LANGATTOMAN LÄHIVERKON LAADUNVALVONTA

Juho Toivonen

Opinnäytetyö
Joulukuu 2012
Tietotekniikka
Tietoliikennetekniikka ja tietoverkot

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka ja tietoverkot

TOIVONEN, JUHO:
Langattoman lähiverkon laadunvalvonta

Opinnäytetyö 59 sivua, josta liitteitä 6 sivua
Joulukuu 2012

IEEE 802.11 -standardiperheen mukaiset langattomat lähiverkot ovat erilaisten matkapuhelinteknologioiden ohella varteenotettava vaihtoehto tavaksi yhdistää päätelaite tietoverkkoon ja mahdollistaa siten liikennöinti langattoman tukiaseman ja palveluntarjoajan kautta muihin verkkoihin. Langallista tiedonsiirtoa hyödyntäviin ympäristöihin verrattuna langattomassa lähiverkossa käyttäjä ei ole niin vahvasti sidottu sijaintiinsa. Yhteyden muodostamiseksi ei myöskään tarvita samanlaisia kaapelointeja kuin langallisissa verkoissa.

Koska langattomissa lähiverkkojen tiedonsiirrossa hyödynnetään siirtomediana sähkömagneettiseen säteilyyn perustuvia radioaaltoja ja tiedonsiirtoon lisensoimattomia ISM-taajuusalueita, on tietoliikenne altis häiriöille. Näitä ongelmia yritetään ratkaista laadunvalvonnalla, jonka tarkoitus on tarjota mahdollisuus tarkkailla ja analysoida verkkoa korjaavia toimenpiteitä varten.

Työssä tehtiin laboratorio-olosuhteissa passiivisia mittauksia 7signal Sapphire -laadunvalvontajärjestelmällä, joka asennettiin Tampereen ammattikorkeakoulun vierailijaverkkoon. Tietoturvasyistä työssä on esitetty vaihtoehtoinen suunnitelma mittausverkolle IP-osoitteineen. Mittauksilla oli tarkoituksena kartoittaa häiriöiden vaikutuksia langattoman lähiverkon tietoliikenteessä häiritsemällä langatonta tukiasemaa toisella langattomalla tukiasemalla. Tarkkailussa olivat erityisesti signaalitasot ja kanavakäyttö. Mittaukset toistettiin kahdella eri tukiasemalla ja kahdella eri etäisyydellä mittalaitteesta.

Mittaustuloksia vertaillessa ilmeni pieniä muutoksia signaalitasoissa, minkä pohjalta voitiin todeta häirinnän vaikuttaneen tiedonsiirtoon. Laadunhallintajärjestelmien arvioitiin kokonaisuudessaan soveltuvan parhaiten sellaisiin ympäristöihin, joissa langattoman lähiverkon toiminta on kriittisessä asemassa yleisen toiminnan kannalta.

Asiasanat: wlan, langaton lähiverkko, laadunvalvonta, wqa, 7signal.

ABSTRACT

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

TOIVONEN, JUHO:
Wireless Quality Assurance

Bachelor's thesis 59 pages, appendices 6 pages
December 2012

IEEE 802.11 -based wireless local area networks are a considerable option to mobile network technologies for achieving an access both to the local network and to the Internet via a wireless access point. Whereas in wired networks, in wireless environments users are not as bound to the specific locations and no cables are required to establish a connection.

Wireless local area networks use electromagnetic radiation based radio waves as the transmission medium and the frequencies used for transmission are located within the unlicensed ISM bands. Under these circumstances wireless local area networks are constantly exposed to interference. Wireless quality assurance systems are developed to solve this issue. The key is to be able to actively monitor and analyze wireless networks in order to solve problems.

The thesis included passive tests in a laboratory environment using the 7signal Sapphire wireless quality assurance system. The system was used in the guest network of Tampere University of Applied Sciences. Due to security reasons the thesis presents an alternative network plan with alternative IP addresses. The measurements were planned to demonstrate the impact of interference in wireless local area networks by forcing an access point to interfere with another access point. The attention was mainly drawn to signal strength and channel usage. The measurements were repeated with two different access points and with two different distances.

The results were that depending on the situation the signal levels varied slightly yet enough to confirm the impact of the interfering devices. Wireless quality assurance systems provide are particularly beneficial when used in an environment where the performance of wireless local area networks is critical.

Key words: wlan, wireless local area network, wireless quality assurance, wqa, 7signal.

SISÄLLYS

LYHENTEET JA TERMIT

ACK	Acknowledgment; CSMA/CA-skeemassa käytetty lippu, jonka avulla ilmaistaan hyötykuormaa kantavan kehyksen saapuminen perille
AES	Advanced Encryption Standard; salausteniikka
CCK	Complementary Code Keying; koodausmenetelmä
CCMP	Counter Cipher Mode with Block Chaining Message Authentication Code Protocol; salaustekniikka
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance; siirrettävän datan törmäysten välttämiseen perustuva skeema
CSMA/CD	Carrier Sense Multiple Access/Collision Detection; siirrettävän datan törmäysten havaitsemiseen perustuva skeema
CTS	Clear to Send; kehys jolla ilmoitetaan vastaanottajan kaistan olevan varattu ja valmis tiedonsiirtoa varten
DCF	Distributed Coordination Function; kilpavaraukseen perustuva MAC-tekniikka
DSSS	Direct Sequence Spread Spectrum; suorasekvenssitekniikka
DQPSK	Differential Quadrature Phase Shift Keying; differentiaalinen vaihemodulaatioon perustuva modulaatiomenetelmä
EAP	Extensible Authentication Protocol; todennustekniikka
EDCA	Enchanced Distributed Channel Access; QoS:ää määrittelevä MAC-tekniikka
FHSS	Frequency Hopping Spread Spectrum; taajuushyppelyyn perustuva hajaspektritekniikka
FTP	File Transfer Protocol; tiedonsiirtomenetelmä
GFSK	Gaussian Frequency Shift Keying; Gauss-suodatettu taajuusavainnus
GPS	Global Positioning System; satelliittipaikannusjärjestelmä
HCCA	HCF Controlled Channel Access; QoS:ää määrittelevä MAC-tekniikka
IEEE	Institute of Electrical and Electronics Engineers; useiden tietotekniikkaan liittyvien standardien määrittämisestä vastaava teknillinen järjestö

