TAMKIN LANGATTOMAN LÄHIVERKON UUDISTAMINEN

Mikko Uusitalo

Opinnäytetyö
Huhtikuu 2012
Tietotekniikka
Tietoliikennetekniikka
ja tietoverkot

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikka
Tietoliikennetekniikka ja tietoverkot

UUSITALO MIKKO:
TAMKin langattoman lähiverkon uudistaminen

Opinnäytetyö 50 sivua, josta liitteitä 4 sivua
Huhtikuu 2012

Kannettavat tietokoneet, älypuhelimet ja tablet-tietokoneet ovat yleistyneet viime vuosina huomattavasti. Niiden ominaisuuksien kokonaisvaltainen hyödyntäminen vaatii yhteyden Internetiin. Yhteys saadaan esimerkiksi koulussa tai kahvilassa langattoman lähiverkon (WLAN) kautta. Myös koulujen luokkaympäristöt ja opetustavat ovat muuttuneet, sillä nykyään yhä useammat voivat tehdä esimerkiksi luentomuistiinpanonsa kannettavalla tietokoneella. Tulevaisuudessa opiskelijoiden omia laitteita voidaan hyödyntää entistä enemmän esimerkiksi konseptissa, jossa koulu tarjoaa opetuksen kannalta välttämättömät ohjelmat ja verkkoyhteyden opiskelijan kannettavalle tietokoneelle.

Tampereen ammattikorkeakoulussa päätettiin uudistaa langaton lähiverkko, johon henkilökunta, opiskelijat ja vierailijat pääsevät. Käytössä oli kaksi erilaista järjestelmää, jotka eivät enää pystyneet tarjoamaan riittävää palvelun laatua. Suurinta osaa tukiasemista ei pystytty hallitsemaan keskitetysti, ja niitä oli alkanut rikkoontua ikääntymisen takia. Lisäksi vierailijaverkkoon yhdistäminen koettiin vaikeaksi, ja sitä oli mahdollista käyttää vain osassa toimipisteitä.

Syksyllä 2011 käyttöön otettiin uusinta tekniikkaa tukeva WLAN-järjestelmä, jota hallitaan keskitetysti. Järjestelmän toiminta perustuu WLAN-kontrolleriin, joka automaattisesti valvoo verkon tilaa ja osaa mukautua mahdollisiin häiriöihin. Tukiasemissa käytetään valmistajan erityistä BeamFlex-tekniikkaa, joka muokkaa antennien suuntakuviota kuuluvuuden ja tiedonsiirtonopeuden parantamiseksi. Koko langaton verkko rakennettiin alusta asti uudelleen, ja tukiasemien paikat valittiin mittausten perusteella. Käyttäjille alettiin myös tarjota salaamatonta langatonta vierailijaverkkoa, johon kirjaudutaan selaimella.

Tukiasemien määrän kasvattaminen ja uusi tekniikka mahdollistivat WLAN-verkon peittoalueen laajentamisen kaikissa toimipisteissä. Uuden vierailijaverkon myötä käyttäjämäärä kasvoi huomattavasti. Myös WLAN-järjestelmän ylläpito helpottui, sillä nyt sitä hallitaan ja valvotaan yhden käyttöliittymän kautta. Tulevaisuudessa on mahdollista alkaa tarjota henkilökunnalle niin sanottua WLAN-sisäverkkoa, johon pääsee koulun omistamilla laitteilla. Vastaavanlaista on jo kokeiltu muutamassa laboratorioluokassa. Vierailijaverkon salaamattomuus voi olla joillekin ongelma, joten sen rinnalla henkilökunnalle ja opiskelijoille tarjotaan myös salattua verkkoa.

Asiasanat: langaton lähiverkko, wlan, adaptiivinen antenni, keilanmuodostus

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
ICT Engineering
Telecommunication and Networks

UUSITALO MIKKO:
Modernization of wireless local area network at TAMK

Bachelor's thesis 50 pages, appendices 4 pages
April 2012

Tampere University of Applied Sciences (TAMK) decided to modernize its wireless local area network (WLAN), which is available for staff, students and guests. There were two different and independent systems, which could not provide the needed quality of service anymore. Also the old wireless guest network was found to be difficult to use.

To improve the situation, a brand new WLAN system was installed. It is based on a WLAN controller, which automatically controls and monitors the network and allows centralized settings deployment. Also the BeamFlex technology in the access points dynamically adjusts radiation pattern to provide more coverage and throughput. In addition to the new equipment, TAMK started to provide unencrypted guest network, which uses browser based authentication.

By increasing the number of access points and using latest techniques, coverage area of the wireless network was expanded in all campuses. As the wireless network became more user friendly, daily user volumes increased significantly. Centralized management made administration of the network easier. There may be some concern about the unencrypted network, so TAMK provides encrypted alternative for students and staff.

Keywords: wireless local area network, wlan, adaptive antenna, beamforming

SISÄLLYS

LYHENTEET JA TERMIT

3G/4G	yleisnimitys kolmannen/neljännen sukupolven matkapuhelinteknologioille
AES	Advanced Encryption Standard, salausmenetelmä
BeamFlex	Ruckus Wirelessin adaptiivinen antenniteknologia
CCK	Complementary Code Keying, modulaatiotekniikka
CCMP	Counter Mode with Cipher Block Chaining Messages Authentication Protocol, salausprotokolla siirrettävän tiedon suojaamiseen
CDMA	Code Division Multiple Access, koodijakokanavointi, jossa jokaiselle käyttäjälle määritetään oma modulaatiokoodi
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance, WLAN-verkon vuoronvaraustekniikka
DHCP	Dynamic Host Control Protocol, IP-asetukset verkon laitteille automaattisesti jakava protokolla
DSL	Digital Subscriber Line, puhelinlinjoja hyödyntävä laajakaistainen Internet-yhteystekniikka
DSSS	Direct Sequence Spread Spectrum, hajaspektritekniikka, jossa jokainen alkuperäisen signaalin bitti esitetään usealla bitillä
DVB	Digital Video Broadcasting, digitaalinen televisiolähetys
EAP	Extensible Authentication Protocol, todennusprotokollan runko
FDM	Frequency Division Multiplexing, taajuuskanavointi, jossa jokaiselle signaalille on oma taajuuskaistansa
FHSS	Frequency-Hopping Spread Spectrum, hajaspektritekniikka, jossa taajuutta vaihdetaan tasaisin väliajoin
IEEE	Institute of Electrical and Electronics Engineer, kansainvälinen tekniikan alan järjestö, joka muun muassa määrittelee standardeja
IP	Internet Protocol, tietoliikennepakettien siirtämisestä huolehtiva protokolla
ISO	International Organization for Standardization, kansainvälinen standardoimisjärjestö
ITU	International Telecommunication Union, kansainvälinen televiestintäliitto
LDAP	Lightweight Diretory Access Protocol, hakemistopalveluprotokolla
LED	Light-emitting diode, valodiodi
LTE	Long Term Evolution, 3G-matkapuhelinteknologia, jossa tiedonsiirron nopeuksia on kasvatettu ja viiveitä lyhennetty aiempiin verrattuna

MAC	Media Access Control, verkon varauksen ja liikennöinnin hoitava järjestelmä
MIMO	Multiple-In/Multiple-Out, tekniikka, jossa sekä lähetykseen että vastaanottoon käytetään samanaikaisesti useampaa kuin yhtä antennia
OFDM	Orthogonal Frequency-Division Multiplexing, taajuuskanavointi, jossa tietoa siirretään useilla taajuuskanavilla samaan aikaan
OFDMA	Orthogonal Frequency-Division Multiple Access, kuin edellä, mutta siirtotietä voi samaan aikaan käyttää useampi kuin yksi käyttäjä
PoE	Power over Ethernet, tekniikka, jolla voidaan syöttää sähkövirta parikaapelia pitkin verkkolaitteelle
PSK	Pre-Shared Key, esijaettu avain, jota käytetään käyttäjien tunnistukseen ja liikenteen salaukseen
RADIUS	Remote Authentication Dial In User Service, käyttäjien tunnistamiseen käytetty protokolla
RF	Radio Frequency, radiotaajuuskaista, 3 kHz - 300 GHz
RFID	Radio Frequency IDentification, radiotaajuuksia käyttävä etätunnistus
SNR, S/N	Signal-to-noise ratio, signaali-kohinasuhde
SSID	Service Set IDentifier, WLAN-verkon käyttäjälle näkyvä tunnus
SSL	Secure Sockets Layer, tiedon salaamiseen käytettävä protokolla
TDM	Time Division Multiplexing, aikajakokanavointi, jossa laitteille varataan oma aikaikkuna tiedon siirtoon
TKIP	Temporal Key Integrity Protocol, WEP-protokollan korvannut salausmenetelmä
VLAN	Virtual Local Area Network, tekniikka, jolla fyysinen tietoliikenneverkko voidaan jakaa loogisiin osiin
WDM	Wavelength Division Multiplexing, kanavointitapa, jossa yhteen kuitukaapeliin syötetään useita signaaleja eri aallonpituuksilla
WEP	Wired Equivalent Privacy, ensimmäinen WLAN-verkon salausmenetelmä
WESM	Wireless Edge Services Module, Hewlett Packardin WLAN-kontrollerimoduuli
WLAN	Wireless Local Area Network, langaton lähiverkkotekniikka
WPA	Wi-Fi Protected Access, WLAN-verkon tietoturvaprotokolla

1 JOHDANTO

Erilaiset kannettavat päätelaitteet, kuten älypuhelimet ja kannettavat tietokoneet, ovat yleistyneet viime vuosina huomattavasti. Uusimpana tuoteryhmänä markkinoille on tullut edellä mainittujen laitteiden väliin sijoittuvia kosketusnäytöllisiä tablet-tietokoneita. Kaikkia näitä laitteita hankkivat muutkin kuin tekniikasta kiinnostuneet ihmiset. Myös koulujen luokkaympäristöissä ja opetustavoissa on tapahtunut muutoksia, sillä nykyään yhä useammat voivat tehdä esimerkiksi luentomuistiinpanonsa kannettavalla tietokoneella.

Laitteet tarvitsevat yhteyden Internetiin, jotta niiden kaikkia toimintoja pystyy hyödyntämään monipuolisesti. Monet operaattorit myyvät kiinteähintaisia 3G-liittymiä, mutta kaikki eivät sellaista hanki, jos käyttö on satunnaista. Lisäksi 3G-yhteyden nopeus ja mahdollinen kuukausittainen siirtoraja saattavat rajoittaa laitteen käyttömahdollisuuksia. Toinen vaihtoehto on liittää laite langattomaan lähiverkkoon (WLAN) esimerkiksi kahvilassa tai koulussa.

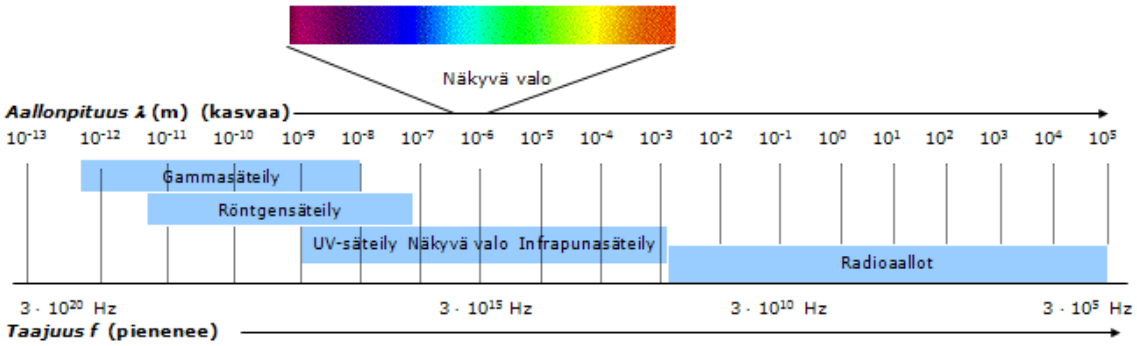
Tampereen ammattikorkeakoulussa päätettiin ajanmukaistaa kahden yhdistyneen koulun langaton lähiverkko. Käyttöön otettiin uusinta tekniikkaa tukeva WLAN-järjestelmä ja samalla uudistettiin niin henkilökunnalle, opiskelijoille kuin vierailijoillekin tarkoitetun verkon konsepti. Vanhaan verkkoon yhdistäminen oli koettu vaikeaksi, ja palautetta oli tullut koulun hallinnosta asti. Tukiasemien määrän kasvattaminen ja uudet tekniikat mahdollistivat verkon peittoalueen laajentamisen ja palvelun laadun parantamisen jokaisessa toimipisteessä.

Opinnäytetyössäni käsitellään ensimmäiseksi langattomiin lähiverkkoihin liittyvä teoria radiotekniikan, WLAN-standardien ja tietoturvan osalta. Sen jälkeen selostetaan lyhyesti vanhan verkon rakenteen ja suurimmat ongelmakodat. Lopuksi vuorossa on uuden järjestelmän osien ja konseptin esittely sekä pohdintaa uudistuksen hyödyistä.

2 RADIOTEKNIIKKA

2.1 Sähkömagneettinen säteily

Sähkömagneettinen säteily on poikittaista aaltoliikettä, joka etenee suoraviivaisesti valonnopeudella tyhjiössä. Käytännössä säteily etenee aina jossakin väliaineessa, kuten ilma. Säteily jaetaan taajuuden ja syntymekanismin perusteella kuuteen osa-alueeseen (kuvio 1), jotka ovat radioaallot, infrapunasäteily, valo, ultraviolettisäteily, röntgensäteily ja gammasäteily. Suuri osa ihmisen saamasta tiedosta tulee sähkömagneettisen säteilyn välityksellä, sillä näkyvä valo havaitaan silmillä ja radioaaltoja käytetään langattomassa tiedonsiirrossa, esimerkiksi televisiolähetyksissä, matkapuhelimissa ja langattomissa tietoverkoissa. (Räisänen & Lehto 2007, 9-11.)



