvelimelle kulkevat EAP-paketit, tukiasema estää kaiken muun liikenteen. Asiakkaan lähettämä Start-viesti käynnistää sarjan viestin vaihtoja asiakkaan todentamiseksi. Autentikointi tapahtuu todennuspalvelimen avulla, joka on yleensä RADIUS-palvelin. Asiakkaan tunnistamisen jälkeen avaa tukiasema portin muunkin tyyppiselle liikenteelle. /1, s. 188-189/

4.3.5 802.11i

IEEE 802.11i-standardi eli WPA2 ratifioitiin kesäkuussa 2004 ja se käyttää AES-kryptausta. Myös WPA2:sta on olemassa kotikäyttöön tarkoitettu WPA2-PSK versio. AES:n (*Advanced Encryption Standard*) käyttämä Rijndael-

algoritmi on uudempi ja tehokkaampi salausalgoritmi, kuin TKIP:n käyttämä RC4-algoritmi. AES vaatiikin tehokaampia prosessoreja ja sillä toteutettu salaus on vaikea murtaa. Tietokoneen ja tukiaseman välinen liikenne salataan parittaisella lähetysavaimella, jota vaihdellaan määräajoin turvallisesti. Lisäksi työasemiin ja tunnistuspalvelimeen määritellään yleisavain (*Master Key*), jonka perusteella muut tarvittavat avaimet määritellään. AES-salauksella toteutetaan CCMP-lohkosalaus (*Counter Mode Encryption*), liitteessä 2 on esitelty CCMP-MPDU. 802.11i pystyy käyttämään 128-, 192- ja 256 bittisiä salausavaimia. /6, s.84; 25/

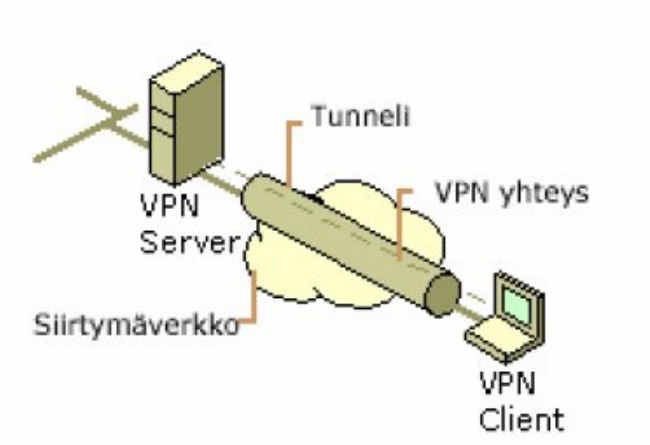
Autentikointi muodostuu 802.11i-standardissa ns. ”kättelyistä”, joissa vaihdetaan yhteinen salaisuus. Yhteistä salaisuutta käytetään lopulliseen salaukseen. Yhteisestä yleisavaimesta generoidaan parittainen yleisavain, PMK (*Pairwise Master Key*). Tunnistuspalvelin lähettää PMK:n yhteyspisteelle, joka generoi PMK:sta ja omasta yksittäisestä bittijonostaan parittaisen tilapäisavaimen, PTK (*Pairwise Transient Key*). PTK puolestaan lähetetään yhteyspisteelle PMK:lla salattuna. Viestinvaihto kuitataan nelinkertaisella kättelyllä ja MIC-otsikko varmistaa sanomien eheyden. Avaintenvaihdon vahvistusavain, salausavain ja tilapäisavain, TK (*Temporar Key*), lasketaan PTK-avaimesta. Datan salaukseen käytetään tilapäisavainta. 802.11i-standardia käytetään yleensä 802.1x-järjestelmissä. Jotta 802.11i olisi turvallinen, tulee 802.1x:n luotettavuus taata. /6, s.84; 21/



Kuva 13 CCMP-salaus /21/

4.3.6 VPN-salaus

VPN (*Virtual Private Network*) on niin sanottu virtuaalinen verkko, jolla voidaan esimerkiksi muodostaa etätyöasemalla yhteys yrityksen tai koulun verkkoon Internetin kautta. Tässä tapauksessa on kyseessä Point to Point-yhteys, jossa etätyöasema on ns. *VPN Client* ja yrityksen palvelin on ns. *VPN Server*. VPN-ratkaisut luovat siis turvallisemman yhteyden, kun käyttäjät liikkuvat julkisilla alueilla.