ISM	Industrial, Scientific and Medical; teolliseen, tieteelliseen ja lääketieteelliseen käyttöön suunniteltuihin lisensoimattomiin taajuuskaistoihin viittaava lyhenne
LAN	Local Area Network; IEEE 802.3 -standardiperheen mukainen lähiverkko
LLC	Logical Link Control; IEEE 802 -verkkoja yhdistävä osa siirtokerroksessa
MAC	Media Access Control; tietoliikenteen ohjaamiseen ja hallintaan siirtotiellä käytettävä protokolla, osa siirtokerrosta
MIC	Message Integrity Check; tietoturvaan liitetty viestin tarkistustoiminto
MIMO	Multiple Input Multiple Output; usean antennin samanaikaista lähetys- ja vastaanottokäyttöä hyödyntävä RF-tekniikka
MISO	Multiple Input Single Output; usean antennin samanaikaista lähetyskäyttöä hyödyntävä RF-tekniikka
OFDM	Orthogonal Frequency-Division Multiplexing; ortogonaalinen taajuusjakokanavointiin perustuva lähetystekniikka
PCF	Point Coordination Function; kilpavarausosasta ja ei-kilpavarausosasta koostuva MAC-tekniikka
PSK	Phase Shift Keying; vaiheavainnus on modulaatiomenetelmä, jossa muutetaan kantoaallon vaihetta
PSK	Pre-Shared Key; salauksessa käytetty jaetun avaimen tekniikka
QAM	Quadrature Amplitude Modulation; vaihe- ja amplitudimodulaation yhdistävä modulaatiomenetelmä
QoS	Quality of Service; palvelunlaatu, osa IEEE 802.11e -standardia
SIMO	Single Input Multiple Output; usean antennin samanaikaista vastaanottokäyttöä hyödyntävä RF-tekniikka
SISO	Single Input Single Output; yhden vastaanotto- ja lähetysantennin käyttöä hyödyntävä RF-tekniikka
SSH	Secure Shell; etäyhteyksissä käytetty protokolla salattuun tiedonsiirtoon
SSID	Service Set Identifier; langattoman lähiverkon verkkotunnus
TKIP	Temporal Key Integrity Protocol; salaustekniikka

WEP	Wired Equivalent Privacy; langattoman lähiverkon salausmenetelmä
WLAN	Wireless Local Area Network; IEEE 802.11 -standardiperheen mukainen langaton lähiverkko
WPA	Wi-Fi Protected Access; langattoman lähiverkon salausmenetelmä
WPAN	Wireless Personal Area Network; IEEE 802.15 -standardiperheen mukainen lyhyen kantaman verkko
WQA	Wireless Quality Assurance; langattoman järjestelmän laadunvalvonta

1 JOHDANTO

Langattomuus on ilmiö, joka yleistyy uusien langatonta tiedonsiirtoa hyödyntävien laitteiden virratessa markkinoille. Matkapuhelinteknologioiden ohella langattomat lähiverkot ovat varteenotettava vaihtoehto tavaksi yhdistää päätelaite tietoverkkoon ja mahdollistaa siten liikennöinti langattoman tukiaseman ja palveluntarjoajan kautta muihin verkkoihin, minkä lisäksi myös paikalliset tietoliikenneyhteydet voidaan toteuttaa yksinkertaisesti saman tukiaseman avulla. Siinä missä aiemmin lähiverkkojen toteutuksissa käytettiin pääsääntöisesti langallisia siirtoteitä, nykyään niistä monet voidaan korvata langattomilla yhteyksillä. Langattomat lähiverkkotekniikat tuovat mukanaan haasteita ja ongelmia, joita voidaan kuitenkin tarkkailla ja analysoida korjaavia toimenpiteitä varten. Laadunvalvonnassa on pohjimmiltaan kyse juuri tästä.

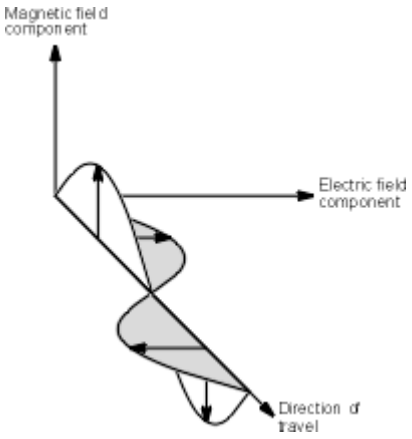
Tässä opinnäytteessä esitellään langattomissa lähiverkoissa käytettyjä tiedonsiirtotekniikoita ja standardeja, kartoitetaan lähiverkon laatuun vaikuttavia asioita ja pohditaan laadunvalvonnan merkitystä erilaisissa ympäristöissä. Merkittävänä osana työtä on 7signal Sapphire -laadunvalvontaratkaisu, josta esitellään käyttöönotto ja toiminta verkkoympäristössä. Järjestelmän ominaisuuksia ja laatuun vaikuttamista esitellään laboratorio-olosuhteissa suoritetuin mittauksin.

2 RADIOTEKNIIKKA

Langattomien lähiverkkojen toteutuksissa hyödynnetään radiotekniikkaa. Käytännössä toteutus tapahtuu liikennöimällä tietyn taajuisilla radioaalloilla, jotka on sovitettu siirtotielle yhteisiä sääntöjä noudattaen. Koska liikennöinti tapahtuu tavallisesti ilmateitse, ilmenee käytännön sovelluksissa myös haasteita ja ongelmakohtia.

2.1 Radioaallot

Radioaallot ovat sähkömagneettista säteilyä, joka koostuu kahdesta komponentista: sähkö- ja magneettikentästä. Kenttien suunnat ovat 90° kulmassa sekä toisiinsa että aaltojen etenemissuuntaan nähden, kuten kuviossa 1 on esitetty. (Adrio Communications 2012b.)



KUVIO 1: Radioaallon rakenne (Adrio Communications 2012b.)

Eräs laskennallinen näkökulma radioaaltoihin on esitetty kaavassa (1), jonka avulla voidaan määrittää aaltoliikkeen suureet nopeus (v), taajuus (f), jaksonaika (T) ja aallonpituus (λ). Olettaen radioaaltojen etenevän vapaassa ilmatilassa, nopeutena voidaan pitää valon nopeutta tyhjiössä (c). Arvo on tällöin pyöristettynä viiteen merkitsevään numeroon $2{,}9979 \cdot 10^8$ m/s. (Mäkelä ym. 2005, 129; Holt & Huang 2010, 16.)

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

Edellistä kaavaa soveltamalla havaitaan kaavassa (2) esitetty taajuuden ja aallonpituuden välinen riippuvuussuhde; kun taajuutta kasvatetaan, aallonpituus pienenee. Eri taajuiset radioaallot etenevät siis myös eri aallonpituuksilla.

$$c = f \cdot \lambda \;\Leftrightarrow\; \lambda = \frac{c}{f} \tag{2}$$

Radioaalloiksi kutsutaan sähkömagneettista säteilyä, joka on taajuudeltaan vähintään 3 Hz ja korkeintaan 300 GHz. Aallot on jaettu taajuuden perusteella eri alakategorioihin, jotka on esitetty taulukossa 1. Sähkömagneettisen säteilyn spektrissä radioaaltoja korkeammille taajuuksille yltävät mm. infrapunasäteily, näkyvä valo, ultraviolettisäteily, röntgensäteily, gammasäteily. (Holt & Huang 2010, 16–17.)

TAULUKKO 1. Radioaallot sähkömagneettisen säteilyn spektrissä

	Aallonpituus (m)		**Taajuus**	
Taajuusalue	**Alaraja**	**Yläraja**	**Alaraja**	**Yläraja**
ELF	10^8	10^7	3 Hz	30 Hz
SLF	10^7	10^6	30 Hz	300 Hz
ULF	10^6	10^5	300 Hz	3 kHz
VLF	10^5	10^4	3 kHz	30 kHz
LF	10^4	10^3	30 kHz	300 kHz
MF	10^3	10^2	300 kHz	3 MHz
HF	10^2	10	3 MHz	30 MHz
VHF	10	1	30 MHz	300 MHz
UHF	1	10^{-1}	300 MHz	3 GHz
SHF	10^{-1}	10^{-2}	3 GHz	30 GHz
EHF	10^{-2}	10^{-3}	30 GHz	300 GHz

Langattomissa lähiverkoissa radioaaltojen lähettämiseen käytetään ISM-taajuusalueita (Industrial, Scientific and Medical), jotka ovat lisensoimattomia ja niin ollen vapaita myös yksityiskäyttöön. Käytössä ovat pääosin 2,4 GHz:n ja 5 GHz:n taajuusalueet. (Gast, M. 2002, 16–17; Holt & Huang 2010, 29.)