KUVIO 1. Sähkömagneettisen säteilyn jaottelu (Hamara, Laukkanen, Lehtonen, Luoto, Vihavainen & Ylihärsilä)

2.1.1 Säteilyn ominaisuudet

Sähkömagneettisen säteilyn ominaisuuksia voidaan yleisesti kuvata neljällä parametrilla. Tiedonsiirron kannalta tärkein ominaisuus on vastaanotettu teho, sillä luotettavaan yhteyteen tarvitaan riittävä signaalin tehotaso häiriöihin verrattuna. Tehoa mitataan watteina (W), mutta koska väliaine vaimentaa signaalia logaritmisesti, on käytännöllisempää esittää tehoarvot desibeliasteikolla (dB). Vertailuarvona käytetään yleensä yhtä milliwattia, joka vastaa nollaa desibelimilliwattia (0 dBm). Vastaanotettu teho riippuu lähettimen tehosta ja signaalin vaimentumisesta. Tiedonsiirrossa käytettävä

taajuus (värähtelyjen lukumäärä/sekunti, yksikkö hertsi, Hz) ja aallonpituus (matka, jonka taajuus etenee yhden värähdyksen aikana) ovat kääntäen verrannollisia toisiinsa kaavan (1) mukaan, ja ne vaikuttavat signaalin kantamaan ja esteiden läpäisykykyyn. (Puska 2005, 53-54.)

$$f = \frac{c}{\lambda} \quad (1)$$

f = taajuus
c = valonnopeus
λ = aallonpituus

Vaihekulma puolestaan tarkoittaa saman lähettimen säteilyaaltojen erotusta, kun ne saapuvat eri vaiheessa vastaanottajalle eripituisista reiteistä johtuen. Aallot voidaan laskea yhteen, jolloin samanvaiheiset vahvistavat toisiaan ja 180 asteen vaihe-erossa saapuvat aallot kumoavat toisensa. Neljäs ominaisuus on polarisaatio, joka riippuu langattoman järjestelmän antennien kulmasta ja ominaisuuksista. Se kertoo, missä suunnassa aaltoliike värähtelee aallon etenemissuuntaan nähden. Käytännössä tällä tarkoitetaan sitä, että ideaalitilanteessa lähettimen ja vastaanottimen antennit ovat samansuuntaiset maanpinnan suhteen. (Puska 2005, 53-55.)

2.1.2 Valon käyttö tiedonsiirrossa

Radioaaltojen lisäksi tietoa voidaan siirtää langattomasti infrapunavalon avulla. Sitä käytetään muun muassa kaukosäätimissä, mutta tehokkaamman tiedonsiirron mahdollistaa vapaan tilan optinen tiedonsiirtomenetelmä, FSO (free-space optics), jossa valo lähetetään vastaanottajalle lasertekniikalla. Infrapunavaloa käyttävää signaalia ei voi havaita silmillä, ja taajuusalueen käyttöön ei tarvita lupaa. Laitteiden välille vaaditaan kuitenkin näköyhteys, joten tekniikkaa onkin käytetty esimerkiksi toisiaan lähellä olevien rakennusten lähiverkkojen yhdistämiseen. Teoreettinen tiedonsiirtonopeus on 1,25 Gb/s (gigabittiä sekunnissa), mihin ei ole aikaisemmin päästy millään muulla langattomalla tekniikalla. Tulevaisuudessa saavutetaan 10 Gb/s:n nopeus WDM-tekniikalla (Wavelength Division Multiplexing). (What is Free Space Optics 2005.)

Näkyvän LED-valon (Light-emitting diode) hyödyntämistä langattomassa tiedonsiirrossa on puolestaan alettu tutkia Bostonin yliopistossa. Tiedonsiirto toteutetaan välkyttämällä valoa tietyn kaavan mukaan, mutta ihmissilmä ei välkkymistä kuitenkaan huomaa. LED-valot voisivat tietyissä tapauksissa tarjota langattoman lähiverkon tukiasemalle vähävirtaisemman vaihtoehdon. Valonlähteen ja päätelaitteen välille tarvitaan kuitenkin näköyhteys, sillä valo ei läpäise esteitä, kuten seiniä. Käyttökohteena voisi olla esimerkiksi auditoriot, joissa kattoon asennetut LED-valot tarjoavat pääsyn verkkoon. (Moon 2008.)

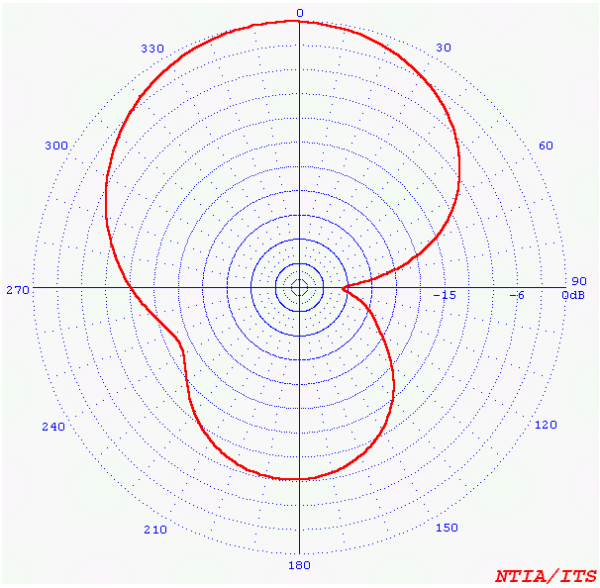
2.2 Radioaallot

Siirtomedialla tarkoitetaan fyysistä reittiä lähettimen ja vastaanottimen välillä. Radioaallot käyttävät ohjaamatonta siirtomediaa, sillä, toisin kuin kaapelissa kulkevilla signaaleilla, niillä ei ilmassa, avaruudessa tai vedessä edetessään ole ennalta määriteltyä kulkureittiä. Tiedonsiirron laatu ja ominaisuudet määräytyvät sekä siirtomedian että signaalin ominaisuuksien mukaan. Ohjaamattoman median tapauksessa käytettävissä oleva kaistanleveys on tärkeämpi tekijä kuin signaalin siirtoon käytettävä media. (Stallings 2007, 103.)

2.2.1 Radiojärjestelmä yleisesti

Radiotekniikassa lähetin tuottaa halutun signaalin radioaaltona syöttämällä sähkövirran antenniin. Siirtomedian toisessa päässä vastaanottimen antenni ottaa radiosignaalin vastaan ja syöttää sen vastaanottimelle, joka muuttaa signaalin takaisin sähkövirraksi. Näin tieto saadaan kulkemaan sähkömagneettisena säteilynä. Kaksisuuntaisessa liikenteessä, kuten langattomassa lähiverkossa, lähettimen ja vastaanottimen toiminnot on yhdistetty samaan laitteeseen. Yhtä antennia voidaan tarvittaessa käyttää sekä signaalin lähetykseen että vastaanottoon, sillä antennin ominaisuudet eivät ole riippuvaisia signaalin kulkusuunnasta. Antennit voivat olla joko ympärisäteileviä, jolloin signaali kuuluu joka suuntaan lähettimen ympärille, tai suunta-antenneja, jotka kohdistavat suurimman osan signaalin tehosta tiettyyn suuntaan. (Stallings 2007, 117.)

Antennin suorituskykyä kuvataan tavallisesti sen säteilykuviolla ja vahvistuksella, ja kuhunkin langattoman tiedonsiirron sovellukseen valitaan sitä varten optimoitu antenni. Edes ympärisäteilevä antenni ei säteile samalla tavalla kaikkiin suuntiin, vaan sillä on aina tietty säteily- eli suuntakuvio. Varsinaisilla suunta-antenneilla on suuntakuviossa pääkeila ja yksi tai useampi sivukeila (kuvio 2). Antenni kohdistaa suurimman osan säteilyn tehosta pääkeilaan. Niin sanotut adaptiiviset antennit pystyvät muuttamaan säteilykuviotaan vastaanottajan sijainnin perusteella, jolloin muualta tulevien häiriöiden vaikutus pienenee ja signaalin voimakkuus kasvaa. Antennivahvistus kertoo suhdeluvun, kuinka paljon voimakkaammin antenni säteilee pääkeilan suuntaan verrattuna ympärisäteilevään antenniin samalla teholla. Yksikkö on dBi, jossa i-kirjain viittaa isotrooppiseen eli ympärisäteilevään antenniin. (Räisänen & Lehto 2007, 159-160, 162.)

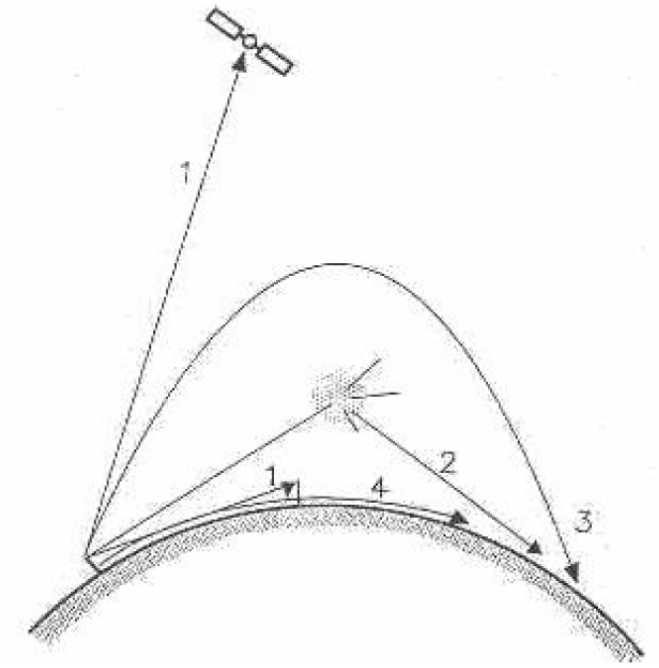


KUVIO 2. Esimerkki säteilykuviosta (Perkiömäki)

2.2.2 Radioaaltojen eteneminen

Radioaaltojen etenemiseen vaikuttaa taajuus, ympäristö sekä sen esteet, etäisyys, antennit sekä niihin syötettävä teho ja häiriöt. Niiden tärkeimmät etenemismekanismit on esitetty alla (kuvio 3). Aalto voi edetä useiden mekanismien avulla. Mitä korkeampi taajuus on, sen lyhyempi kantomatka, pienemmät antennit, suurempi tehontarve ja vähäisemmät häiriöt.

1. Näköyhteysreittiä pitkin (0,3 - 300 GHz). Lähettimen ja vastaanottimen antenneilla on näköyhteys toisiinsa. Koska maanpinta on kaareva ja signaali kaareutuu sen mukaan, radiohorisontti on kauempana kuin geometrinen horisontti.
2. Sironnan avulla (0,3 - 10 GHz). Signaali muuttaa suuntaansa ilmakehän epähomogeenisuuksista johtuen. Tällaisia ovat pienet partikkelit sekä esimerkiksi vesipisarat ja tekstiilikuidut. Sironta voi tuottaa myös uusia radioaaltoja eri suuntiin.
3. Ionosfäärin kautta (3 - 30 MHz). Signaali heijastuu ilmakehän ionosfäärikerroksesta (60 - 1000 km). Heijastumalla uudelleen maanpinnasta signaali voi edetä ympäri maapallon.
4. Maanpinta-aaltona (0,03 - 10 MHz). Signaali etenee maanpinnan suuntaisesti maaperän sähkönjohtavuuden ansiosta. (Räisänen & Lehto 2007, 189-190.)

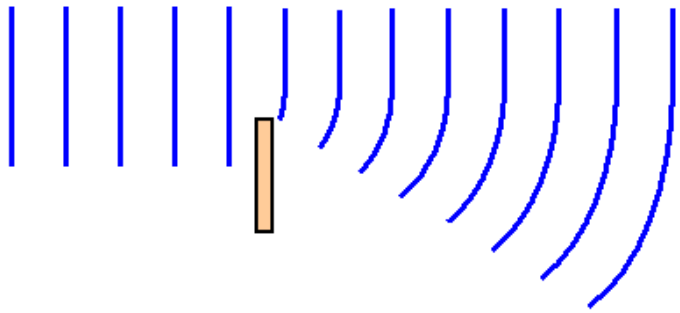


KUVIO 3. Radioaaltojen tärkeimmät etenemistavat (Juutilainen, 9)

Radioaallot etenevät suoraviivaisesti ja vaimentumatta vain tyhjiössä. Kaikentyyppiset langattomat signaalit vaimenevat vähintään hajonnan takia. Hajonta tarkoittaa signaalin leviämistä aina suuremmalle ja suuremmalle alueelle, kun etäisyys lähettimeen kasvaa. Tästä ilmiöstä käytetään nimeä vapaan tilan vaimennus. Vaimennusta ilmassa aiheuttaa absorptio, joka tarkoittaa signaalin tehon imeytymistä vesihöyryyn, happimolekyyleihin ja muihin esteisiin. Signaalit eivät aina pääse kulkemaan esteettömästi ja suoraan, vaan ne heijastuvat yhteen tai useampaan suuntaan erilaisista esteistä. Tästä aiheutuu monitie-etenemistä, kun alkuperäisestä signaalista muodostuu kopioita, jotka saapuvat vas-

taanottajalle eri aikaan. Luvussa 2.1.1 esitellyn vaihekulman teorian perusteella monitie-etenemisestä voi olla hyötyä signaalin vahvistamisessa, kun se otetaan huomioon radiojärjestelmän suunnittelussa. (Stallings 2007, 129, 132.)

Taipuminen eli diffraktio mahdollistaa langattomien signaalien kulkemisen paikkoihin, joihin ei esteiden takia ole suoraa näköyhteyttä. Radioaallot taipuvat ja leviävät osuessaan esteeseen (kuvio 4). Edellä esiteltyjen asioiden lisäksi signaalin heikentymistä aiheuttaa myös häipyminen, joka voi olla hidasta tai nopeata. Hitaassa häipymisessä signaalin keskiarvo muuttuu signaalin kulkureitin muutoksen takia. Nopeassa häipymisessä alkuperäisestä signaalista jakautuneet osasignaalit summautuvat vastaanottajalla, mikä johtuu sekä monitie-etenemisestä että liikkeestä. (Juutilainen, 29-30.)



KUVIO 4. Esimerkki taipumisesta (Gibbs 2010)

Kaikissa radioyhteyksissä esiintyy kohinaa, joka asettaa rajat signaalin kantamalle ja yhteyden luotettavuudelle. Vastaanotetun signaalin täytyy olla tarpeeksi voimakas kohinaan verrattuna, jotta signaalin sisältämä tieto voidaan tulkita oikein. Kohina tarkoittaa kaikkia hyötysignaaliin sekoittuvia, ei-toivottuja signaaleja, ja sitä aiheutuu kahdesta lähteestä: vastaanottimen elektronisista piireistä ja häiriösäteilystä, jota vastaanottimen antenni havaitsee hyötysignaalin lisäksi. Signaali-kohina-suhde (SNR tai S/N) on luku, joka ilmaisee signaalin ja kohinan suhteen desibeleinä kaavan (2) mukaan. Mitä suurempi suhdeluku on, sitä parempi on signaalin laatu. (Fette, Aiello, Chandra, Dobkin, Bensky, Miron, Lide, Dowla & Olexa 2008, 90-91.)

$$SNR_{dB} = \log_{10}\left(\frac{P_s}{P_n}\right) \quad (2)$$

P_s = signaalin teho

P_n = kohinan teho

2.3 Taajuusalueet

Radioaallot sijoittuvat taajuuksille 3 kHz - 300 GHz (Radio Frequency, RF). Ne on edelleen ryhmitelty osa-alueisiin käyttötarkoituksen mukaan (taulukko 1). Esimerkiksi VHF-aluetta käyttää muun muassa FM-radio ja UHF-aluetta matkapuhelimet. Koska radioaallot voivat häiritä toista käyttäjää, radiotaajuuksien käytöstä sovitaan kansainvälisin sopimuksin. Kansainvälinen televiestintäliitto ITU (International Telecommunication Union) järjestää joka toinen tai kolmas vuosi konferenssin, jossa kansainvälinen radio-ohjesääntö tarkistetaan ja vahvistetaan. Useimmissa tapauksissa radiotaajuuksien käyttö ei kuitenkaan voi häiritä maailmanlaajuisesti signaalien kantaman takia, ja maapallo onkin jaettu kolmeen alueeseen, joilla kullakin on oma radiotaajuuksien jako. (Räisänen & Lehto 2007, 12.)