Kuva 14 VPN-elementit /22/

Toimiakseen VPN-verkkossa tulee olla seuraavat 7 elementtiä: VPN-palvelin (*VPN Server*), VPN-asiakas (*VPN Client*), tunneli, VPN-yhteys, tunnelin rakentamisen protokollat, tunneloitava data ja siirtymä verkko. Kuvassa 14 on esitelty nämä VPN-elementit. VPN-palvelimena toimii tietokone, joka käsittelee ja hyväksyy yhteydenotot. VPN-asiakas on puolestaan tietokone, jolla luodaan yhteys VPN-palvelimeen. Data puolestaan kapsuloidaan tunnelissa ja VPN-yhteys salaa sen. Siirtymäverkkona voi toimia esimerkiksi Internet. /22; 6, s. 85/

VPN:ssä käytetään seuraavia salausprotokollia: Ipsec-protokolla, L2TP-tunnelointiprotokolla, L2F-tunnelointiprotokollaa ja PPTP. Ipsec-protokollaa käytetään sekä etäkäyttöön, että lähiverkkojen yhdistämiseen. L2TP-tunnelointi-protokollaa käytetään puolestaan pelkästään etäkäyttöön, salaus tapahtuu kuitenkin Ipsec-protokollan avulla. L2F-protokollaa käytetään vain lähiverkkojen yhdistämiseen. PPTP on puolestaan Microsoftin oma etäkäyttö-protokolla. /28/

5 WLAN EATON POWER QUALITY OY:SSÄ

Espoon Koskelossa sijaitseva Eaton Power Quality Oy kuuluu kansainväliseen Eaton-konserniin, jonka pääkonttori sijaitsee Yhdysvaltojen Raleighissa. Eaton on maailman johtava toimittaja sähkön laatuun ja sen hallintaan liityvissä kokonaisratkaisuissa. Espoon yksikössä valmistetaan eri teholuokkaisia UPS-laitteita (*Uninterruptible Power Supply*), joiden tehtävänä on taata tasainen virransyöttö lyhyissä sähkökatkoksissa ja syöttöjännitteen epätasaisuuksissa. Myös langattomien lähiverkkojen sähkönsyötöstä huolehditaan usein UPS-laitteilla. Espoon yksikössä työskentelee noin 250 henkilöä. /12/

Kuva 15 Eaton Power Quality Oy:n tehdasrakennus Espoossa /12/

Espoon tehtaassa on koko tehdasrakennuksen kattava langaton lähiverkko. Langaton lähiverkko otettiin käyttöön vuosituhannen vaihteessa. Tällä hetkellä yrityksessä on käytössä kahta eri standardia. Vanhemmat tukiasemat tukevat 802.11b-standardia ja uudemmat standardia 802.11g. Verkon nopeus on 54 Mbit/s. Tukiasemia tehdasrakennuksessa on yhteensä 10 ja päätelaiteita noin 100. Tukiasemat on jaoteltu ympäri tehdasta siten, että niille tulisi mahdollisimman tasainen kuormitus. Uudemmat tukiasemat ovat CISCO-merkkisiä. /10/

Eatonin tehtailla on käytössä yhteinen tietoturvastandardi. Tällä hetkellä on käytössä WEP-salaustekniikka 128-bittisellä salausavaimella, mutta uudempaan salaustekniikkaan ollaan siirtymässä lähitulevaisuudessa. /10/

6 YHTEENVETO

Tässä insinöörityössä käsiteltiin langattomia lähiverkkoja. Luvussa 2 keskityttiin tarkastelemaan tyyppillisimpiä WLAN:lle ratifioituja standardeja. 802.11-standardiperheeseen kuuluvat eri versiot ovat yleisimmin käytettyjä WLAN-standardeja. Tämän hetken käytetyin standardi on 802.11g, mutta jo vuoden 2007 loppupuolella tulee markkinoille uusi ja nopeampi standardi 802.11n. Muita esiteltyjä standardeja ovat HiperLAN-standardit, bluetooth-standardi ja WiMAX.