2,4 GHz:n taajuusalue sijoittuu UHF-kategoriaan (Ultra High Frequency) ja 5 GHz:n taajuusalue SHF-kategoriaan (Super High Frequency). Taajuusalueiden käyttöä langattomissa lähiverkoissa käsitellään tarkemmin IEEE:n (Institute of Electrical and Electronics Engineers) julkaisemiin standardeihin keskittyvässä luvussa 3.3.

RF-järjestelmän säteilyteho lasketaan tavallisesti dBm:issä, jotka kuvastavat teholukemaa verrattuna yhteen milliwattiin. Milliwattilukemasta voidaan muuntaa dBm-lukema ja päinvastoin kaavalla (3) (Rapidtables.com 2012).

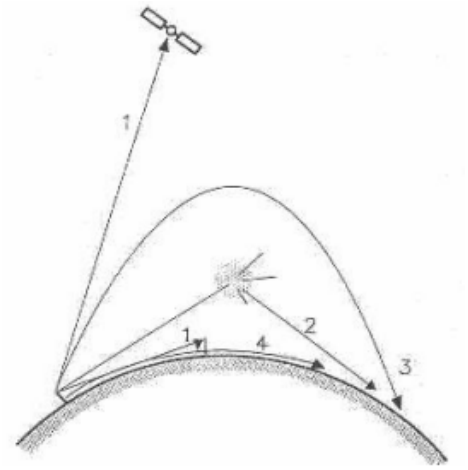
$$P_{\mathrm{mW}} = 10^{\left(\frac{P_{\mathrm{dBm}}}{10}\right)} \Leftrightarrow P_{\mathrm{dBm}} = 10 \cdot \log_{10}\left(\frac{P_{\mathrm{mW}}}{1\ \mathrm{mW}}\right) \quad (3)$$

Suomessa ISM-taajuuskaistalla 2400–2483,5 MHz suurin sallittu lähetysteho on 100 mW (Toivonen 2008, 11). Kaavaa (3) soveltamalla voidaan todeta lukeman vastaavan 20 dBm:ää.

$$P_{\mathrm{dBm}} = 10 \cdot \log_{10}\left(\frac{P_{\mathrm{mW}}}{1\ \mathrm{mW}}\right) = 10 \cdot \log_{10}\left(\frac{100\ \mathrm{mW}}{1\ \mathrm{mW}}\right) = 20\ \mathrm{dBm}$$

2.2 Radioaaltojen eteneminen

Signaalia lähetettäessä on otettava huomioon radioaaltojen lainalaisuudet, jotka vaikuttavat signaalin välittymiseen vastaanottajalle. Sen lisäksi, että radioaallot välittyvät suoraa näköyhteyttä pitkin, ne voivat saavuttaa vastaanottimen myös sironnan avulla, heijastumalla ionosfäärin kautta tai maanpinta-aaltona (Juutilainen 2007a, 10–13). Kuviossa 2 on esitetty nämä etenemistavat numeroimalla ne siten, että numero 1 kuvastaa suoraa näköyhteyttä, numero 2 sirontaa, numero 3 ionosfääriheijastusta ja numero 4 maanpinta-aaltoa.

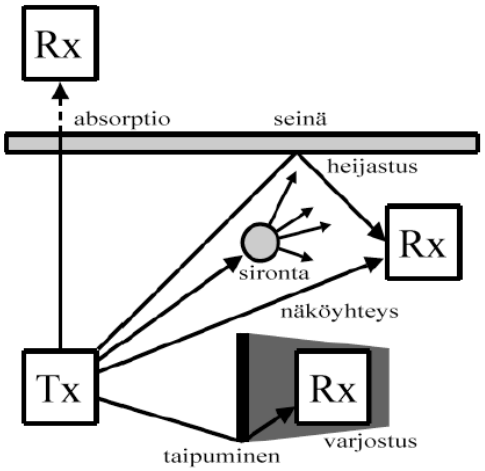


KUVIO 2: Radioaaltojen tärkeimmät etenemistavat (Juutilainen 2007a, 9.)

Koska yli 30 MHz taajuuksilla lähetetyt radioaallot eivät heijastu ionosfääristä ja maan pintaa seuraavina maanpinta-aaltoina pystyvät liikennöimään korkeintaan muutaman megahertsin taajuiset radioaallot (Juutilainen 2007a, 10), näistä etenemistavoista langattomiin lähiverkkoihin vaikuttavat lähinnä suora näköyhteys ja sironta.

Sirontaa tapahtuu silloin, kun radioaallot törmäävät epäsäännöllisen muotoiseen esteeseen, ja säteilyn energia luo sen seurauksena uusia, eri suuntiin hajautuvia radioaaltoja. Tällöin signaalin vaiheessa ja polarisaatiossa näkyy usein muutoksia. (Holt & Huang 2010, 25; Juutilainen 2007a, 27)

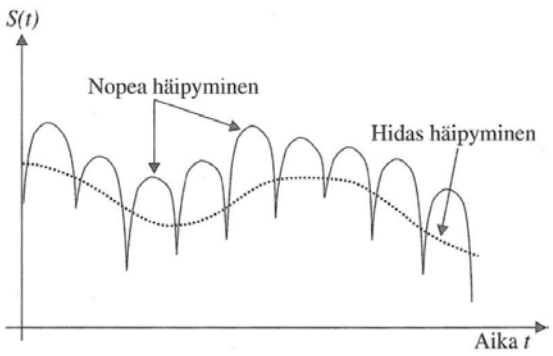
Langattoman lähiverkon kohdalla sironnassa on kyse yleensä epätasaisista pinnoista, tarkemmin kuvailtuna pintojen epäjatkuvuuskohdista kantoalueella; sisätiloissa usein huonekalut ja muu irtaimisto, seinät sekä elävät kohteet aiheuttavat signaalin sirontaa. Mikäli signaali osuu tasaiseen pintaan ja kimpoaa siitä siroutumatta vastaanottimeen, kyse on heijastumisesta; toisaalta signaali voi joissakin tilanteissa esteeseen osuessaan taipua ja kulkea siten näköyhteydestä poikkeavaa reittiä vastaanottimeen, jolloin myös varjostetut vastaanottimet voidaan saavuttaa (Holt & Huang 2010, 24; Juutilainen 2007a, 26). Säteily voi saavuttaa vastaanottimen myös läpäisemällä esteitä, jolloin kyse on absorptiosta; läpäisykyky ja signaalin vaimeneminen riippuu läpäistävän esteen valmistusmateriaalin ominaisuuksista (Holt & Huang 2010, 22). Edellä mainitut sähkömagneettisen säteilyn ominaisuudet on havainnollistettu kuviossa 3.