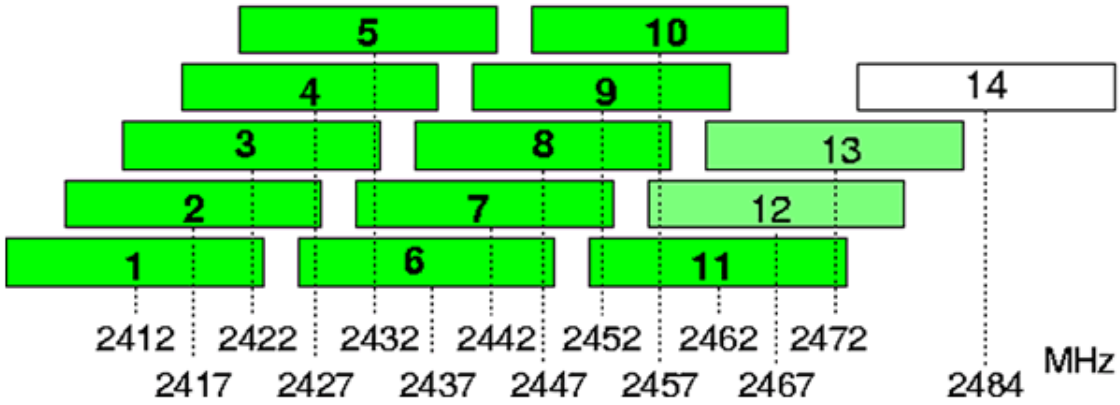
TAULUKKO 1. Radioaaltojen taajuusalueet (Räisänen & Lehto 2007, 10)

Taajuusalue	Nimi	Lyhenne
3 - 30 kHz	Very Low Frequencies	VLF
30 - 300 kHz	Low Frequencies	LF
300 - 3000 kHz	Medium Frequencies	MF
3 - 30 MHz	High Frequencies	HF
30 - 300 MHz	Very High Frequencies	VHF
300 - 3000 MHz	Ulta High Frequencies	UHF
3 - 30 GHz	Super High Frequencies	SHF
30 - 300 GHz	Extremely High Frequencies	EHF

Taajuusalueesta riippuen sen hyödyntäminen saattaa vaatia luvan kansalliselta säätelyviranomaiselta. On olemassa myös lisenssivapaita taajuusalueita, joiden hyödyntämiseen ei tarvita lupaa, kunhan laitteiden ominaisuudet ovat määräysten mukaiset. (Puska 2005, 53.) Suomessa lupia myöntää Viestintävirasto, joka on viime vuosina myynyt taajuusalueita muun muassa uusien 4G-matkapuhelinverkkojen käyttöön.

Radiotekniikan sovelluksille on edellä esitetyistä taajuusalueista lohkottu omat taajuusalueet, joita ne voivat käyttää. Esimerkiksi langaton lähiverkkotekniikka käyttää standardista riippuen 80 MHz:n taajuuskaistaa 2,4 GHz:n taajuusalueella tai kolmea 100 MHz:n kaistaa 5 GHz:n taajuusalueella. Sovellusten käyttämä taajuusalue on puolestaan

jaettu vielä pienempiin osiin, joita kutsutaan kanaviksi. 2,4 GHz:n taajuusalueella kanavia on 5 MHz:n välein, Euroopassa 13. WLAN-tekniikassa kanavan kaistanleveys täytyy kuitenkin olla 20 MHz, joten kanavia, jotka eivät häiritse toisiaan, on vain kolme (kuvio 5). 5 GHz:n taajuusalueella on enemmän kanavia, ja niiden keskitaajuudet ovat 20 MHz:n päässä toisistaan, joten kanavat eivät häiritse toisiaan.



KUVIO 5. Kanavat ja keskitaajuudet 2,4 GHz:n taajuusalueella (Air-Stream Wireless)

2.4 Hajaspektritekniikka

Hajaspektritekniikan avulla jaetaan siirrettävän tiedon sisältämä signaali leveämmälle taajuuskaistalle, jos signaali ei muuten pystyisi hyödyntämään koko kapasiteettia. Se on tärkeä koodausmuoto langattomalle tiedonsiirrolle, ja sen ansiosta signaalin häirintä ja estäminen vaikeutuu. Toiminta perustuu siihen, että ennen signaalin siirtämistä siirtomediaan sitä moduloidaan niin sanotulla hajautuskoodilla. Vaikka tekniikka tuhlaa radiospektriä, siitä on seuraavia hyötyjä: Signaali sietää paremmin monia häiriölähteitä ja monitie-etenemisestä johtuvia vääristymiä. Vain vastaanottaja, joka tietää hajautuskoodin, voi purkaa koodatun signaalin. Lisäksi useat käyttäjät voivat samanaikaisesti käyttää samaa taajuuskaistaa aiheuttamatta suuria häiriöitä toisille. Hajaspektrin tyyppejä on kolme: Frequency-Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) ja Code Division Multiple-Access (CDMA). (Stallings 2007, 275-276.)

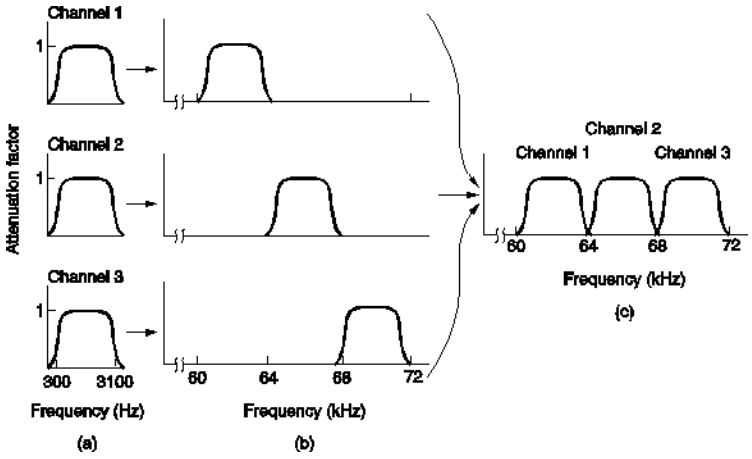
FHSS:ssa vaihdetaan tasaisin väliajoin taajuutta, jolla signaalia lähetetään (”taajuushyppely”). Vastaanottajalla on tiedossa taajuudet ja vaihtojärjestys, joten se pystyy ymmärtämään vastaanottamansa tiedon. Muun muassa Bluetooth käyttää taajuushyppelyä.

DSSS:ssa puolestaan jokainen alkuperäisen signaalin bitti esitetään usealla bitillä ja näin lähetettävä signaali hajautetaan taajuuskaistalle. CDMA:ssa jokaiselle käyttäjälle määritetään oma koodi, jolla kunkin signaalia moduloidaan. Näin eri käyttäjien signaalit voidaan erottaa toisistaan. (Stallings 2007, 277, 282, 287.)

2.5 Kanavointi

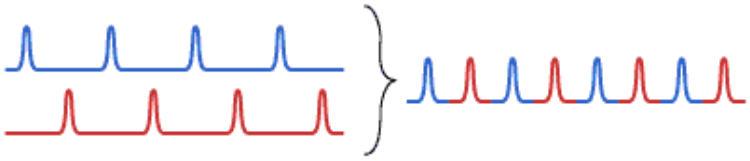
2.5.1 FDM ja TDM

Langatonta siirtotietä voidaan hyödyntää tehokkaasti käyttämällä kanavointia. Se tarkoittaa sitä, että lähettimet jakavat siirtokapasiteetin pienempiin osiin ja käyttävät sitä samanaikaisesti, jolloin koko kanava saadaan käytettyä tiedonsiirtoon. Tekniikan kaksi yleisintä muotoa ovat taajuusjakoinen (Frequency Division Multiplexing, FDM) ja aikajakoinen (Time Division Multiplexing, TDM) kanavointi. FDM:ssä (kuvio 6) useita signaaleja siirretään samassa siirtomediassa moduloimalla jokaiselle niistä oma taajuuskaista. (Stallings 2007, 240.)



KUVIO 6. Taajuusjakoinen kanavointi (Mederly 2007)

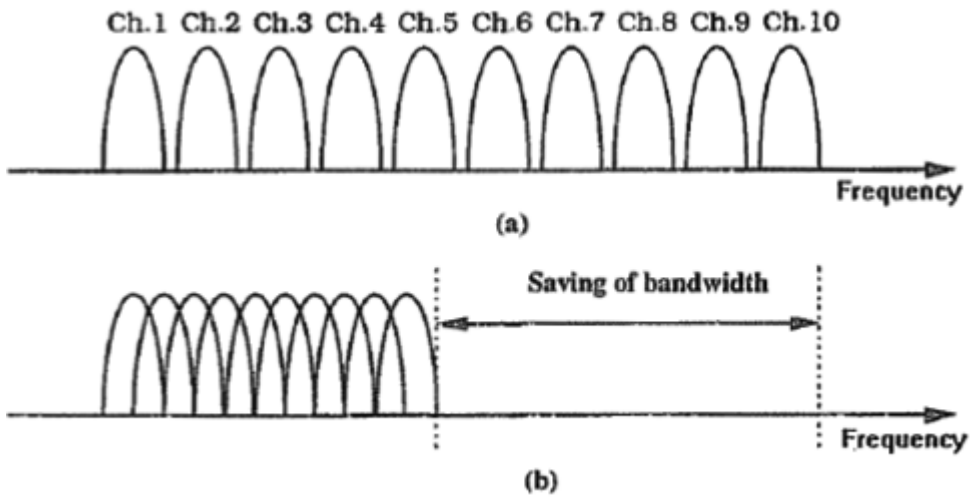
TDM:ää (kuvio 7) on kahta tyyppiä: synkroninen ja tilastollinen. Ensimmäisessä tietoa siirretään peräkkäisissä kehyksissä, joissa jokaiselle lähettimelle on varattu yksi tai useampi aikaikkuna, jonka aikana siirrettävän tiedon voi asettaa kehykseen. Tilastollinen pyrkii olemaan tehokkaampi puskuroimalla siirrettävää tietoa ja lähettämällä sitä eteenpäin mahdollisimman nopeasti. (Stallings 2007, 240.)



KUVIO 7. Aikajakoinen kanavointi (Paschotta)

2.5.2 OFDM

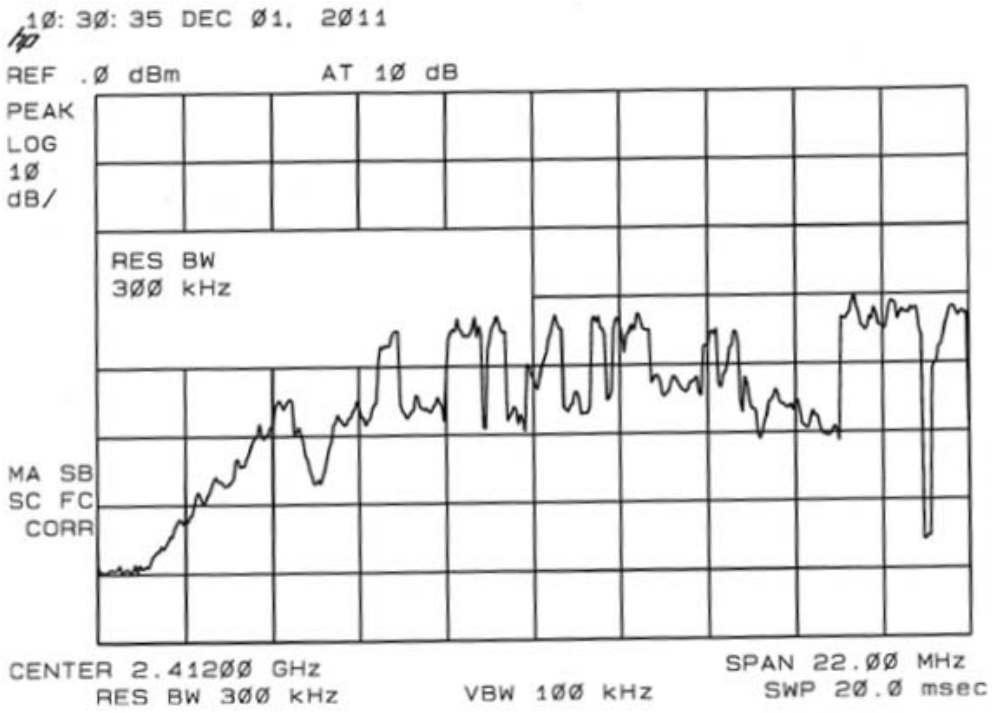
Orthogonal Frequency Division Multiplexing (OFDM) on taajuusjakoinen kanavointitekniikka, jossa tiedonsiirtokanava on tasaisesti jaettu useisiin taajuuskaistoihin. Siirrettävä tieto jaetaan vastaavasti osiin ja jokainen alikantoaalto siirtää osan tiedosta jokaisella kaistalla. OFDM on erityinen taajuusjakoinen (FDM) järjestelmä, jossa alikantoaaltojen sivukaistat menevät toistensa päälle, mutta signaalit voidaan silti havaita ilman viereisestä alikantoaallosta aiheutuvia häiriöitä. Tämä johtuu siitä, että alikantoaallot ovat matemaattisesti kohtisuorassa toisiinsa nähden. Tavanomaisessa FDM-järjestelmässä, taajuuksien välissä on niin sanottu turvakaista, joka erottaa kantoaallot toisistaan. OFDM tarvitsee näin ollen vähemmän kaistaa kuin FDM (kuvio 8). OFDM:ää käyttävät monet tiedonsiirtosovellukset, esimerkiksi useat DSL-tekniikat (Digital Subsciber Line), tietyt WLAN-standardit ja digitaaliset televisiolähetykset (DVB). (Fette ym. 2008, 803.)