Luvussa 3 valotettiin lukijalle langattomien lähiverkkojen käyttämää tekniikkaa. Tarkemmin perehdyttiin WLAN-verkkojen hajaspektritekniikoihin, modulointimenetelmiin sekä verkkotopologioihin. Langattomien lähiverkkojen tietoturvallisuutta käsiteltiin luvussa 4. Kyseisessä luvussa keskityttiin esittelemään langattomien lähiverkkojen tietoturvapuutteita ja esittämään niihin parannusehdotuksia. Insinöörityön luettuaan tulisi lukijalla olla paremmat edellytykset rakentaa itselleen turvallinen langaton lähiverkko. Luvussa 5 esiteltiin lyhyesti Espoossa sijaisevan elektroniikka-alan yrityksen Eaton Power Quality Oy:n langaton lähiverkko.

WLAN:in tulevaisuus näyttää hyvältä. Tällä hetkellä ympäri maailmaa rakennetaan runsaasti langattomia lähiverkkoja. Tavoitteena on luoda aluksi koko kaupungin kattavia ja sen jälkeen koko maan kattavia langattomia verkkoja. Luvussa 2.5 on esitelty espanjalaisen yrityksen Fonin ideaa koko maailman kattavasta langattomasta verkosta. Tällä hetkellä Suomessa Digita ja Siemens Oy rakentavat yhteistyössä koko Suomen kattavaa langatonta verkkoa. Tavoitteena on, että verkko toimii koko Suomessa vuoden 2009 lopussa. Kyseessä olisi ensimmäinen koko maan kattava langaton verkko koko maailmassa. Eurooppalaisiin kaupunkeihin rakennettaviin kaupunkiverkkoihin arvioidaan käytettävän rahaa jopa yli 100 miljoonaa euroa lähivuosina.

LÄHDELUETTELO

Painetut lähteet

1 Geier, Jim, Langattomat verkot. IT Press. Helsinki 2005. 236 s.

2 Granlund, Kaj, Langaton tiedonsiirto (1. painos). Docendo Finland Oy. Porvoo 2001.

3 Helin, Ari – Karttunen, Jussi – Pitkänen, Jussi, WLAN ja tietoturva. Seminaarityö. Turun kauppakorkeakoulu. Turku 2002. 26 s.

4 Lehtonen, Satu, Turvallisuuden hallinta langattomissa lähiverkoissa. Diplomityö. Helsingin teknillinen korkeakoulu. Tietotekniikan osasto. Helsinki 2004. 92 s.

5 Niemi, Juha, WLAN-turvallisuus. Seminaarityö. Helsingin yliopisto. Tietojenkäsittelytieteen laitos. Helsinki 2003. 16 s.

6 Puska, Matti, Langattomat lähiverkot. Talentum Media Oy. Jyväskylä 2005. 294 s.

7 Saksa, Markku, Espanjalainen Fon rakentaa maailmaan langatonta verkkoa. Helsingin Sanomat 17.3.2006, s. B13.

8 Silander, Tea, Langattomien laitteiden tietoturva. Aine. Helsingin yliopisto. Tietojenkäsittelytieteen laitos. Helsinki 2003. 15 s.