KUVIO 3. Radioaaltojen etenemiseen vaikuttavia tekijöitä (Holt & Huang 2010, 22, muokattu.)

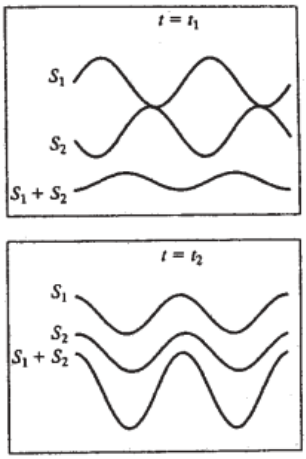
Muita signaaliin vaikuttavia tekijöitä ovat vapaan tilan vaimennus, häipyminen ja monitie-eteneminen (Juutilainen 2007a, 17). Vapaan tilan vaimennus koskee ensisijaisesti suoraa näköyhteyttä; kun sähkömagneettinen säteily etenee ilmassa, sen teho vaimenee etäisyyden kasvaessa.

Termi häipyminen sisältää sekä nopean että hitaan häipymisen. Hidas häipyminen johtuu vastaanottajan liikkeestä; varsinkin varjostus aiheuttaa vaihtelua signaalin keskiarvossa ja sen myötä häiriöitä signaaliin (Belloni 2004, 17; Juutilainen 2007a, 30). Nopeassa häipymisessä kyse on yleensä monitie-etenemisen aiheuttamasta useiden signaalien summautumisessa vastaanottimessa (Belloni 2004, 8). Kun signaalit etenevät – tavallisesti suoran näköyhteyden lisäksi – useita eri reittejä pitkin vastaanottimeen, sama signaali saapuu useampana kappaleena perille. Tämä johtaa amplitudin vaihteluun signaalissa (Juutilainen 2007a, 30). Kuviossa 4 on esitetty hidas ja nopea häipyminen aikatasossa.



KUVIO 4. Nopea ja hidas häipyminen (Juutilainen 2007a, 31.)

Nopea häipyminen johtuu siis samasta signaalista eri etenemisteitä pitkin kulkevien kopioiden summautumisesta vastaanottimessa. Vastaanotettujen signaalien summautumisen tuloksena on vääristynyt signaali. Vääristymä riippuu pääosin viiveistä signaalien saapumisajankohtien välillä sekä mahdollisista vaihe-eroista signaalien välillä. Kaksi ääritilannetta, destruktiivinen ja konstruktiivinen summautuminen, on esitetty kuviossa 5.



KUVIO 5. Destruktiivinen ja konstruktiivinen häiriö (Belloni 2004, 9.)

Destruktiivisessa summautumisessa signaalit saapuvat perille siten, että summautuessa niiden välillä on vaihe-ero. Ääritapauksessa, vaihe-eron ollessa 180°, signaalit voivat kumota toisensa. Vastaavasti konstruktiivista summautumista tapahtuu silloin kun signaalien vaihe-ero on 0° eli signaalit saapuvat vastaanottimeen samaan aikaan tai ne ovat muuten samanvaiheiset. Tällöin signaalien summautuminen vääristää alkuperäistä signaalia siten, että amplitudi kasvaa suuremmaksi kuin on ollut tarkoitus.

2.3 Lähetystekniikat

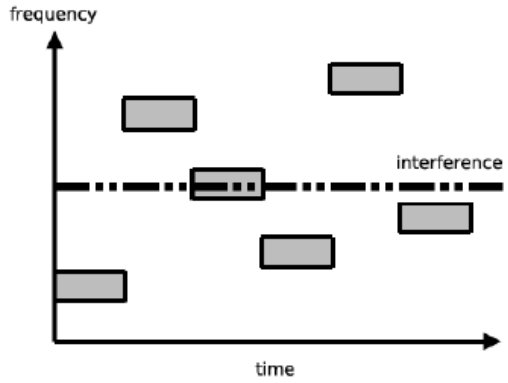
Langattomissa lähiverkoissa käytetään kolmea eri lähetystekniikkaa. Niistä kaksi ensimmäistä ovat hajaspektritekniikoita, joita yhdistää koko taajuusalueen hyödyntäminen lähetyksessä, ja kolmas on usean kantoaallon lähetykseen perustuva tekniikka. Kuhunkin lähetystekniikkaan liittyy tiiviisti osana tiedonsiirrossa käytettävä kanavointitekniikka ja erilaiset modulaatiomenetelmät.

2.3.1 FHSS ja DSSS

FHSS (Frequency Hopping Spread Spectrum) eli taajuushyppely ja DSSS (Direct Sequence Spread Spectrum) eli suorasekvenssitekniikka ovat hajaspektritekniikoita, joissa lähetettävä signaali nimenmukaisesti hajautetaan käytettävälle taajuuskaistalle (Porras 2009a, 42).

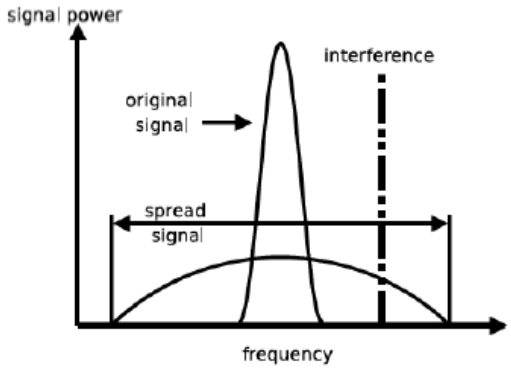
Taajuushyppely toteutetaan siten, että tietoa siirretään tietyllä taajuudella lyhyt aikajakso kerrallaan. Sen jälkeen lähetystaajuus muuttuu siten, että uuden taajuuden ero edelliseen on vähintään 6 MHz. Peräkkäisten lähetystaajuuksien välisellä erolla pyritään minimoimaan mahdollisen häiriön vaikutus lähetykseen; mikäli lähetys hyppää taajuudelle, jolla ilmenee häiriöitä, saman häiriön ei suuremmalla todennäköisyydellä pitäisi vaikuttaa enää seuraavaan lähetystaajuuteen. FHSS:ssä modulaatiomenetelmänä käytetään langattomissa lähiverkoissa GFSK:ta (Gaussian Frequency Shift Keying) eli Gauss-suodatettua taajuusavainnusta. (Holt & Huang 2007, 51–52; Institute of Electrical and Electronics Engineers 1996, 6.)

Koska lähetystaajuus vaihtelee usein, tulee lähettäjällä ja vastaanottajalla olla yhteisesti sovittu satunnainen hyppelyjärjestys. Kuviossa 6 on esitetty esimerkki taajuushyppelystä ja häiriöpiikistä taajuuskaistalla.



KUVIO 6. Taajuushyppely ja häiriöpiikki taajuuskaistalla (Holt & Huang 2007, 52.)

DSSS:ssä alun perin kapealla kaistalla lähetettäväksi tarkoitettu signaali hajautetaan leveämmälle kaistalle tehon kustannuksella, kuten kuviossa 7 on esitetty. Koska signaali hajautetaan, häiriöpiikit voidaan havaita helpommin, jolloin niiden vaikutus voidaan minimoida.