KUVIO 8. FDM:n (a) ja OFDM:n (b) ero (Klug 2011)

2.6 Spektrianalyysi

Signaalia tarkastellaan yleensä taajuustasossa, eli signaalin tehoa taajuuden suhteen. Aikatason esitys kertoo vain, kuinka esimerkiksi signaalin voimakkuus muuttuu ajan suhteen. Taajuustasossa puolestaan näkyy signaalin spektri, eli taajuusjakauma (kuvio 9). Spektrianalysaattori ei ole sidottu tietyntyyppiseen liikenteeseen (esimerkiksi WLAN tai Bluetooth), vaan se tarkastelee signaalia säteilynä. Sillä nähdään myös kohinataso ja mahdolliset häiriölähteet, jotka käyttävät samaa taajuutta.



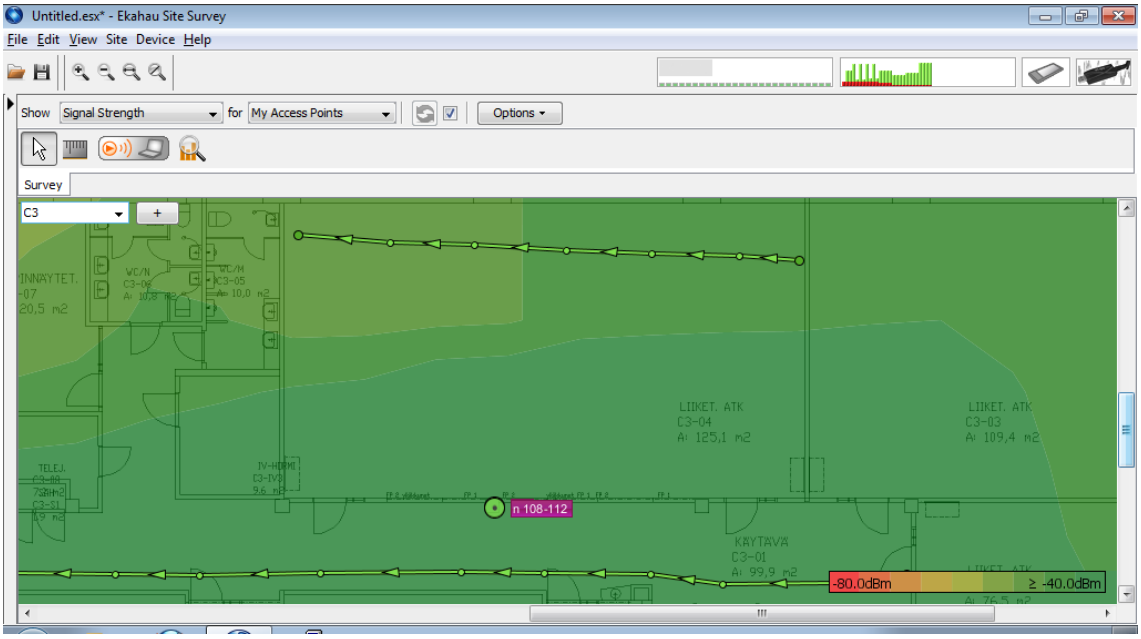
KUVIO 9. WLAN-signaalin spektrin signaalitasojen maksimiarvot eräässä mittauksessa

2.7 Site survey

Site survey on olennainen ja lähes pakollinen osa langattoman lähiverkon suunnittelua ja toteutusta. Se sisältää kuuluvuusmittauksen, RF-kartoituksen ja tukiasemien asennuspaikkojen valinnan, ja sen avulla saadaan yleiskuva ympäristöstä, johon verkkoa suunnitellaan. Muiden kuin WLAN-laitteiden aiheuttamia häiriöitä voidaan arvioida spektrianalyysilla. Toteutusvaiheen aikana mitataan, täyttääkö verkko sille asetetut vaatimukset, joihin kuuluvat muun muassa peittoalue, kapasiteetti ja siirtonopeudet. Mikäli van-

haa verkkoa ja laitteistoa ollaan päivittämässä, saadaan site surveyllä selville verkon lähtötilanne ja mahdolliset ongelmakohdat.

Markkinoilla on olemassa erilaisia site survey -ohjelmia, joista yleisimmät ovat Ekahau Site Survey (kuvio 10) ja Fluke Networksin AirMagnet. Ohjelmaan tuodaan kartoitettavan rakennuksen pohjapiirustus, jonka mittakaava määritetään. Kartoitus tapahtuu kulkemalla rakennuksessa ja merkitsemällä karttaan kulkureitti (kuvassa vihreä nuoliviiva). Ohjelma mittaa langattoman verkon signaalin kuuluvuutta (passiivinen site survey) ja muita parametreja, kuten vasteaikaa (aktiivinen site survey). Ohjelma osaa mittaustulosten perusteella arvioida verkon kuuluvuuden niillä alueilla, joilla ei ole käyty. Molemmilla on myös suunnitteluohjelma, joka arvioi sekä tarvittavien tukiasemien määrän että sijoituspaikat rakennuksen pohjapiirustuksen ja rakenteiden sekä verkon vaatimusten perusteella. Lisäksi internetissä on ladattavissa ilmaisia ohjelmia, joilla näkee lähellä olevien WLAN-verkkojen käyttämät kanavat ja signaalivoimakkuudet. Esimerkki tällaisesta ohjelmasta on InSSIDer.



KUVIO 10. Ekahau Site Survey

2.8 Haasteet ja tulevaisuus

Lisenssivapaita taajuusalueita hyödyntävien standardien suurin ongelma on se, että samalla taajuusalueella on muitakin laitteita. Esimerkiksi lyhyen kantaman tiedonsiirtoon tarkoitettu Bluetooth, WLAN ja mikroaaltouunit toimivat samalla 2,4 GHz:n taajuusalueella. Kyseisellä taajuusalueella on WLAN-laitteita varten vain kolme kanavaa, jotka eivät häiritse toisiaan. Tästä johtuen uusimmat WLAN-standardit ovat alkaneet käyttää korkeampia taajuusalueita, joilla signaalin kantama on kuitenkin lyhyempi. Ruuhkattomammat taajuudet mahdollistavat myös kahden tai useamman kanavan yhdistämisen, jolloin tiedonsiirtonopeus kasvaa.

Uusia tekniikoita tiedonsiirron nopeuden kasvattamiseksi ja viiveiden pienentämiseksi kehitetään erityisesti WLAN- ja matkapuhelinpuolella. Samalla pyritään taajuusalueen tehokkaampaan hyödyntämiseen. OFDM on ollut käytössä WLAN-standardeissa vuosia, ja siitä kehitetty versio OFDMA (Orthogonal Frequency Division Multiple Access), joka alkuperäiseen verrattuna sallii usean yhtäaikaisen käyttäjän, on otettu käyttöön uusimman sukupolven LTE-matkapuhelinverkoissa (Long Term Evolution).

Matkapuhelin- ja WLAN-verkkojen yhteistyö lisääntyy tulevaisuudessa, kunhan laitteet saadaan saumattomasti ilman katkoja vaihtamaan eri verkkojen välillä. Matkapuhelinverkoissa siirretyn tiedon määrä on moninkertaistunut viime vuosina, ja operaattorit haluavat vähentää verkkojensa kuormitusta. Ideana on, että matkapuhelinverkkoa käyttävä päätelaite siirtyisi automaattisesti käyttämään suuremman tiedonsiirtokapasiteetin tarjoavaa WLAN-verkkoa, kun sellainen on lähellä. Tästä käytetään termiä ”WiFi offload”. (Zander 2011.)

Tulevaisuudessa mobiilimaksaminen voi korvata erilliset maksukortit. RFID (Radio Frequency IDentification) on radiotaajuuksilla toimiva etätunnistusmenetelmä, jota voidaan verrata viivakoodiin, mutta teknologian toiminta perustuu tiedon tallentamiseen RFID-tunnisteeseen ja sen langattomaan lukemiseen RFID-lukijalla. Sitä on hyödynnetty kauan esimerkiksi kulkuavaimissa, matkakorteissa ja teollisuudessa. Yksi RFID-tekniikkaa hyödyntävä sovellus on NFC (Near Field Communication), jossa koskettamalla (lukuetäisyys 4 cm) esineitä puhelimella voidaan mm. käynnistää palveluita sekä kerätä ja välittää tietoa. (RFID Lab Finland ry.)

3 LANGATON LÄHIVERKKO

Langaton lähiverkko eli WLAN käyttää edellisessä luvussa esiteltyjä radioaaltoja tiedon siirtämiseen. Käyttäjä muodostaa langattomalla verkkosovittimella varustetulla laitteellaan yhteyden toiseen päätelaitteeseen tai WLAN-verkon tukiasemaan, joka on yleensä kytketty langalliseen verkkoon, josta on edelleen yhteys Internetiin. Käytettävissä olevat verkot erotetaan toisistaan verkon nimen kertovalla SSID-tunnuksella (Service Set IDentifier).

3.1 IEEE:n 802.11-standardit

Institute of Electrical and Electronics Engineers (IEEE) on kansainvälinen järjestö, joka on julkaissut langattoman lähiverkon toiminnan määrittelevät 802.11-standardit. Ne ovat saaneet virallisen kansainvälisen aseman, kun kansainvälinen standardisoimisjärjestö ISO (International Organization for Standardization) on ottanut määritelmät käyttöön omilla standardinumeroillaan. Standardit määrittelevät sekä fyysisen kerroksen että siirtokerroksen ominaisuudet. Fyysiseen kerrokseen kuuluu kanavan, siirtonopeuden, kanavointitavan, hajaspektritekniikan ja modulaation määritys. Siirtokerroksella kehystetään verkkokerroksen paketti siirtoa varten, ja sen MAC-alikerros (Media Access Control) huolehtii siirtotien varauksesta, verkkoon liittymisestä ja tunnistautumisesta. (Puska 2005, 25-26.)

Langattomassa verkossa käytetään CSMA/CA-vuoronvarausta (Carrier Sense Multiple Access with Collision Avoidance). Päätelaitteen, joka haluaa lähettää tietoa, täytyy ensin kuunnella kanavaa saadakseen selville, onko se vapaa. Törmäyksiä yritetään välttää sallimalla vain yksi lähetys kerrallaan, koska on mahdollista, että kaksi päätelaitetta kuulevat tukiaseman, mutta eivät toisiaan signaalin vaimentumisen takia. WLAN-verkossa voidaan käyttää myös RTS/CTS-kättelyä (Request To Send/Clear To Send), jolloin tukiasema myöntää kullekin päätelaitteelle erikseen luvan lähetykseen. Päätelaite pyytää lupaa RTS-viestillä, johon tukiasema vastaa CTS-viestillä, kun kanava on vapaa. (Puska 2005, 29.)

3.1.1 802.11a ja 802.11b

Sekä 802.11a että 802.11b julkaistiin samoihin aikoihin vuonna 1999. Standardi 802.11a käyttää kerrallaan yhtä 20 MHz:n kanavaa 5 GHz:n taajuusalueella ja mahdollistaa tiedonsiirtonopeudeksi 54 megabittiä sekunnissa (Mb/s). Standardi 802.11b käyttää myös 20 MHz:n kanavia, mutta se toimii 2,4 GHz:n taajuusalueella ja teoreettinen siirtonopeus on vain 11 Mb/s. Vaikka 802.11a on lukujen perusteella parempi, sen yleistymistä haittasi suurempaa taajuutta tukevien piirien hinta, ja se jäi lähinnä yrityskäyttöön. 802.11a käyttää OFDM-tekniikkaa, ja 802.11b puolestaan käyttää CCK-koodausta (Complementary Code Keying), joka perustuu DSSS-modulaatioon. Standardit eivät ole yhteensopivia keskenään eri taajuusalueista johtuen, mutta laitteissa voi olla molemmille omat radionsa. (IEEE 802.11 standards tutorial, 2-3.)

3.1.2 802.11g

Vuonna 2003 julkaistu 802.11g-standardi kehitettiin nostamaan 802.11b-standardiin perustuneen verkkojen nopeutta. Kuten edeltäjänsä, 802.11g käyttää 2,4 GHz:n taajuusaluetta, mutta sen teoreettinen tiedonsiirtonopeus on sama kuin 802.11a:ssa, eli 54 Mb/s. Modulaatiotekniikkaa vaihdetaan tiedonsiirtonopeuden mukaan yhteensopivuuden takaamiseksi, eli käytettävissä on niin OFDM (6-54 Mb/s), CCK (5,5 ja 11 Mb/s) kuin DSSS:kin (1-2 Mb/s). (IEEE 802.11 standards tutorial, 5.)

802.11g on alaspäin yhteensopiva 802.11b-laitteiden kanssa. Nopeampaa 802.11g-standardia käyttävien laitteiden siirtonopeus tosin saattaa hidastua, jos samassa verkossa on myös 802.11b-laitteita, joita joudutaan odottamaan. Vain 802.11b-standardia tukevia laitteita ei kuitenkaan ole markkinoilla ollut pitkään aikaan, sillä 802.11g syrjäytti vanhemman standardin nopeasti.

3.1.3 802.11n

WLAN-verkon nopeutta haluttiin edelleen kasvattaa, joten vuonna 2009 julkaistiin uusi standardi, 802.11n. Se sisältää teknisiä uudistuksia, joiden avulla teoreettinen siirtono-

peus on 150, 300 tai jopa 600 Mb/s. Uuden standardin myötä otettiin uudelleen käyttöön myös 5 GHz:n taajuusalue, eli 802.11n toimii kummallakin taajuusalueella. (IEEE 802.11 standards tutorial, 7.)

802.11n-standardi mahdollistaa kahden 20 MHz:n kanavan yhdistämisen, minkä avulla yhden datavirran tiedonsiirtonopeus kaksinkertaistuu. Kanavien yhdistäminen ei useinkaan ole mahdollista 2,4 GHz:n taajuusalueella sen ruuhkaisuudesta johtuen, joten ominaisuutta voidaan hyödyntää vain 5 GHz:n radiolla varustetuissa laitteissa. Toinen tiedonsiirtonopeutta kasvattava uudistus on MIMO-tekniikka (Multiple-In/Multiple-Out). Siinä hyödynnetään kahdesta neljään antennia ja monitie-etenemistä, joka aiemmin on aiheuttanut häiriötä. Siirrettävä tieto jaetaan erillisiksi datavirroiksi, jotka siirtyvät omaa reittiään eri antennien välillä. 802.11n sallii korkeintaan neljä yhtäaikaista virtaa, ja päätelaitteen ja tukiaseman antennien määrä määrittelee, montaako voidaan käyttää. (IEEE 802.11 standards tutorial, 7.)