9 Tuurala, Antti, Salaa aaltosi, Mikrobitti 2/2006, s. 91-93.

Painamattomat lähteet

10 Riiheläinen, Markku, IT Specialist. Haastattelu 22.12.2006. Eaton Power Quality Oy.

Sähköiset lähteet

11 Bazoge. [www-sivu]. [viitattu 13.10.2006] Saatavissa: http://bazoge.scn.infovx.net/fi/FHSS

12 Eaton Power Quality Oy. [www-sivu]. [viitattu 8.1.2007] Saatavissa: http://www.powerware.com/Suomi/

13 Jaaranen, Markku. [www-sivu]. [viitattu 18.5.2006] Saatavissa: http://www.cs.joensuu.fi/~mjaarane/laudaturseminaari/seminaari.html#3

14 Juutilainen, Matti. [www-sivu]. [viitattu 22.5.2006] Saatavissa: http://www.it.lut.fi/kurssit/03-04/010651000/luennot/wlan.pdf

15 Lehto, Tero. Tietokone. [www-sivu]. [viitattu 18.4.2006] Saatavissa: http://www.tietokone.fi/uutta/uutinen.asp?news_id=26166&tyyppi=1

16 Lehto, Tero. Tietokone. [www-sivu]. [viitattu 6.12.2006] Saatavissa: http://www.tietokone.fi/uutta/uutinen.asp?news_id=28951&tyyppi=1

17 MV-net. [www-sivu]. [viitattu 2.12.2006] Saatavissa: http://www.mvnet.fi/index.php?osio=Tietokoneet&sivu=Langaton_kotiverkko#salaukset

18 Ojanperä, Veijo. Tietokone. [www-sivu]. [viitattu 4.12.2006] Saatavissa: http://www.tietokone.fi/uutta/uutinen.asp?news_id=28895&tyyppi=1

19 Plaza. [www-sivu]. [viitattu 6.4.2006] Saatavissa: http://www.soneraplaza.fi/tietokoneet/artikkeli/0,2998,h-9093_a-142588,00.html

20 Speth, Michael. [www-sivu]. [viitattu 22.10.2006] Saatavissa: http://www.iss.rwth-aachen.de/Projekte/Theo/OFDM/www_ofdm.html

21 Taavila, Erik. [www-sivu]. [viitattu 24.11.2006] Saatavissa: http://www.it.lut.fi/kurssit/04-05/010626000/seminaarit/Taavila_WLAN_Security.ppt#7

22 Tietoverkot-opas. [www-sivu]. [viitattu 22.11.2006] Saatavissa: http://www.2kmediat.com/vpn/elementit.asp

23 Wikipedia. [www-sivu]. [viitattu 12.4.2006] Saatavissa: http://fi.wikipedia.org/wiki/IEEE_802.11#802.11

24 Wikipedia. [www-sivu]. [viitattu 12.11.2006] Saatavissa: http://fi.wikipedia.org/wiki/Langattoman_l%C3%A4hiverkon_tietoturva