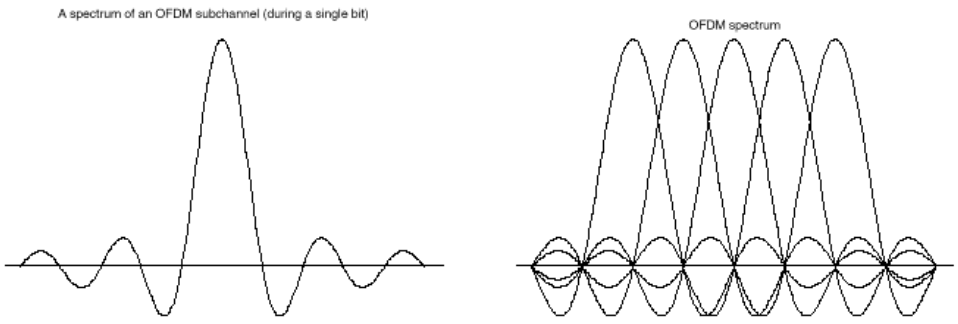


KUVIO 7. Signaalin hajautus ja häiriöpiikki taajuuskaistalla (Holt & Huang 2007, 55.)

Hajauttaminen suoritetaan ennen lähetystä hajautuskoodilla, jonka tarkoitus on esittää jokainen alkuperäisen signaalin biteistä useana bittinä. Vastaavasti vastaanottaja purkaa koodin alkuperäisen signaalin bittijonon selvittämiseksi. Signaalin hajauttamiseen ja kantoaallon moduloimiseen käytetään langattomissa lähiverkoissa PSK:n (Phase-Shift Keying) eli vaiheavainnuksen variantteja. (Juutilainen 2007c, 30–31; Holt & Huang 2007, 54.)

2.3.2 OFDM

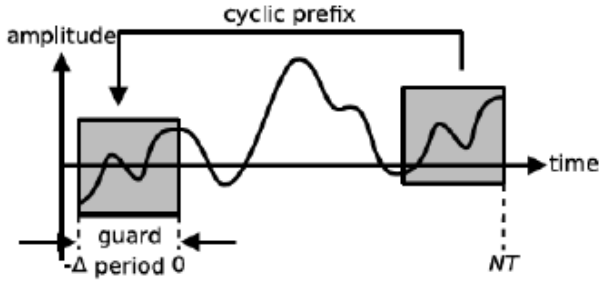
OFDM-tekniikka (Orthogonal Frequency Division Multiplexing) mahdollistaa hajaspektritekniikoita suuremmat tiedonsiirtonopeudet, ja osin siitä syystä se on toteutustapana suosittu nykyaikaisissa langattomissa lähiverkoissa. Tekniikka perustuu usean alikantoaallon hyödyntämiseen tiedonsiirrossa (Holt & Huang 2007, 58). Kuviossa 8 on esitetty yksittäinen kantoaalto ja viisi rinnakkaista kantoaaltoa taajuustasossa.



KUVIO 8. Yksittäisen kantoaallon ja viiden rinnakkaisen kantoaallon taajuustason esitykset OFDM-tekniikassa (Matic 1999.)

OFDM:ää lähetystekniikkana käyttävissä langattomissa lähiverkoissa modulaatiomenetelminä käytetään joko PSK:n variantteja tai vaihe- ja amplitudimodulaation yhdistävän QAM:n (Quadrature Amplitude Modulation) variantteja, joilla on mahdollista saavuttaa verrattain suurempia tiedonsiirtonopeuksia. (Prasad 2004, 25–26.)

OFDM-tekniikassa tietoa lähetettäessä symbolien väliin lisätään GI (Guard Interval) eli suojaväli, jonka tarkoitus on ehkäistä monitie-etenemisestä johtuvien signaalin vääristymien vaikutukset vastaanottimessa. Suojaväli toteutetaan lisäämällä kunkin symbolin eteen saman symbolin loppuosasta kopioitu liite kuviossa 9 esitetyllä tavalla. (Armstrong 2002, 18; Holt & Huang 2007, 60–61.)



KUVIO 9. Suojaväli ja etuliite aikatasossa (Holt & Huang 2007, 61.)

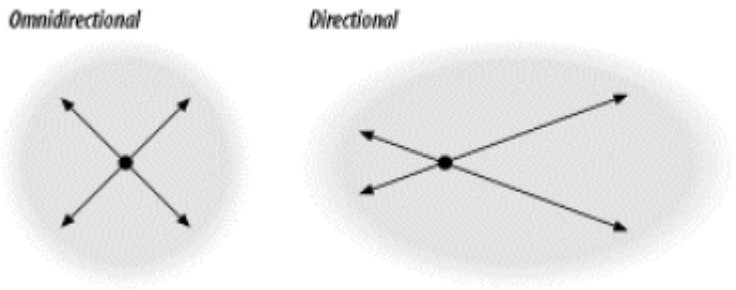
Vastaanotin odottaa suojavälin määrittämän ajan mahdollisia kopioita alkuperäisestä, jo perille saapuneesta signaalista. Tavoitteena on saavuttaa tilanne, jossa signaalia näytteistettäessä vastaanottimeen ei enää saapuisi kopioita, jotka vääristäisivät alkuperäistä signaalia. (Adrio Communications 2012d.)

2.4 Antennit

2.4.1 Yleisimmät antennityypit

Antennit jakautuvat kahteen pääryhmään: isotrooppisiin eli ympärisäteileviin antenneihin ja suunta-antenneihin. Isotrooppisuudella saavutetaan vaakatasossa teoriassa sama teho samalla etäisyydellä kaikkiin suuntiin, kun taas suuntaamalla voidaan kohdistaa verrattain sama energia laajan alan sijaan kapealle sektorille ja saavuttaa sen myötä pidempi lähetys- ja vastaanottoetäisyys. Tällöin sektorin ulkopuolella sijaitsevat lähettimet ja vastaanottimet jäävät tukiaseman peittoalueen ulkopuolelle. (Cisco Systems, Inc. 2007)

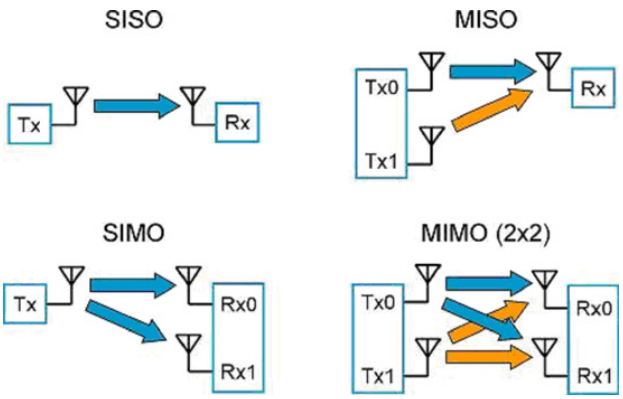
Kuviossa 10 on esitetty ympärisäteilevä antennin ja eräänlaisen suunta-antennin tuottaman sähkömagneettisen säteilyn periaatekuvat ylhäältäpäin tarkasteltuna.



KUVIO 10. Ympärisäteilevä antenni ja suunta-antenni vaakatasossa (Gast 2002, 166.)