Myös antennitekniikkaa kehitettiin. Antennikuviota voidaan muuttaa niin, että aiempaa suurempi osa signaalin tehosta kohdistetaan vastaanottajalle. Tästä käytetään termiä keilanmuodostus. Sen ansiosta kantama pitenee ja kanava saadaan hyödynnettyä paremmin parantuneen signaali-kohina-suhteen ansiosta. Kasvanut antennimäärä antaa lisäksi mahdollisuuden valita tiedonsiirrolle kulloinkin parhaat signaaliolosuhteet. (IEEE 802.11 standards tutorial, 7.) 802.11n-standardin keilanmuodostus perustuu eri antenneihin tulevan signaalin vaihe-eroon, eli MIMO-tekniikkaa ei voi käyttää samaan aikaan samoilla antenneilla.

Uudistusten lisäksi 802.11n on 2,4 GHz:n taajuusalueella yhteensopiva 802.11b:n ja 80211g:n kanssa. Nykyään myytävät laitteet tukevat siis 802.11b:tä, 802.11g:tä ja 802.11n:ää. Jos laitteessa on kaksi radiota, toinen niistä on määritetty 5 GHz:n taajuusalueen 802.11a- ja 802.11n-standardille, ja sitä käytetään ensisijaisena paremman tiedonsiirtonopeuden ja ruuhkattomuuden takia.

3.1.4 802.11ac ja 802.11ad

Vielä luonnosvaiheessa ovat standardit 802.11ac ja 802.11ad, joilla siirtonopeudet nousevat gigabittiluokkaan. Niistä 802.11ac käyttää vain 5 GHz:n taajuusaluetta ja kasvattaa kaistanleveyden 80 MHz:iin sekä mahdollisuuksien mukaan jopa 160 MHz:iin. Koska siinä yhdistetään neljä tai kahdeksan kanavaa, standardissa on mukana kaistanleveyden automaattinen valinta käytettävissä olevien kanavien mukaan. Lisäksi 802.11n-standardissa käyttöön otettua MIMO-tekniikkaa laajennetaan niin, että samaan aikaan voidaan lähettää datavirtoja usealle käyttäjälle. Tästä käytetään termiä Multi-User MIMO (MU-MIMO). Samanaikaisten datavirtojen määrä on kaksinkertaistettu kahdeksaan. (IEEE 802.11 standards tutorial, 8.)

Standardi 802.11ad on tarkoitettu lyhyen kantaman tiedonsiirtoon, esimerkiksi teräväpiirtovideon siirtoon kahden samassa huoneessa olevan laitteen välillä. Sille suunniteltu 60 GHz:n taajuus, jossa kaistanleveyttä voidaan kasvattaa edelleen, ei kanna muutamaa metriä pidemmälle. Standardin teoreettiseksi nopeudeksi on ennakoitu 6 gigabittiä sekunnissa (Gb/s) ja 802.11ac:lle 1 Gb/s. (IEEE 802.11 standards tutorial, 8-9.)

3.1.5 802.11af

Tulevaisuudessa 802.11af-standardi tulee hyödyntämään televisiolähetyksiltä käyttämättömäksi jäänyttä radiospektriä, joka sijoittuu 1 GHz:n taajuusalueelle. Matalampi taajuus parantaa signaalin kantamaa. Sen toiminta ei kuitenkaan saa aiheuttaa häiriötä jäljelle jääneille TV-lähetyksille. Tämä toteutettaisiin joko kognitiivisella radiolla, joka osaa vaihtaa kanavaa TV- tai muun lähetyksen havaitessaan, tai tietokannalla, joka sisältää maakohtaiset tiedot sallituista kanavista. (IEEE 802.11 standards tutorial, 10.)

3.1.6 Muut standardit

Edellä esiteltyjen verkon siirtonopeuteen liittyvien standardien lisäksi IEEE on julkaissut standardeja, jotka tarjoavat lisäominaisuuksia. Esimerkiksi 802.11d lisää verkon mainostukseen mukaan maakoodin. Verkkoon liittyvä laite osaa sen perusteella valita

käytettävissä olevat kanavat ja signaalitehot. Standardi 802.11u (Hotspot 2.0) liittyy aiemmin mainittuun ”WiFi offload” -verkonvaihtoon, eli matkapuhelinverkossa olevalle laitteelle tarjotaan mahdollisuus saada palveluntarjoajien sopimusten määrittelemiä palveluita WLAN-verkon kautta. Perimmäinen ajatus on parantaa käyttökokemusta, kun käyttäjän ei tarvitse enää tietää oikean WLAN-verkon nimeä, vaan hän saa listan tarjolla olevista palveluista. (About.com Encyclopedia.)

3.2 Tietoturva

Radiosignaalin etenemistä ei voi rajoittaa vain tietylle alueelle ja jaetussa mediassa liikennettä on helpompi salakuunnella kuin kaapelissa, joten langattoman lähiverkon liikenne kannattaa salata tiedon luottamuksellisuuden takaamiseksi. Salaamattomia verkkoja puoltaa niiden helppokäyttöisyys, mutta käyttäjien tulee olla tietoisia siitä, että kuka tahansa samassa verkossa oleva voi tarkkailla liikennettä. Verkon käyttäjiä voidaan myös vaatia tunnistautumaan käyttäjätunnuksella ja salasanalla ennen kuin liikennöinti sallitaan. Lisäksi verkkoon voidaan sallia vain tietyt laitteet käyttämällä MAC-osoitteisiin perustuvia pääsylistoja, kunhan se ei ole ainoa suojauskeino, sillä MAC-osoitteen väärentäminen on mahdollista. Verkon SSID voidaan piilottaa, mutta sen saa silti helposti selville WLAN-verkkoja kartoittavilla ohjelmilla.

Tukiasemissa, jotka tukevat virtuaalilähiverkkoja (Virtual Local Area Network, VLAN), voidaan eri SSID-tunnuksille määritellä erilaiset tunnistus-, salaus- ja IP-osoiteasetukset. Eri WLAN-verkkojen liikennettä voidaan tällöin suodattaa, jolloin eri käyttäjäryhmille saadaan tarjottua eri palveluita. Esimerkiksi yrityksessä voi olla WLAN-verkko sen omia laitteita varten ja toinen verkko vierailijoille. Yrityksen omassa verkossa käytetään vahvaa salausta ja tunnistautumista, ja sen kautta voi päästä samoihin palveluihin kuin kaapeliyhteydelläkin. Vierailijoiden salaamattomasta verkosta, johon kirjaudutaan www-sivulla henkilökunnalta saadulla tunnuksella, pääsee rajoitetusti esimerkiksi Internetiin, ja se on eristetty palomuurilla yrityksen sisäverkosta.

3.2.1 WEP

WEP eli Wired Equivalent Privacy on ensimmäinen WLAN-verkon salausmenetelmä, joka käyttää samaa WEP-salausavainta kaikille päätelaitteille. Verkkoon ei saa yhteyttä, ellei tiedä sen salausavainta, joka voi olla 40- tai 104-bittinen. WEP käyttää RC4-koodausta, jota ei ole tarkoitettu käytettäväksi uudestaan samalla avaimella. Siksi WEP-avain laajennetaan 24-bittisellä alustusvektorilla (Initialization Vector, IV). Alustusvektori lähetetään selväkielisenä vastaanottajalle, jotta se voisi purkaa salauksen. WEP-salausta ei enää nykyään voida pitää luotettavana, koska nykyaikaiset tietokoneet voivat murtaa salauksen nopeasti kokeilemalla eri avainyhdistelmiä. Lisäksi alustusvektoreita tarkkailemalla hyökkääjä voi saada salauksen parametreja selville. WEP ei suojaa tiedon väärentämiseltä, eli hyökkääjä voi muuttaa salatun kehyksen sisältöä purkamatta salausta ja vastaanottajan huomaamatta. Ylläpidon kannalta kaikilla käytössä oleva sama avain aiheuttaa ongelmia, sillä avaimen paljastuttua se joudutaan erikseen vaihtamaan kaikkiin laitteisiin. (Bardwell & Akin 2005, 426-428.)

3.2.2 TKIP

TKIP (Temporal Key Integrity Protocol) kehitettiin korjaamaan WEP-salauksen tietoturvaongelmat. Siinä parannettiin RC4-salauksen toteutustapaa sallimalla vain 104-bittiset avaimet ja antamalla jokaiselle tukiasemalla sama WEP-avain, joka yhdistetään tukiaseman MAC-osoitteen kanssa tukiasemakohtaisen avaimen luomiseksi. Tämä lisää avainyhdistelmien määrää, ja jokainen kehys salataan eri avaimella. TKIP:ssä tukiasema voi vaihtaa saamansa WEP-avaimen väliajoin, esimerkiksi joka 10000. kehyksen jälkeen. Lisäksi alustusvektorin pituus kasvatettiin 48 bittiin, ja tietojen väärentäminen estetään MIC:llä (Message Integrity Checksum), jossa kahdeksalla tavulla tarkistetaan, onko kehys muuttunut. TKIP voitiin ottaa laitteissa käyttöön pelkällä ohjelmistopäivityksellä ja samalla säilyttää WEP-yhteensopivuus. (Bardwell & Akin 2005, 428-430.)

3.2.3 802.1X ja EAP

Lähiverkon käyttäjien tunnistamiseen on kehitetty 802.1X-standardi. Siinä kytkimen portit vaativat käyttäjää tunnistautumaan ennen kuin liikenne sallitaan. Standardi käyttää EAP-protokollaa (Extensible Authentication Protocol), jossa on monta erilaista tapaa käyttäjän tunnistukseen, kuten käyttäjätunnus/salasana-pari ja SSL-varmenne (Secure Sockets Layer). Langattomissa verkoissa 802.1X otettiin käyttöön niin, että WLAN-tukiasema muodostaa jokaiselle käyttäjälle oman virtuaalisen portin. Käyttäjätunnistuksen taustapalveluna käytetään tyypillisesti RADIUS-palvelinta (Remote Authentication Dial In User Service) ja jonkin tyyppistä käyttäjätietokantaa. Langattomaan verkkoon voidaan tämän avulla kirjautua samalla tunnuksella kuin muihinkin organisaation tarjoamiin palveluihin. Tunnistautumisessa on kolme osapuolta: verkkoon haluava laite, tunnistautumisliikenteen välittäjä (yleensä tukiasema tai kytkin) ja tunnistautumispalvelin (RADIUS). (Bardwell & Akin 2005, 431-432.)

3.2.4 WPA

Langattoman verkon tietoturvan parantamiseksi edelleen perustettiin vuonna 2001 komitea kehittämään 802.11i-standardia. Sen julkaisua odoteltaessa WLAN-laitteiden yhteensopivuudesta huolehtiva Wi-Fi Alliance julkaisi TKIP:tä ja 802.1X:ää tukevan WPA-standardin (Wi-Fi Protected Access). Kyseessä oli 802.11i-standardin esiversio, jolla haluttiin valmistaa, että eri valmistajien laitteet olisivat yhteensopivia. Tämä nopeutti vahvempien tietoturvaominaisuuksien käyttöönottoa markkinoilla. (Bardwell & Akin 2005, 438.)

WPA:ssa on käytössä kaksi erilaista tunnistautumis- ja avaimenhallintatapaa. Ensimmäisessä käytetään RADIUS-palvelinta ja toisessa esijaettua avainta (Pre-Shared Key, PSK). WPA-PSK kehitettiin kotikäyttöä ja pieniä toimistoja ajatellen, joissa ei haluta tai tarvita RADIUS-palvelinta. Siinä käytetään päätelaitteiden tunnistukseen tukiasemaan esimääriteltyä merkkijonoa, joka jaetaan kaikille verkkoon haluaville laitteille. Samaa merkkijonoa ei kuitenkaan käytetä liikenteen salaamiseen, vaan EAP-protokollaa käytetään määrittämään jokaiselle päätelaitteelle oma WEP-avain. Samalla tavalla toimitaan RADIUS-palvelimen kanssa, mutta verkkoon kirjaudutaan esimerkiksi käyttäjätunnuk-

sen ja salasanan avulla, jolloin käyttäjät voidaan erottaa toisistaan, eikä avainta tarvitse vaihtaa esimerkiksi työntekijöiden vaihtuessa. (Bardwell & Akin 2005, 439-440.)

Valmis 802.11i-standardi, joka tunnetaan myös nimellä WPA2, julkaistiin vuonna 2004. Siinä otettiin käyttöön AES-koodaus (Advanced Encryption Standard) ja CCMP-protokolla (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), joka määrittelee, kuinka AES:a käytetään liikenteen salaukseen. AES on paljon vahvempi algoritmi kuin tähän asti käytössä ollut RC4. (Bardwell & Akin 2005, 440-441.) Koska WPA2+AES on tällä hetkellä vahvin mahdollinen WLAN-verkkojen salaustapa, sitä suositellaan käytettävän aina kun mahdollista.

3.3 Roaming

Kun alueella on vain yksi langattoman verkon tukiasema, käyttäjän päätelaite pysyy verkossa niin kauan kuin pysytään sen kantaman sisäpuolella. Jos samaa SSID:tä tarjoavia tukiasemia on enemmän, niiden peittoalueet ovat yleensä hieman päällekkäin ja päätelaite liittyy niistä siihen, jonka signaali kuuluu parhaiten. Päätelaitteen siirtyessä paikasta toiseen, tukiasemien signaalien tehosuhteet todennäköisesti muuttuvat ja päätelaite vaihtaa toiseen tukiasemaan. Tällöin hyödynnetään WLAN-tekniikan tarjoamaa roaming-palvelua, joka mahdollistaa tukiaseman vaihtamisen ilman tiedonsiirron katkeamista (Puska 2005, 138).

IEEE:n standardi 802.11r määrittelee nopean tukiaseman vaihdon, joka saa kestää enintään 50 millisekuntia yhteyden häiriintymättä. 802.11r:n avulla päätelaite tunnistautuu uuteen tukiasemaan ja varaa tarvitsemansa resurssit ennen koko yhteyden siirtämistä. Uuden tukiaseman valintaan vaikuttaa 802.11k-standardi, jolla kerätään tietoa parhaan tukiaseman valitsemiseksi. Normaalisti valitaan tukiasema, jonka signaali on vahvin, mutta se ei välttämättä ole aina paras vaihtoehto tukiaseman käyttäjämäärän ja käyttäjien sijainnin perusteella. Standardin avulla saadaan jaettua kuormaa tukiasemien kesken. (About.com Encyclopedia.)

3.4 WLAN-järjestelmät

Langaton lähiverkko voi perustua autonomisiin tai kontrolleripohjaisiin tukiasemiin. Autonomiset tukiasemat toimivat nimensä mukaisesti itsenäisesti ilman erillistä ohjainta, mutta niitä voidaan silti hallita, eli valvoa ja muuttaa asetuksia, keskitetysti. Tukiasemat eivät vaihda tietoa keskenään, vaan ne tekevät päätökset muun muassa lähetystehosta ja kanavasta itse. Myöskään käyttäjien tasainen jako tukiasemien kesken ei ole mahdollista, sillä tukiasema ei voi tietää, kuuluuko lähellä oleva tukiasema samaan verkkoon.