25 Wikipedia. [www-sivu]. [viitattu 15.11.2006] Saatavissa: http://fi.wikipedia.org/wiki/802.11i

26 Wikipedia. [www-sivu]. [viitattu 19.11.2006] Saatavissa: http://fi.wikipedia.org/wiki/802.1x

27 Wikipedia. [www-sivu]. [viitattu 2.10.2006] Saatavissa: http://fi.wikipedia.org/wiki/FSK

28 Wikipedia. [www-sivu]. [viitattu 24.11.2006] Saatavissa: http://fi.wikipedia.org/wiki/VPN#VPN-markkinat

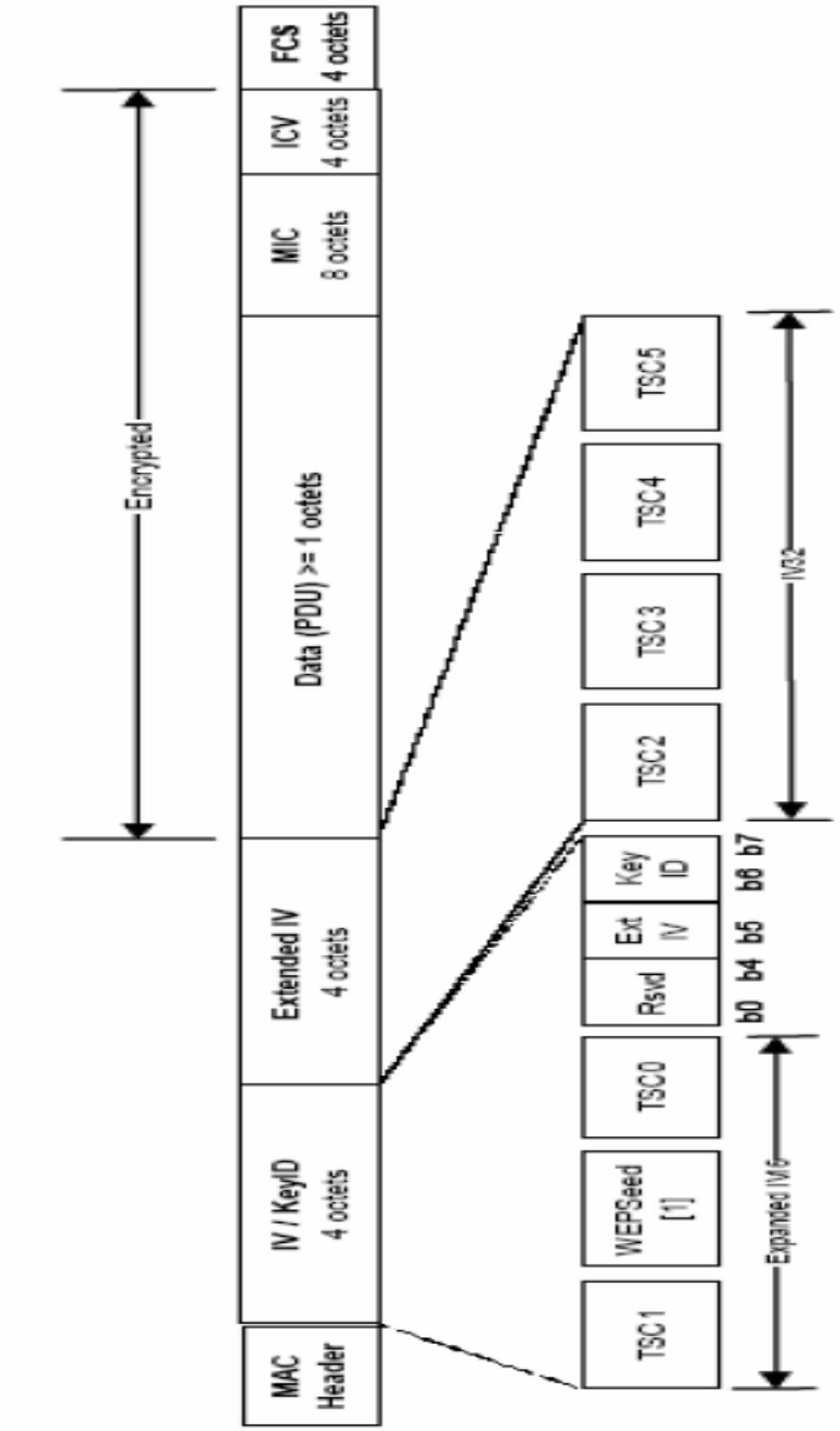
29 Wikipedia. [www-sivu]. [viitattu 28.11.2006] Saatavissa: http://fi.wikipedia.org/wiki/HiperLAN