2.4.2 Antennijärjestelmät

Tiedon lähettämiseen ja vastaanottamiseen tarvitaan vähintään yksi lähetin ja yksi vastaanotin. Kuten myöhemmissä luvuissa todetaan, langattomissa lähiverkoissa tiedonsiirron on oltava kaksisuuntaista, joten jokaisessa verkko- tai päätelaitteessa on oltava sekä lähetin että vastaanotin. Tavallisesti laitteissa ei ole kuitenkaan tarpeen olla lähetystä ja vastaanottoa varten erillisiä antenneja; tiedonsiirto kulkee sekä sisään- että ulospäin saman antennin kautta. Laitteissa voidaan kuitenkin käyttää useaa eri antennia joko vastaanottamiseen tai lähettämiseen. Kuviossa 11 on esitetty erilaisten antennijärjestelmien periaatekuvat.



KUVIO 11. Yhden ja useamman antennin käyttö tiedonsiirrossa (Agilent Technologies 2009.)

SISO-tekniikassa (Single Input Single Output) käytetään yhtä antennia sekä lähetykseen että vastaanottoon. SISO:n etu onkin sen yksinkertaisuus; toisaalta verrattuna usean antennin järjestelmiin häipyminen ja häiriöt vaikuttavat enemmän SISO-järjestelmään ja tiedonsiirtokapasiteetti on rajoitetumpi. (Adrio Communications 2012c.)

SIMO-tekniikassa (Single Input Multiple Output) signaali lähetetään yhdellä antennilla ja vastaanotetaan kahdella tai useammalla antennilla. Tekniikan etuihin lukeutuu se, että usean antennin käyttö vastaanottimessa vähentää häipymisen ja häiriöiden aiheuttamia vääristymiä signaalissa. Vastaanottimessa olevia antenneja voidaan hyödyntää joko käyttäen vain vahvimman signaalin vastaanottavaa antennia tai käyttäen kaikkia antenneja yhtäaikaisesti, jolloin eri antenneihin saapuvat saman signaalin kopiot summataan keskenään. (Adrio Communications 2012c.)

MISO-tekniikka (Multiple Input Single Output) pohjautuu kahden tai useamman antennin käyttämiseen lähetyksessä ja yhden antennin käyttämiseen vastaanotossa. Järjestelmän etuihin voidaan lukea se, että signaali saapuu vastaanottimeen optimaalisena, kun se lähetetään samanaikaisesti usealla eri antennilla. (Adrio Communications 2012c.)

MIMO-tekniikassa (Multiple Input Multiple Output) sekä lähetykseen että vastaanottoon käytetään kahta tai useampaa antennia. Tekniikalla on mahdollista saavuttaa suurempi tiedonsiirtokapasiteetti edellyttäen, että vastaanotin käyttää kaikkia antennejaan yhtäaikaisesti vastaanottamiseen sen sijaan, että käytössä olisi vain vahvimman signaalin saava antenni. (Holt & Huang 2007, 62.)

3 LANGATTOMAT LÄHIVERKOT

Langattomia lähiverkkoja on kehitetty nykyisessä muodossaan yli 20 vuotta. Siinä ajassa on kehitetty ja julkaistu lukuisia aiheeseen liittyviä standardeja ja niihin liittyviä tekniikoita. Tässä luvussa käsitellään langattoman lähiverkon perusteita ja rakennetta ja syvennytään nykypäivänä käytössä oleviin tekniikoihin ja menetelmiin.

3.1 Perusteet

Lähiverkoilla eli LAN:illä (Local Area Network) tarkoitetaan paikallisia tiedonsiirtoyhteyksiä tietoteknisten laitteiden välillä. Yhteys voidaan toteuttaa joko erillisen verkkolaitteen avulla tai mahdollisuuksien mukaan yhdistämällä laitteet suoraan toisiinsa. Yhteys voidaan saavuttaa joko langallista tai langatonta siirtotietä pitkin; siirtotien teknisen toteutustavan määrittelee tavallisesti kuhunkin tekniikkaan liittyvä standardi.

Langallisista toteutustavoista nykyään käytössä on pääosin IEEE 802.3 -standardiperheeseen perustuva Ethernet-tekniikka; muita aiemmin käytettyjä IEEE:n standardoimia langallisia lähiverkkotekniikoita – Token Busia ja Token Ringiä – ei juurikaan enää käytetä. (Holt & Huang 2010, 3.)

Ensimmäiset IEEE 802.11 -perheeseen kuuluvat langattoman lähiverkon standardit julkaistiin 1990-luvulla, joskin standardin pohjalla ollutta tekniikkaa ja muita ratkaisumalleja oli suunniteltu jo ennen sitä. Suurin haastaja, ETSI-järjestön (European Telecommunications Standards Institute) 2000-luvun alussa julkaisema HiperLAN-standardi, oli suorituskyvyltään kilpailukykyinen vaihtoehto, mutta IEEE 802.11 -standardiperheen tuilla varustetut laitteet valtasivat kuitenkin markkinat. (Holt & Huang 2010, 3–4.)

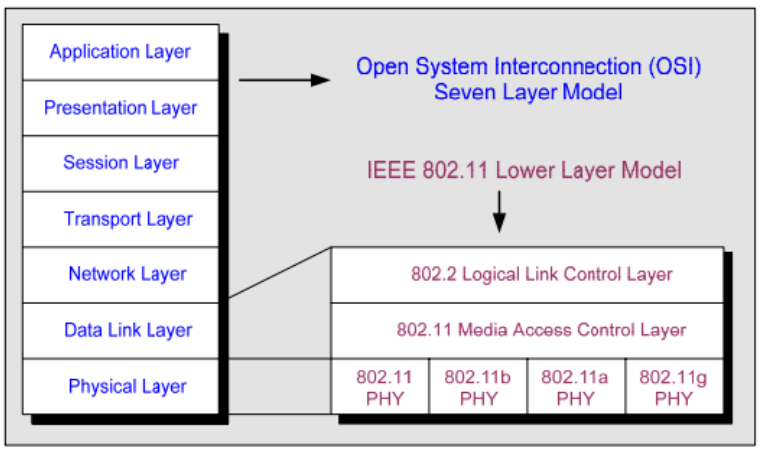
Langattomaan tiedonsiirtoon perustuvien tekniikoiden tarkoitus on mahdollistaa tiedonsiirtoyhteys tietoteknisten laitteiden välillä ilman kaapelointia, ja periaate pätee myös IEEE 802.11 -standardiperheeseen perustuviin langattomiin lähiverkkoihin, joista käytetään yleisesti lyhennettä WLAN (Wireless Local Area Network). Käytännössä langattomalla lähiverkolla voidaan korvata lähiverkoissa IEEE 802.3 -standardin mukaiset Ethernet-yhteydet tai tuoda langaton vaihtoehto langallisten yhteyksien rinnalle. Esi-

merkiksi 24-porttinen Ethernet-kytkin voidaan korvata 4-porttisella langattomalla tukiasemalla, jossa langallisen siirtotien sijaan käytetään langatonta siirtotietä. Rajapinta vaihtuu siis tavallisesti käytetystä Ethernetistä WLAN:ään. Muutos edellyttää sitä, että jokaisessa verkkoon liitettävässä päätelaitteessa on langattomassa tukiasemassa käytettävää lähiverkkotekniikkaa tukeva verkkosovitin ja datan lähetykseen ja vastaanottoon soveltuva antenni.