Kontrollerilla puolestaan on kuva koko verkosta tukiasemien kautta, ja se valvoo sekä niiden että verkon tilaa. Juuri se, että yksi laite tuntee verkon peittoalueen radiosignaaliympäristön ja pystyy mukauttamaan koko verkon sen mukaisesti, tekee kontrolleripohjaisesta verkosta ylivoimaisen autonomisiin tukiasemiin verrattuna. Kontrolleri hoitaa myös käyttäjien 802.1X/EAP-tunnistautumisen ja kuormanjaon sekä toimii tarvittaessa palomuurina. Tukiasemissa ei siis tarvita yhtä paljon elektroniikkaa autonomisiin tukiasemiin verrattuna. WLAN-verkkojen liikennettä ei nykyään ole pakko kierrättää kontrollerin kautta, joten se ei muodostu pullonkaulaksi ja aiheuta hidastelua vilkasliikenteisissä verkoissa. Langattoman verkon ja tukiasemien toiminta on kuitenkin tietyissä määrin riippuvainen yhdestä laitteesta, mikä on kontrolleripohjaisen järjestelmän huono puoli.

Verkkolaitevalmistaja Aerohive on kehittänyt näiden kahden arkkitehtuurin väliin kuuluvan WLAN-järjestelmän. Siinä ei ole keskitettyä ohjainta, mutta tukiasemat kommunikoivat keskenään sitä varten tehdyn protokollan avulla. Tekniikka tarjoaa siis kontrolleripohjaisen verkon hyvät puolet yhdistettynä siihen, että verkon toiminta ei ole riippuvainen yhdestä laitteesta. (Controller-less WLAN Architecture.) Tekniikka on uusi, eikä vastaavanlaista ole tarjolla muilla valmistajilla, joten kontrolleripohjaiset verkot tulevat olemaan johtavassa asemassa vielä vuosia. Autonomisia tukiasemia ei kuitenkaan kannata enää hankkia organisaatiotason verkkoja rakennettaessa, joten Aerohiven tekniikka tarjoaa varteenotettavan ja kustannustehokkaan vaihtoehdon uutta järjestelmää hankittaessa.

4 TAMKIN VANHA WLAN-VERKKO

Tampereen ammattikorkeakoulu (TAMK) sai nykyisen muotonsa, kun se ja Pirkanmaan ammattikorkeakoulu (PIRAMK) yhdistyivät vuoden 2010 alussa. Tässä työssä käytetään termejä ”entinen TAMK” ja ”entinen PIRAMK” viittaamaan kuhunkin kouluun ennen yhdistymistä. Molemmilla oli käytössä erilaiseen arkkitehtuuriin perustuva WLAN-järjestelmä.

4.1 Kaksi järjestelmää

Entisen TAMKin WLAN-tukiasemat olivat Proxim-merkkisiä ja malliltaan ORiNOCO AP-700 ja AP-4000. Ensin mainittu sisältää 2,4 GHz:n radion, ja se tukee 802.11b/g-standardeja. AP-4000:ssa on radio myös 5 GHz:n taajuusalueelle, joten se tukee lisäksi 802.11a-standardia. Ensimmäiset tukiasemat olivat vuodelta 2004 ja uusimmatkin jo vuodelta 2006. Ne ovat autonomisia, eikä niillä ollut keskitettyä hallintaa, eli muutokset täytyi tehdä jokaiseen tukiasemaan erikseen. Niiden tilaa valvottiin valmistajariippumattomalla WiFi Manager -ohjelmalla, jonka tuki on loppunut toukokuussa 2011.

Entisen PIRAMKin WLAN-järjestelmä perustui Hewlett Packardin (HP) WESM-kontrolleriin (Wireless Edge Services Module), joka nimensä mukaisesti on lisämoduuli sitä tukeviin HP:n kytkimiin. Se ohjaa käytössä olleita Radio Port 210 -mallin tukiasemia, jotka tukevat 802.11b/g-standardeja 2,4 GHz:n taajuusalueella. Ne eivät siis toimi ilman yhteyttä kontrolleriin, jolla myös asetukset jaetaan keskitetysti tukiasemille. WESM:n ominaisuuksiin kuuluu erityisen yleislähetysalueen luominen tukiasemia varten, minkä ansiosta eri WLAN-verkkojen VLAN-määritykset tehdään vain siihen kytkimeen, johon moduuli on asennettu. Tämä tosin tarkoittaa sitä, että WLAN-verkkojen liikenne kulkee kontrollerin kautta, mikä voi aiheuttaa hidastelua vilkasliikenteisessä verkossa.

Proxim-tukiasemien (65 kappaletta) peittoalue kattoi suurimman osan entisen TAMKin tiloista, joihin kuuluu kymmenen rakennusta Kuntokadun ja yksi kuusikerroksinen rakennus Finlaysonin kampusalueella. Suurin puute oli parikymmentä teorialuokkaa käsit-

tävässä viisikerroksisessa rakennuksessa, jossa ei ollut yhtään tukiasemaa. Lisäksi yhdessä rakennuksessa tukiasemat oli sijoitettu teletiloihin, mikä ei ollut optimaalinen ratkaisu, sillä signaalit pääsivät helposti kulkeutumaan metallisia kaapelitikkaita pitkin kerroksesta toiseen aiheuttaen häiriöitä muiden kerrosten tukiasemien signaaleihin. Tukiasemien toimintavarmuus oli alkanut laskea, sillä osa tukiasemista käynnistyi ajoittain uudelleen, mikä aiheutti aina lyhyen katkon palvelun toimintaan kunkin tukiaseman peittoalueella.

Entisessä PIRAMKissa oli 23 tukiasemalla katettu niin suuri alue kuin mahdollista. Tukiasemien pienen määrän takia kaikissa seitsemässä toimipisteessä oli katettu vain välttämättömimmät tilat. Niiden sijoittelu oli rajoittunut verkkorasioiden lähettyville, joten aina ei ollut voitu valita parasta sijoituspaikkaa. Verkon peittoalueen kasvattamista oli erityisesti toivottu Ikaalisten, Mänttä-Vilppulan ja Virtain toimipisteissä, joissa oli vain muutama tukiasema. HP:n tukiasemissa ei ollut esiintynyt toimivuusongelmia, mutta ne olivat riippuvaisia WESM-kontrollerista, joka hajotessaan tekisi kaikki tukiasemat toimintakyvyttömiksi.

4.2 Langaton vierailijaverkko

Entisen TAMKin langaton vierailijaverkko tarjosi yhteyden Internetiin, ja se oli vahvasti suojattu, eli päätelaitteen ominaisuuksista riippuen käytettiin WPA+TKIP- tai WPA2+AES-tekniikkaa. Käyttäjien tunnistukseen käytettiin 802.1X/EAP-protokollaa ja RADIUS-palvelinta, joka hakee käyttäjätiedot TAMKin LDAP-hakemistosta (Lightweight Directory Access Protocol). Vierailijaverkko oli tarkoitettu henkilökunnalle, opiskelijoille ja vierailijoille. Vierailijaverkko-nimitys tulee siitä, että verkko on eristetty TAMKin sisäverkosta. Tiettyjä sisäverkon palveluita (esimerkiksi levyjaot) voi kuitenkin käyttää Citrix-etäyhteyden avulla. Henkilökunta ja opiskelijat voivat kirjautua verkkoon samoilla tunnuksilla kuin esimerkiksi koulun tietokoneille. IT-tuella oli käytössään komentorivipohjainen työkalu, jolla aktivoitiin LDAP-hakemistossa olevia ja oikeuksiltaan rajoitettuja WLAN-tunnuksia vierailijoiden käyttöön.

Entisessä PIRAMKissa ei ole ollut varsinaista vierailijaverkkoa, mutta erilaisia tapahtumia varten oli tarvittaessa toteutettu väliaikainen verkko tapahtuman osallistujille.

Henkilökunta ja opiskelijat olivat kuitenkin voineet käyttää eduroam-verkkoa, jota myös TAMKissa tarjotaan. Kyseessä on kansainvälinen langaton verkko, jota korkeakoulujen henkilökunta ja opiskelijat voivat käyttää tunnuksillaan missä tahansa korkeakoulussa, jossa verkkoa tarjotaan.

TAMKin vierailijaverkko ei toteutustapansa takia ollut vielä nykyäänkään käyttäjäystävällinen, sillä erityisesti Windows-käyttöjärjestelmä ei ollut osannut tunnistaa verkon asetuksia oikein. Verkkoon ei siis saanut yhteyttä valitsemalla sen Windowsin langattomien verkkojen listasta ja kirjoittamalla käyttäjätunnuksen. Käyttäjille on jaettu monisivuista ohjetta, jossa neuvotaan usean valikon takaa asetettavat asetukset. IT-tuessa oli ollut tapauksia, joissa oikeilla asetuksillakaan ei ollut aina saanut yhteyttä, tai asetukset oli jouduttu määrittelemään useaan kertaan ennen yhteyden muodostumista. Oman ongelmaryhmänsä muodostivat toimialueelle liitetyt tietokoneet, jotka automaattisesti yrittivät tunnistautua verkkoon vääränmuotoisella käyttäjätunnuksella. Puhelimilla, tablettietokoneilla sekä OS X:ää tai Linuxia käyttävillä kannettavilla tietokoneilla tilanne oli ollut parempi, mutta niilläkään langattoman verkon käyttö ei aina ollut ongelmatonta.

5 TAMKIN UUSI WLAN-VERKKO

5.1 Suunnittelu

Yhdistyneen TAMKin WLAN-verkon uudistuksen lähtökohtana oli kaksi asiaa: vanhojen tukiasemien korvaus uusilla ja vierailijaverkkokonseptin uudistaminen. Molemmat auttavat palvelun laadun parantamisessa. Ne jaettiin omiin vaiheisiinsa, sillä WLAN-järjestelmän kilpailutus aloitettiin vasta kun uusi vierailijaverkkokonsepti oli testikäytössä. Myös verkon ylläpito helpottuu keskitetyn hallinnan ja tekniikan yhtenäistymisen ansiosta. Samalla tarkastetaan kaikki langattomaan verkkoon liittyvä dokumentaatio. Suunnitelma kattoi kaikki yhdeksän toimipistettä, jotka sijaitsevat Tampereen lisäksi Ikaalisissa, Mänttä-Vilppulassa ja Virroilla.

Varsinkin Ikaalisissa, Mänttä-Vilppulassa ja Virroilla WLAN-verkon peittoaluetta haluttiin kasvattaa. Esimerkiksi Mänttä-Vilppulassa TAMK on antanut osalle opiskelijoista kannettavan tietokoneen, jota voi paremmin hyödyntää opiskelussa langattoman verkon avulla. Tampereella ongelmana oli entisen TAMKin tukiasemien heikentynyt toimintavarmuus. Vaikka suurin osa tukiasemien asennusta oli vanhojen korvaamista uusilla, koko verkko rakennettiin alusta asti uudelleen ja yhdenkään vanhan tukiaseman senhetkisen asennuspaikan ei oletettu olevan paras mahdollinen. Kolmas hyöty on koko TAMKin laajuisen langattoman vierailijaverkon käyttöönotto, jolloin palvelu on samanlainen toimipisteestä riippumatta. Verkon piti myös olla helppokäyttöinen, ja vierailijatunnuksia piti pystyä tekemään muutkin kuin IT-tuki, esimerkiksi infopisteiden ja kirjastojen työntekijät.

5.1.1 Vanhan ja uuden yhteensovitus

Uusien tukiasemien käyttöönoton Ikaalisissa, Mänttä-Vilppulassa ja Virroilla esti se, että toimipisteet Tampereen verkkoon yhdistäviin yhteyksiin ei saatu tarvittavia VLAN-määrityksiä palveluntarjoajalta. Entisen PIRAMKin WESM-järjestelmän käyttöikää päätettiin jatkaa, sillä sen toimintavarmuudessa ei ollut lähes ollenkaan huomautettavaa. Järjestelmän tukiasemilla saatiin katettua kyseisten toimipisteiden kaikki tilat. Sijoitus-

paikkoja valittaessa otettiin huomioon, että ne tukevat vain 802.11b- ja 802.11g-standardia. Koska uudelleensijoitettavissa oli parikymmentä tukiasemaa, voitiin niiden asennuspaikat valita niin, että joka tilaan pystytään tarjoamaan riittävä signaalitaso ja verkon nopeus. WESM-kontrollerilla tukiasemia valvotaan ja hallitaan keskitetysti.

Tähän asti ilman langatonta verkkoa olleeseen rakennukseen saatiin verkko toteutettua, kun ensimmäiseksi toimitetuilla uusilla tukiasemilla oli korvattu muualla TAMKissa olleita vanhoja tukiasemia. Kuudella AP-700-tukiasemalla katettiin rakennuksen kolme ylintä kerrosta, joissa siis sijaitsee parikymmentä teorialuokkaa. Tukiasemien sijoituspaikat valittiin site survey -mittauksen avulla niin, että jokaiseen kerrokseen asetettiin vuorotellen kaksi testitukiasemaa jakamaan kerros kahteen osaan, minkä jälkeen kuuluvuusalue mitattiin. Mittauksissa havaittiin, että signaali vaimenee liikaa kerrosten välillä, eli tukiasemat voisivat kattaa riittävästi vain oman kerroksensa. Koska vanhoja tukiasemia oli koko ajan vapautumassa lisää, uusien tukiasemien korvatessa niitä, voitiin joka kerrokseen asentaa tarvittavat kaksi tukiasemaa. Tukiasemat liitettiin samaan hallintaverkkoon kuin uudet tukiasemat, ja valvontaa hoitava WiFi Manager -sovellus siirrettiin käytöstä poistettavalta palvelimelta virtuaalipalvelinympäristöön. Rakennus on menossa remonttiin tänä vuonna, joten sinne asennetaan uuden järjestelmän tukiasemat remontin valmistuttua.

5.1.2 WLAN-sisäverkko

Langattomien lähiverkkojen nopeuden kasvaessa niitä voidaan alkaa hyödyntää kaapeliyhteyksien tilalla. Tällöin vierailijaverkon rinnalle tarjottaisiin toinen verkko, josta pääsee suoraan TAMKin sisäverkkoon samoin kuin kaapelin kauttakin. WLAN-sisäverkko olisi tarkoitettu koulun omille laitteille, joiden tietoturvan taso voidaan taata. Verkko toteutettaisiin vahvasti salattuna ja MAC-osoitesuodatuksella. TAMKissa WLAN-sisäverkkoa on kokeiltu muutamassa laboratorioluokassa, joihin koulu on ostanut kannettavat tietokoneet ja joissa kaapeliyhteyden käyttäminen ei olisi mahdollista koneiden liikuttelun takia. Esimerkiksi katosta riippuvat kaapelit olisivat myös työskentelyn tiellä. Samoin on toimittu eräässä opiskelijoiden ryhmätyötilassa, jossa huoneisiin ei vielä ole vedetty verkkokaapeleita. Vaihtoehdot verkon tietoturvan toteuttamiseksi

ovat WPA2+AES tai uusi tekniikka nimeltä Dynamic PSK, joka ominaisuuksiensa puolesta tarjoaa helppokäyttöisen ja vahvasti suojatun yhteyden verkkoon.