30 Wikipedia. [www-sivu]. [viitattu 28.11.2006] Saatavissa: http://fi.wikipedia.org/wiki/WiMAX

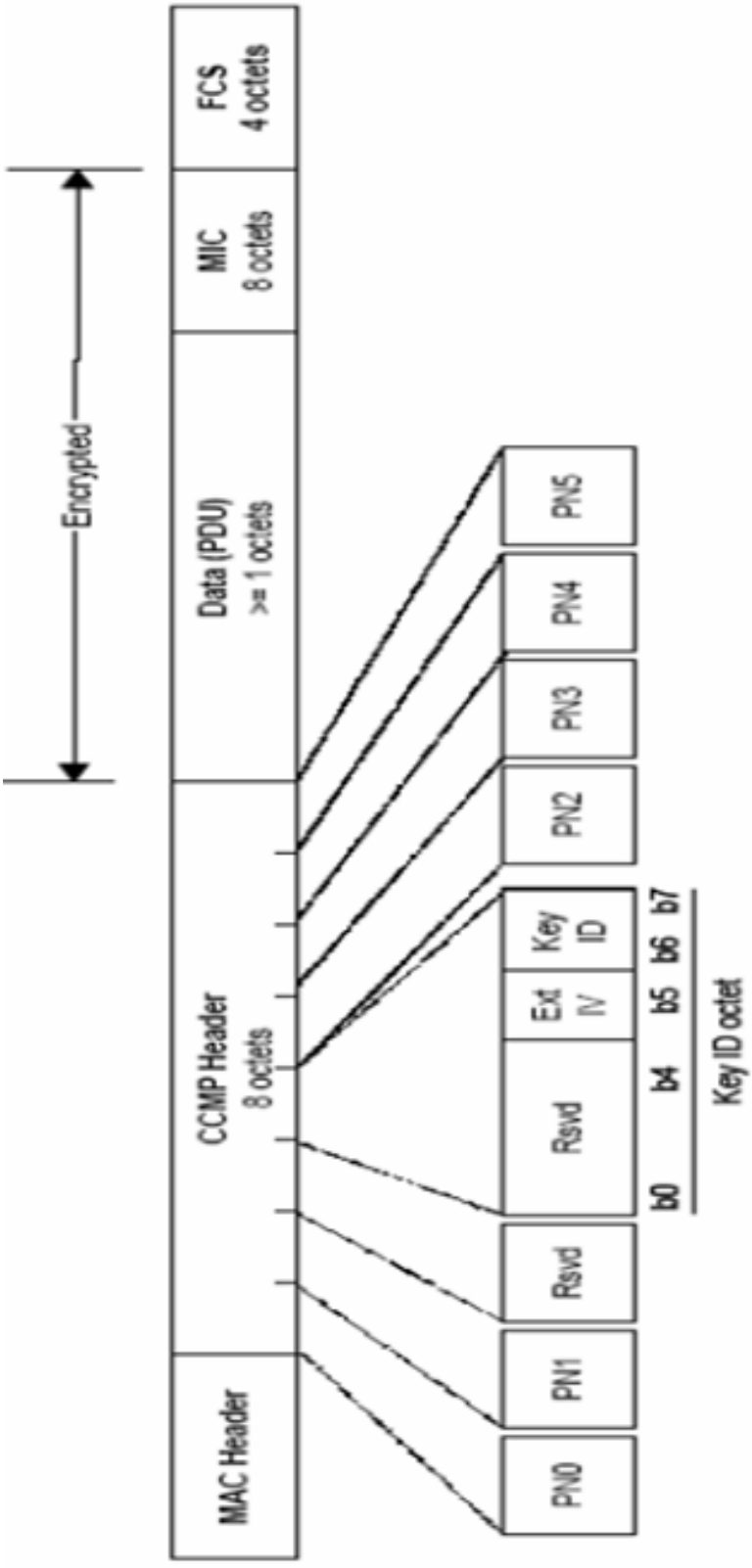
31 Wikipedia. [www-sivu]. [viitattu 2.4.2006] Saatavissa: http://fi.wikipedia.org/wiki/IEEE

32 Wikipedia. [www-sivu]. [viitattu 2.10.2006] Saatavissa: http://fi.wikipedia.org/wiki/FHSS

33 Wikipedia. [www-sivu]. [viitattu 4.4.2006] Saatavissa: http://fi.wikipedia.org/wiki/OSI-malli



TKIP-kehys /21/


Encrypted
MAC Header
CCMP Header
8 octets
Data (PDU)
>= 1 octets
MIC
8 octets
FCS
4 octets
PN0
PN1
Rsvd
Rsvd
Ext IV
Key ID
PN2
PN3
PN4
PN5
b0
b4
b5
b6
b7
Key ID octet

CCMP-MPDU /21/