Konkreettisin hyöty WLAN-tekniikoista lienee se, että voidaan välttää kaapeloinnin aiheuttamat taloudelliset kustannukset sekä rajoitukset laitteiden siirrettävyydessä. Taloudellinen näkökulma on tuettuna myös verkkolaitehankintojen kannalta, kun Ethernet-rajapinta ei ole ehdoton edellytys päätelaitteen liittämiseksi verkkoon. Kannettavista päätelaitteista älypuhelimissa ja taulutietokoneissa ei tavallisesti edes ole Ethernet-liitäntämahdollisuutta kokorajoitustensa vuoksi, jolloin langattoman yhteyden saatavuuden merkitys kasvaa. Toisaalta langaton siirtotie voidaan nähdä langallista haasteellisempana, sillä signaalin etenemiseen vaikuttavia tekijöitä on ilmatiellä huomattavasti enemmän kuin kaapelissa.

3.2 OSI-malli ja tiedonsiirto

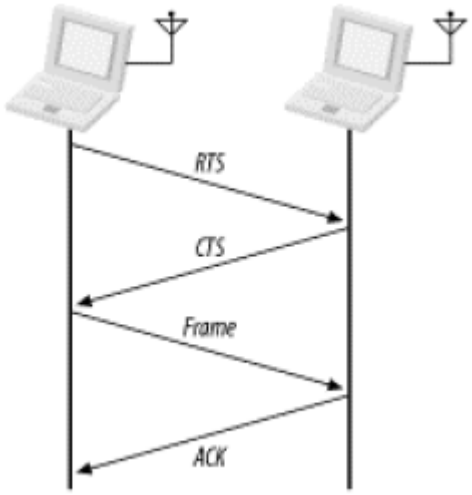
OSI-mallissa IEEE 802.11 -standardi sijoittuu fyysiseen kerrokseen sekä osin siirtokerrokseen (kuvio 12). Fyysisessä kerroksessa on kuvattuna fyysisenä rajapintana toimiva spesifi standardi. Tämän lisäksi siirtokerroksen alempi puolisko on IEEE 802 -verkoille tyypillisesti standardia vastaava MAC-alikerros (Media Access Control), joka on siis tässä tapauksessa IEEE 802.11 -standardiperheen mukainen.



KUVIO 12. IEEE 802.11 -standardi OSI-mallissa (Masica 2007, 3.)

Fyysinen kerros vastaa tiedon lähettämisestä ja vastaanottamisesta; kerros sisältää tiedot käytettävästä modulointimenetelmästä sekä taajuuksista siirtotiellä. Siirtokerros puolestaan vastaa liikennöinnin hallinnasta; standardispesifi MAC-alikerros voidaan käsittää porttina ylemmistä kerroksista fyysiseen kerrokseen – tai päinvastaisesti fyysisestä kerroksesta ylempiin kerroksiin –, kun taas LLC-alikerros (Logical Link Control) on ylemmät kerrokset ja MAC-alikerroksen yhteensovittava kappale, joka on usein vastuussa myös datavuon ohjauksesta ja virheenhallinnasta. (Holt & Huang 2010, 3; Masica 2007, 2.)

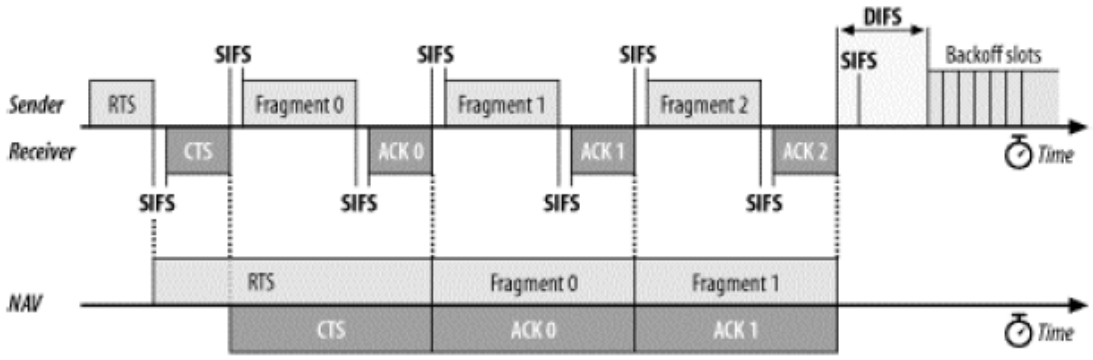
Kun lähetettävä tieto on edennyt kuviossa 12 esitettyjä kerroksia ylhäältä alaspäin aina siirtokerroksen puoliväliin asti, MAC-alikerros valmistelee datan fyysistä kerrosta varten kehystämällä sen. MAC:n yhteydessä IEEE 802.11 -standardi käyttää yhteyksissään tiedonsiirtokaistaa tuhlaavien törmäysten varalta CSMA/CA-skeemaa (Carrier Sense Multiple Access/Collision Avoidance), joka eroaa IEEE 802.3 -standardissa käytetystä CSMA/CD-skeemasta (Carrier Sense Multiple Access/Collision Detection) siten, että datan törmäyksiä pyritään tunnistamisen sijaan välttämään, ja siksi tilannetta siirtokaistalla tiedustellaan ennen tiedon lähettämistä (Gast, M. 2002, 38). Kuviossa 13 on esitetty edellä kuvaillun CSMA/CA-skeeman mukainen nelivaiheinen kättely.



KUVIO 13. CSMA/CA-skeeman mukainen nelivaiheinen kättely (Gast 2002, 38.)

Kättelyssä tietoa lähettävä osapuoli lähettää ensin vastaanottajalle pyyntönä tiedonsiirron aloittamiseksi RTS-kehyksen (Request to Send) ja varaa sillä siirtotien omalta osaltaan. Vastaanottaja vastaa tähän CTS-kehyksellä (Clear to Send) ja varaa siirtotien omalta osaltaan. Tällä tavalla varmistetaan se, että siirtotie on vapaa muista signaaleista

ja kehyksinä lähetettävä varsinainen data ei törmää muihin vastaanottajalle lähetettäviin kehyksiin. Kun lähetetty data on saapunut vastaanottajalle, lähettää tämä vahvistuksena siitä ACK-kehyksen (Acknowledge). Mikäli alkuperäinen lähettäjä ei saa vahvistusta viestin saapumisesta perille, lähetys todetaan epäonnistuneeksi. Tällöin kehystä yritetään lähettää uudestaan siihen määritetyn viiveen kuluttua. Kehysten sisältämä hyötykuorma voidaan tarvittaessa pilkkoa pienempiin osiin ja lähettää useampina kehyksinä. Häiriöalttiissa ympäristöissä myös pienemmät hyötykuormat voidaan pilkkoa robustisuuden lisäämiseksi (kuvio 14). (Gast 2002, 38; 43–44; 47)



KUVIO 14. CSMA/CA-skeeman mukainen kättely ja pilkotun datan siirto (Gast 2002, 46.)