Dynamic PSK käyttää nimensä mukaisesti esijaettuja salausavaimia, mutta tietoturvaa lisää se, että jokaiselle laitteelle luodaan automaattisesti oma avain, jolle määritetään voimassaoloaika. Helppokäyttöisyys toteutetaan joko langallisessa tai avaimen luontia varten tehdyssä langattomassa verkossa avautuvalla www-sivulla, jossa käyttäjä kirjautuu henkilökohtaisella tunnuksellaan. Kirjautumisen jälkeen laitteelle luodaan oma salausavain, minkä jälkeen se ja muut verkon asetukset ladataan automaattisesti laitteeseen. Tämän jälkeen laitteella voidaan käyttää WLAN-sisäverkkoa ilman hankalia asetusmäärittelyitä ja tietohallinnon apua. MAC-osoitesuodatuksella voidaan sallia vain haluttujen laitteiden pääsy verkkoon, ja myös käyttäjätunnusten perusteella tapahtuvalla suodatuksella voidaan rakentaa lisäturvaa. Sallittujen laitteiden MAC-osoitteet voidaan kopioida olemassa olevasta laitetietokannasta RADIUS-palvelimelle, jolloin pääsylistoja ei tarvitse ylläpitää käsin.

Jos salausavaimen voimassaolo loppuu, käyttäjän täytyy vain kirjautua verkkoon uudelleen. Jokainen avain on sidottu laitteeseen, jolle se on luotu, joten avaimen paljastuminen ei ole läheskään yhtä suuri riski kuin normaaleja esijaettuja avaimia käyttävässä verkossa. Jos verkkoon tunnistautunut laite varastetaan tai työntekijän työsuhde päättyy, muille käyttäjille ei aiheudu ongelmia, eikä avaimia tarvitse vaihtaa. Verkon ylläpidon täytyy vain poistaa kyseiselle laitteelle automaattisesti muodostettu salausavain tietokannasta, jolloin sitä ei voi enää käyttää, eikä laitteella saa enää WLAN-sisäverkkoon yhteyttä.

5.2 Tekniikka ja laitteet

Järjestelmän toimittamisesta järjestetyn kilpailutuksen voitti Ruckus Wireless -nimisen yhtiön laitteisiin pohjautunut tarjous. Valmistaja ei ollut entuudestaan tuttu kenellekään projektiin kuuluneista, mutta tarjoukseen tutustumisen aikana tuli selväksi, että puutteita ei ole ja tekniikka pystyy kilpailemaan suurempien valmistajien kanssa. Kenelläkään muulla ei esimerkiksi ollut vastaavanlaista antennitekniikkaa tukiasemissaan.

5.2.1 WLAN-kontrolleri

Uuden järjestelmän toiminta perustuu WLAN-kontrolleriin, jonka malli on ZoneDirector 3000. Kyseessä on laitekehikkoon asennettava palvelinlaite, jossa on Ruckus Wirelessin kehittämä ohjelmisto. Siihen saa jopa 500 tukiaseman lisenssin, joten laajennusvaraa tulevaisuutta ajatellen on riittävästi.

Kontrollerin asennus ja tukiasemien liittäminen siihen oli helppoa. Kontrollerille annettiin vain kiinteä IP-osoite WLAN-laitteille varatusta hallintaverkosta ja verkkonimi, minkä jälkeen tukiasemia voitiin alkaa ottaa käyttöön. Kun tukiasema kytketään hallintaverkkoon, se saa kontrollerissa käyttöön otetulta DHCP-palvelimelta (Dynamic Host Control Protocol) automaattisesti IP-osoitteen, joka voidaan myöhemmin vaihtaa kiinteäksi. Tukiasema voidaan tarvittaessa siirtää toiseen aliverkkoon, sillä se löytää kontrollerin myös IP-osoitteen perusteella. Kontrollerin löydettyään tukiasema tarkistaa, täsmääkö sen maakoodi ja ohjelmistoversio kontrolleriin. Jos ei, maakoodi vaihdetaan ja ohjelmisto päivitetään automaattisesti. Tämän jälkeen tukiasema voidaan määrittää mainostamaan haluttuja verkkoja ja ottaa käyttöön.

Radiotien käytön optimointi toteutetaan ohjaamalla käyttäjät 5 GHz:n taajuusalueelle, jos ne sitä tukevat, jakamalla kuormaa tukiasemien kesken ja takaamalla jokaiselle käyttäjälle yhtä iso osa tiedonsiirtoaikaa. WLAN-verkko toimii aina hitaimman mukaan, joten muille tulee taata sama aika siirtää tietoa kuin hitaimmalle. Mitä parempi signaalin teho ja suorituskyky, sitä enemmän käyttäjä ehtii siirtää tietoa. Näin nopeita yhteyksiä käyttävien tiedonsiirtonopeus ei hidastu liikaa hitaampia odotellessa.

Jos kontrollerin yhteys verkkoon katkeaa, käyttäjät eivät pysty kirjautumaan 802.1X/EAP-tunnistautumista käyttäviin verkkoihin, eikä tukiasemia voida valvoa ja hallita. WLAN-verkkojen liikennettä ei kuitenkaan tunneloida kontrollerin kautta, joten vikatilanteen sattuessa verkossa jo olevien käyttäjien tiedonsiirto ei keskeydy. Käyttäjän siirtyminen tukiasemasta toiseen ei kuitenkaan ole mahdollista, koska se vaatii aina uuden tunnistautumisen. Koska kontrolleri on tärkeä verkon toiminnan kannalta, se voidaan kahdentaa. Tukiasemat siirtyvät automaattisesti varalaitteen hallintaan, jos yhteys ensisijaiseen kontrolleriin katkeaa. Ominaisuuden ansiosta verkon toimintakyky ei laske vakavassakaan häiriötilanteessa. Laitteille on annettu NBD-vaihtotakuu (Next Business

Day), joten toista kontrolleria ei ainakaan vielä lisätty hankintalistalle. Tilanne voi muuttua, jos langatonta verkkoa aletaan hyödyntää muuhun kuin vierailijaverkkoon.

5.2.2 Tukiasemat

Järjestelmän tukiasemat ovat malliltaan ZoneFlex 7363 (kuvio 12). Niissä on kaksi radiota (2,4 GHz ja 5 GHz) ja 14 antennielementtiä, ja ne pystyvät siirtämään kaksi tietovirtaa kumpaankin suuntaan (2x2 MIMO). Yhden radion teoreettinen siirtonopeus on 300 Mbps ja signaalivahvistukseksi ilmoitetaan 4 dBi. Tukiasemissa on lisäksi PoE-tuki (Power over Ethernet), mikä helpottaa asennuspaikan valintaa. Kontrolleri hoitaa tukiasemien kanavanvaihdot ja lähetystehon muuttamisen.

KUVIO 12. Tukiaseman asennuspaikka katonrajassa

Tukiasemat käyttävät Ruckus Wirelessin patentoitua adaptiivista antenniteknologiaa nimeltä BeamFlex. Ne muokkaavat antennien suuntakuviota käyttäjän tiedonsiirtonopeuden perusteella. Käytettävä kuvio valitaan ZoneFlex 7363 -tukiaseman tapauksessa reilun 300 vaihtoehdon joukosta. Tukiasema kokeilee vaihtoehtoja, joilla käyttäjälle

saataisiin paras tiedonsiirtonopeus, eli signaalin voimakkuutta ei siis oteta huomioon. Suuntakuvio valitaan pakettikohtaisesti, eli jos käyttäjä liikkuu tai RF-ympäristön olosuhteet muuttuvat, suuntakuvio mukautuu siihen. Ominaisuuden ansiosta suurin osa lähetystehosta saadaan suunnattua käyttäjää kohti, mikä parantaa tiedonsiirron nopeutta ja häiriönsietokykyä. Toisin kuin kappaleessa 3.1.3 mainittu 802.11n-standardin signaalien vaihe-eroon perustuva keilanmuodostus, Ruckus Wireless käyttää useita antennielementtejä halutun suuntakuvion muodostukseen. Kumpaankin yhtäaikaiseen tietovirtaan voidaan käyttää omaa kuviota, ja tekniikka toimii myös vanhemmilla WLAN-standardeilla, eli käyttäjän päätelaitteessa ei tarvitse olla mitään erityistä tukea.

5.3 Kuuluvuusmittaukset

Vanhan WLAN-järjestelmän peittoalueen selvittämiseksi suoritettiin kuuluvuusmittaus, jolla saatiin selvitettyä alueet, joissa langattoman verkon signaali kuuluu heikosti tai ei ollenkaan. Kuntokadun iso kampusalue kartoitettiin kokonaan, sillä vanhojen tukiasemien sijainnin perusteella peittoalueen pitäisi olla erittäin kattava. Lisäksi siellä on suurin osa verkon käyttäjistä. Pohjapiirustuksia ei läheskään kaikista toimipisteistä ollut saatavilla, mutta koska osassa niissä oli ennen uudistusta vain muutama tukiasema, peittoalueen selvitys kokonaisvaltaisella site survey -mittauksella ei edes ollut tarpeen. Joissakin toimipisteissä piti ottaa huomioon mahdollisten muiden toimijoiden tukiasemat eipäällekkäisten kanavien takia.

Uusien ja uudelleensijoitettavien tukiasemien asennuspaikat kartoitettiin asentamalla testitukiasema valittuun kohtaan ja mittaamalla sen signaalitasot alueilla, joissa sen haluttiin tai oletettiin kuuluvan. Tarvittaessa voitiin asentaa myös kaksi tukiasemaa testejä varten, jos piti mitata niiden yhteinen peittoalue. Mittausten perusteella paikka todettiin hyväksi tai tukiasema siirrettiin toiseen paikkaan. Toimipisteissä, joissa verkkokaapelin vetäminen lähimmästä teletilasta tukiasemalle oli mahdollista, verkkorasioiden sijainnin ei annettu vaikuttaa asennuspaikkaan. Kaapelia kului projektin aikana useita satoja metrejä. Virta syötetään tukiasemille verkkokaapelia pitkin PoE-tekniikan avulla, joten asennuspaikan lähellä ei tarvitse olla sähkörasioita.

Site survey -mittauksia tehtiin myös uuden järjestelmän asennuksen jälkeen, ja tuloksia verrattiin vanhan järjestelmän tilanteeseen. Esimerkiksi ongelma-alueeksi tiedetyn B-siiven kuuluvuuskartoissa (liitteet 1 ja 3) näkyy, kuinka signaaleissa esiintyy suuria vaihteluita. Tiettyinä hetkinä ja tietyissä paikoissa signaali kuuluu hyvin, mutta tilanne ei välttämättä ole jatkuva. Tukiasemien signaalit kuuluvat toistensa päälle, kun toisen kerroksen tukiaseman signaali kantaa metallirakenteita pitkin jopa kuudenteen kerrokseen. Uuden järjestelmän tukiasemat sijoitettiin B-siiven käytäville parempiin paikkoihin. B6-kerroksen peittoalue vanhalla järjestelmällä on liitteessä 1 ja uudella järjestelmällä liitteessä 2. Kerros on uusilla tukiasemilla katettu kokonaan, ja RF-ympäristö on paljon rauhallisempi. Sama toistuu jokaisessa kerroksessa. Toisena esimerkkinä B4-kerroksen peittoalue vanhalla järjestelmällä (liite 3) ja uudella järjestelmällä (liite 4).

5.4 Selaintunnistaumiseen perustuva vierailijaverkko

TAMKin tietohallinto oli päättänyt muuttaa vierailijaverkon konseptia aiempaa käyttäjäystävällisempään suuntaan. Uusi vierailijaverkko on salaamaton ja siihen tunnistaudutaan WWW-selaimeen avautuvalla sivulla. Kaikki verkon liikenne kulkee siis oletusarvoisesti selkokielisenä, ja sitä voidaan salakuunnella, mutta esimerkiksi WWW-palvelujen kirjautumissivut on pääsääntöisesti suojattu SSL-salauksella, jolloin käyttäjätietoja ei saa selville. Samoin useat palveluntarjoajat antavat käyttää salattuja protokollia muun muassa sähköpostin kanssa. Käyttäjiä täytyy valistaa verkon käytön mahdollisista vaaroista. Henkilökunnalle ja opiskelijoille on jatkossakin tarjolla myös salattu eduroam-verkko.

Selaintunnistautuminen on toteutettu verkon yhdyskäytäväpalvelimessa, jonka palomuuri estää kunkin päätelaitteen kaiken liikenteen Internetiin ennen kirjautumista. Käyttäjän yrittäessä mille tahansa WWW-sivulle, selain ohjataan automaattisesti kirjautumissivulle. Kirjautumisen voi jälkeen aloittaa surffailun tai esimerkiksi SSH-istunnon (Secure Shell). Kirjautumissivu lähettää lankaverkkoa pitkin tunnistautumispyynnön TAMKin RADIUS-palvelimelle, eli se käyttää samaa protokollaa käyttäjien tunnistautumiseen kuin vanha vierailijaverkkokin. Tietoturva- ja muita asetuksia ei kuitenkaan tarvitse määrittää, vaan riittää että yhdistää TAMK-GUEST-nimiseen verkkoon ja avaa selaimen. Palomuurilla on lisäksi mahdollisuus sallia pääsy tiettyihin palveluihin ilman

langattomaan verkkoon kirjautumista. Esimerkiksi TAMKin intranet, sähköposti ja www-sivusto valittiin tällaisiksi palveluiksi.

Uuden vierailijaverkon myötä myös vierailijatunnukset muuttuivat erilaisiksi. Tätä varten koodasin PHP:llä (Hypertext Preprocessor) ohjelman, joka käyttää vierailijaverkkojärjestelmän toimittajan API:a (Application Progamming Interface) WWW-sivulla, jossa kahdella hiiren klikkauksella saa tunnuksen luotua ja paperin tulostettua. Helppokäyttöisyyden ansiosta vierailijatunnuksien teko-oikeudet voitiin antaa myös esimerkiksi infopisteiden ja kirjastojen työntekijöille. Näin vierailijoiden ei tarvitse etsiä paikallista IT-lähitukea tunnuksen saadakseen, mikä osaltaan vähentää myös IT-tuen työtaakkaa.

6 POHDINTA

Langattoman lähiverkon uudistaminen tuli ajankohtaiseksi Tampereen ammattikorkeakoulussa, kun yhdistyneellä koululla ei ollut yhtenäistä vierailijaverkkopalvelua ja laitteet alkoivat olla liian vanhoja tarjotakseen riittävää palvelun laatua, jota osaltaan huononsi myös entisessä TAMKissa käytössä olleen vierailijaverkon huono saavutettavuus. Kokonaan uuden järjestelmän hankinta antoi mahdollisuuden aloittaa langattoman verkon rakentaminen alusta asti uudelleen, ja jo pelkästään tukiasemien uudelleensijoittelulla saatiin parannusta aikaan. Uusi vierailijaverkkokonsepti tarjoaa käyttäjille helppokäyttöisen tien Internetiin, jolloin verkkoa voi hyödyntää yhä useampi. Tekniikan uusiminen mahdollistaa tulevaisuudessa langattoman verkon hyödyntämisen myös muussa kuin vierailijaverkkokäytössä. Yksi odotettu tulevaisuuden sovellus tulee olemaan WLAN-sisäverkko, kun kannettavien päätelaitteiden määrä lisääntyy ja niitä toivottavasti aletaan hyödyntää opetuksessa enemmän. Työskentely ei olisi enää ole sidottu esimerkiksi tiettyyn tietokoneluokkaan.

Tärkeimpänä tavoitteena oli parantaa langattoman lähiverkon palvelun laatua sekä tekniikan että helppokäyttöisyyden osalta kaikissa TAMKin toimipisteissä. Tässä onnistuttiin, sillä uuden järjestelmän asennuksen jälkeen suoritettujen site survey -mittausten mukaan parannusta tapahtui kaikkialla. Käyttöön otettiin 802.11n-standardia tukevat tukiasemat, joiden tiedonsiirtonopeus riittää raskaampiinkin sovelluksiin. Tämä on osaltaan laitteiden valmistajan adaptiivisen antennitekniikan ansiota, mutta muissa kuin Tampereen toimipisteissä peittoaluetta ja verkon nopeutta keskityttiin parantamaan lisäämällä tukiasemien määrää ja sijoittamalla ne optimaalisiin paikkoihin. Verkkoa valvotaan ja asetuksia muutetaan kahden kontrollerin hallintasivun kautta, mutta tulevaisuudessa on tarkoitus saada ajettua myös nyt käyttöön jäänyt HP-järjestelmä alas. Uuden järjestelmän kontrolleri pitää huolen siitä, että tukiasemat toimivat aina RF-ympäristöön sopivalla kanavalla ja lähetysteholla. Kuluvan vuoden aikana päästään eroon viimeisistäkin entisen TAMKin tukiasemista, joiden hallinta on työlästä.

Uusi vierailijaverkko on mahdollistanut WLAN-verkon mahdollisimman tehokkaan hyödyntämisen kaikissa toimipisteissä. Verkkoon pääsee nyt kaikenlaisilla laitteilla, eikä monimutkaisia asetuksia tarvitse enää määrittää. Uudistus on otettu hyvin vastaan

TAMKissa, sillä verkossa on päivittäin kirjautuneena keskimäärin 250 käyttäjää samanaikaisesti, kun aikaisemmin jäätiin reiluun sataan käyttäjään. Koska vierailijatunnuksia saa aiempaa useammasta paikasta, kuten kirjastoista ja infopisteistä, vierailijatkin pääsevät verkkoon aiempaa helpommin. IT-tuessa avun tarvitsijoiden määrä on vähentynyt huomattavasti, ja ongelmat liittyvät nykyään lähinnä siihen, että verkkoon haluavassa koneessa ei ole automaattinen IP-asetusten haku päällä. Tämän saa helposti korjattua ja neuvottua puhelimessakin.

Uudella järjestelmällä TAMKin langaton verkko toiminee vähintään yhtä kauan kuin nyt käytöstä poistetut tukiasemat. Uusien tukiasemien liittäminen verkkoon on helppoa, ja niiden asennuspaikkaa valittaessa on hyvä käyttää samoja periaatteita kuin tässä työssä. Langattomalta verkolta tullaan tulevaisuudessa vaatimaan suurta kapasiteettia signaalitehon asemesta, mikä saadaan huomioitua suunnittelu- ja mittausohjelmilla. Tukiaseman asennuspaikkaa kannattaa suunnitella tarkasti ja käyttää apuna jo olemassa olevia karttoja verkon peittoalueesta sekä muuta dokumentaatiota. Projektin aikana kävi ilmi, että positiivista palautetta tulee tasaiseen tahtiin, mutta mahdollisia ongelmakohtia ei välttämättä tuoda julki. Vaikka verkko on kerran rakennettu mahdollisimman ”täydellisesti”, radioaallot ovat muuttuva ja vaikeasti ennustettava siirtotie. Seuraavia langattoman verkon sovelluksia suunniteltaessa voisi olla hyvä järjestää henkilökunnalle ja opiskelijoille kysely, jossa kartoitetaan heidän kokemuksiaan verkosta sekä mitä he odottavat palvelulta.

LÄHTEET

About.com Encyclopedia. [www-sivu]. Luettu 10.3.2012.
http://www.associatepublisher.com/e/i/ie/institute_of_electrical_and_electronics_engineers.htm

Air-Stream Wireless. Channels for 802.11.g. [www-sivu]. Luettu 2.3.2012.
http://www.air-stream.org/channel_802_11g

Bardwell, J. & Akin, D. 2005. Certified Wireless Network Administrator Official Study Guide. Amerikan Yhdysvallat: McGraw-Hill/Osborne.

Controller-less WLAN Architecture. Aerohive. [www-sivu]. Luettu 12.3.2012.
http://aerohive.com/solutions/technology-behind-solution/controller-less-wlan-architecture

Fette, B., Aiello, R., Chandra, P., Dobkin, D. M., Bensky, A., Miron, D., Lide, D. A., Dowla, F. & Olexa, R. 2008. RF & Wireless Technologies. Amerikan Yhdysvallat: Elsevier Inc.

Gibbs, K. 2010. Schoolphysics. [www-sivu]. Luettu 2.3.2012.
http://www.schoolphysics.co.uk/age14-16/Wave%20properties/text/Diffraction_/index.html

Hamara, J., Laukkanen, M-L., Lehtonen, P. O., Luoto, K., Vihavainen, M., Ylihärsilä, A. Laboratorioanalyysit. Spektrometriset menetelmät.
http://www03.edu.fi/oppimateriaalit/laboratorio/analyysimenetelmat_5-1_yleista_spektroskopiasta.html

IEEE 802.11 standards tutorial. Radio-Electronics.com. [www-sivu]. Luettu 12.2.2012.
http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php

Juutilainen, M. Radiotekniikan perusteet. [pdf-tiedosto]. Luettu 12.2.2012.
http://www2.it.lut.fi/kurssit/06-07/Ti5312600/luentokalvot/luento03.pdf

Klug, B. 2011. Verizon 4G LTE: Two Datacards and a WiFi Hotspot Massively Reviewed. AnandTech. [www-sivu]. Luettu 7.3.2012.
http://www.anandtech.com/show/4289/verizon-4g-lte-two-datacards-wifi-hotspot-massively-reviewed/2

Mederly, P. 1997. Trunks and multiplexing. [www-sivu]. Luettu 3.3.2012.
http://fmfi-uk.hq.sk/Informatika/Distribuovane%20Systemy/knihy/ICN/ch2s4p2.htm

Moon, M. 2008. LED Lights Eyed to be Next-Gen Low Power Wireless Technology. [www-sivu]. Luettu 27.2.2012.
http://goodcleantech.pcmag.com/future-tech/280296-led-lights-eyed-to-be-next-gen-low-power-wireless-technology

Paschotta, R. Encyclopedia of Laser Physics and Technology. Time division multiplexing. [www-sivu]. Luettu 3.3.2012.
http://www.rp-photonics.com/time_division_multiplexing.html

Perkiömäki, J. [www-sivu]. Luettu 29.2.2012.
http://lipas.uwasa.fi/~jpe/ant/3el19/

Puska, M. 2005. Langattomat lähiverkot. Helsinki: Talentum.

RFID Lab Finland ry. RFID-tietoutta. [www-sivu]. Luettu 10.3.2012.
http://www.rfidlab.fi/rfid-tietoutta

Räisänen, A. & Lehto, A. 2007. Radiotekniikan perusteet. 12. painos. Helsinki: Otatieto.

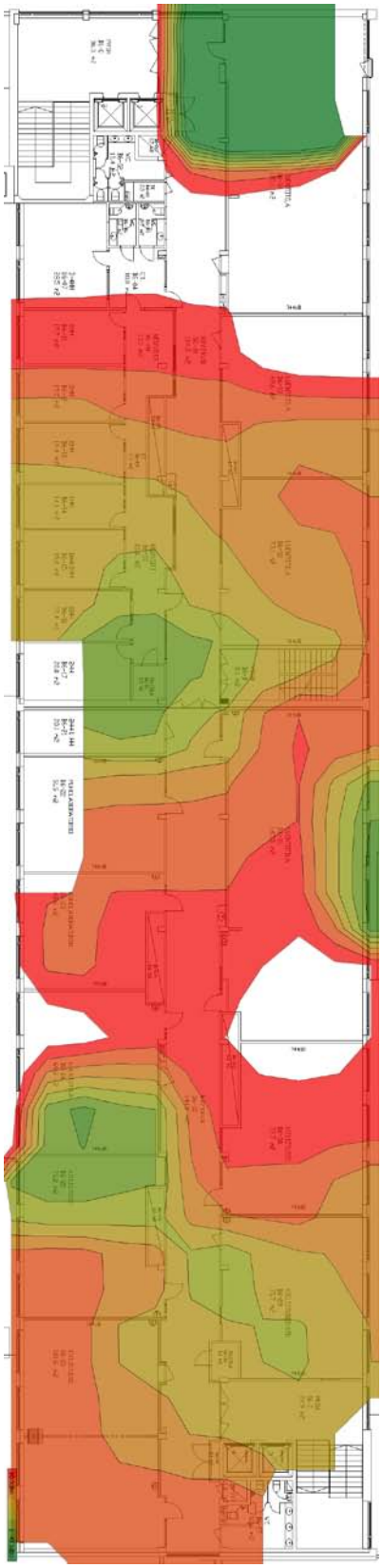
Stallings, W. 2007. Data and Computer Communications. 8. painos. Amerikan Yhdysvallat: Pearson Education Inc.

What is Free Space Optics. 2005. [www-sivu]. Luettu 27.2.2012.
http://www.freespaceoptics.org/freespaceoptics/

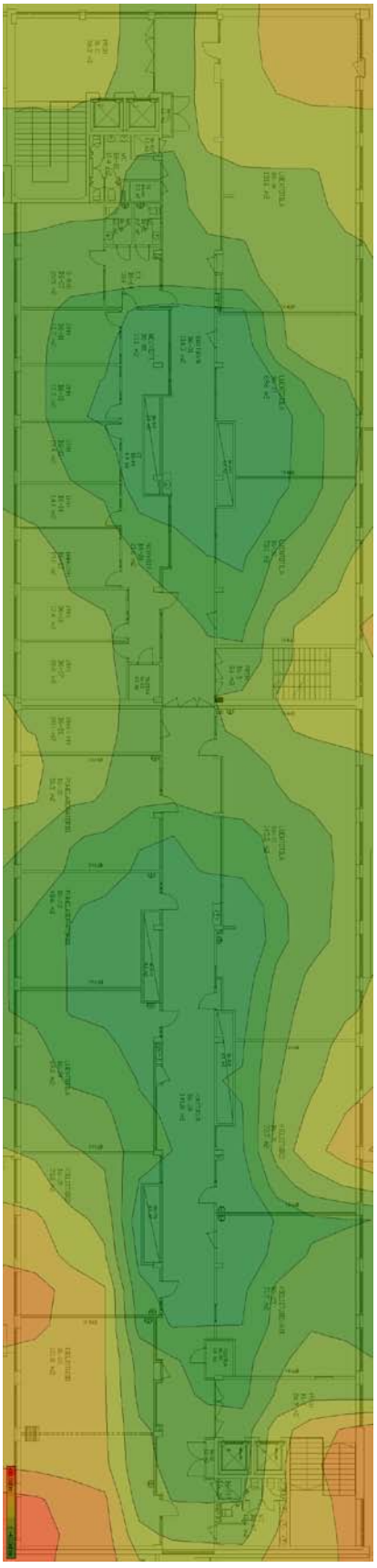
Zander, J. 2011. WiFI offload – getting ahead of the bandwidth curve NOW. The Unwired People. [www-sivu]. Luettu 10.3.2012.
http://theunwiredpeople.com/wifi-offload-getting-ahead-of-the-bandwidth-curve-now/

LIITTEET

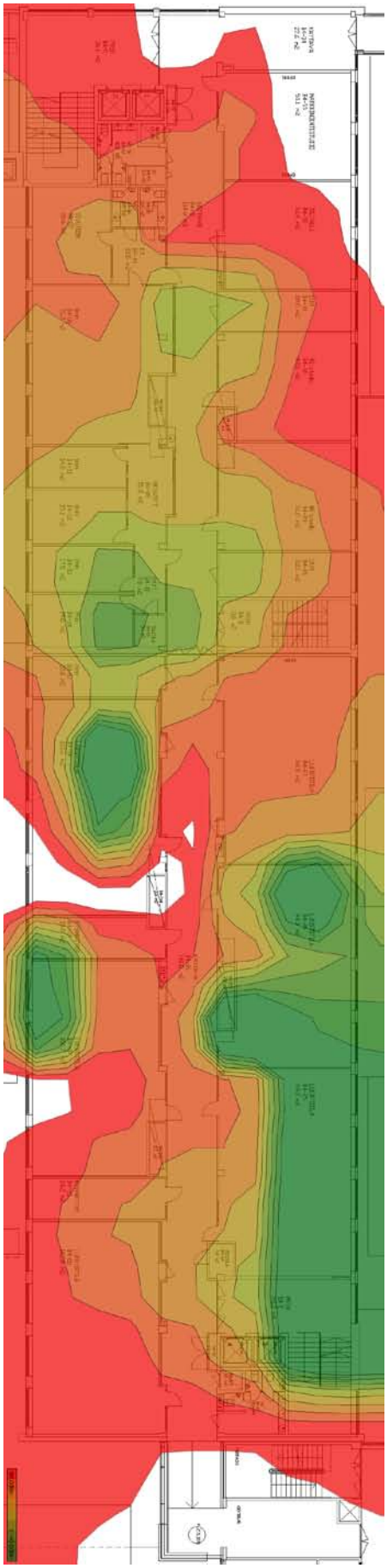
Liite 1. Peittoalue vanhalla järjestelmällä B6-kerroksessa



Liite 2. Peittoalue uudella järjestelmällä B6-kerroksessa



Liite 3. Peittoalue vanhalla järjestelmällä B4-kerroksessa



Liite 4. Peittoalue uudella järjestelmällä B4-kerroksessa