Kuviossa 14 on esitetty tilanne, jossa siirretään ja vahvistetaan pilkottu ja numeroitu data. NAV (Network Allocation Vector) ilmaisee varaukset siirtotiellä; RTS-kehyksen lähetyksen jälkeen siirtotietä varataan, kunnes Fragment 0 -nimellä kuviossa ilmaistun ensimmäisen kehyksen lähetys voidaan aloittaa. Vastaavasti CTS-vahvistuksen lähetyksestä lähtien vastaanottajan siirtotie varataan alkavaa tiedonsiirtoa varten. Vastaanottaja lähettää numeroidun ACK-vahvistuksen (Acknowledgment) jokaisesta saapuneesta kehyksestä.

MAC-alikerrokseen liittyvät kiinteästi tekniikat DCF (Distributed Coordination Function) ja PCF (Point Coordination Function). DCF-tekniikka perustuu kilpavaraukseen, mikä voi aiheuttaa ruuhkatilanteissa laskun tiedonsiirtonopeudessa. PCF puolestaan perustuu kahteen osaan, joista toisessa käytetään kilpavarausta ja toisessa ei. Kilpavarausosassa käytetään DCF:ää, ja kilpavarauksettomassa osassa tukiasema antaa kordinaattorin ominaisuudessa erikseen luvan lähettää tietoa. (Girish 2008, 6; Väärämäki 2007, 13.)

MAC-alikerrokselta siirrytään fyysiselle kerrokselle, joka vastaa tiedon välittämisestä tiedonsiirtoon osallistuvien laitteiden fyysisten rajapintojen välillä; fyysinen kerros käytännössä määrää siirtomedian ja lähetystekniikan. Langattomassa lähiverkossa siirtomediana käytetään radioaaltoja ja lähetystekniikka vaihtelee standardin mukaan.

3.3 IEEE 802.11 -standardiperhe

Alkuperäinen IEEE 802.11 -standardi suunniteltiin 1990-luvun loppupuolella mahdollistamaan 1 ja 2 Mb/s langaton tiedonsiirtonopeus 2,4 GHz:n ISM-taajuusalueella. Standardiin määritettiin toteutustavoiksi kaksi eri hajaspektritekniikkaa: FHSS ja DSSS. Standardi laajeni standardiperheeksi, kun vaatimukset tiedonsiirtonopeuden suhteen nousivat. Vuosien mittaan on julkaistu useita alkuperäistä standardia täydentäviä ja päivittäviä laajennuksia. (Molisch 2011, 731.)

Tässä luvussa käsitellään standardiperheen sisältämistä lukuisista standardeista vain IEEE 802.11a/b/g/n/ac/e.

3.3.1 IEEE 802.11a/b/g

Suuren suosion saavuttanut 2,4 GHz:n taajuusalueelle suunniteltu IEEE 802.11b -laajennus nosti teoreettisen tiedonsiirtonopeuden alkuperäisestä 2 Mb/s:sta 11 Mb/s:iin käyttäen DQPSK- (Differential Quadrature Phase Shift Keying) ja CCK-menetelmiä (Complementary Code Keying). Samana vuonna julkaistu IEEE 802.11a liikennöi ruuhkattomalla 5 GHz:n taajuusalueella, ja standardin korkeimmaksi mahdolliseksi tiedonsiirtonopeudeksi ilmoitettiin 54 Mb/s. Tämä verrattain huomattavasti suurempi tiedonsiirtonopeus saavutettiin käyttämällä uudempaa lähetystekniikkaa, OFDM:ää, ja sen tukemaa 64QAM-menetelmää. Samaa tekniikkaa hyödynnettiin IEEE 802.11g -laajennuksen suunnittelussa. IEEE 802.11b:n tavoin myös IEEE 802.11g:ssä käytettiin 2,4 GHz:n taajuusaluetta. (Holt & Huang 2007, 56–57; Molisch 2011, 731–732; Prasad 2004, 25.)

Vaikka IEEE 802.11a tarjosikin aiempia standardeja korkeamman tiedonsiirtonopeuden ja ruuhkattoman taajuusalueen, se osoittautui väliinputoajaksi viimeistään IEEE

802.11g:tä tukevien laitteiden saavuttua markkinoille. Uudemman standardin käyttöä puolsi myös 2,4 GHz:n taajuusalue ja sen myötä standardia tukevien tukiasemien mahdollisuus yhteensopivuuteen IEEE 802.11b:n kanssa.

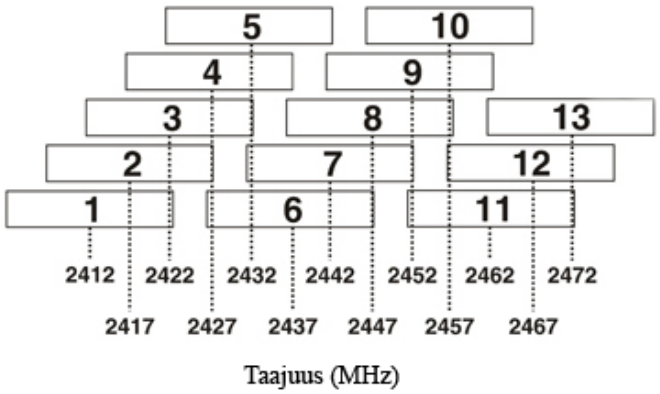
Taulukkoon 2 on kerätty standardien merkittävimmät tiedot havainnollistamaan näiden standardien eroavaisuuksia (Molisch 2011, 731–732; Nobel ym. 2012).

TAULUKKO 2: IEEE 802.11a/b/g -standardien vertailutaulukko

Standardi	Vuosi	Taajuusalue	Tiedonsiirtonopeus (max)	Lähetystekniikka
802.11	1997	2,4 GHz	2 Mb/s	FHSS, DSSS
802.11a	1999	5 GHz	54 Mb/s	OFDM
802.11b	1999	2,4 GHz	11 Mb/s	DSSS
802.11g	2002	2,4 GHz	54 Mb/s	OFDM

Euroopassa on voimassa ETSI:n määräysten mukaisesti 13 kanavaa, jotka ovat kaistanleveyksiltään nimellisesti 20 MHz. Vierekkäisten kanavien keskitaajuuksien välillä on 5 MHz:n erotus. Jotta vältetään päällekkäisten kanavien käyttö ja siitä koituvat häiriöt, on samalla peittoalueella operoivissa tukiasemissa käytettävien kanavien välillä oltava 25 MHz:n erotus. Tämä mahdollistaa korkeintaan kolmen kanavan käytön rinnakkain samalla alueella. Mahdollisuuksia rinnakkaisille kanaville on kolme: 1, 6 ja 11, 2, 7 ja 12 tai 3, 8 ja 13. (Adrio Communications 2012e; Holt & Huang 2007, 30.)

Kuviossa 15 on esitetty 2,4 GHz:n taajuusalueen WLAN-kanavat ja niiden keskitaajuudet.



KUVIO 15. 2,4 GHz:n taajuusalueen kanavat (Phoenix Contact 2012, muokattu.)

3.3.2 IEEE 802.11n

IEEE 802.11n -standardi hyödyntää sekä 2,4 GHz:n että 5 GHz:n taajuusalueita. Nimelliseksi tiedonsiirtonopeudeksi määritettiin standardiin 600 Mb/s. Aiempiin saman standardiperheen standardeihin verrattuna moninkertainen nopeus voidaan saavuttaa pääosin kahden uuden ominaisuuden avulla. Ominaisuuksista ensimmäinen on aiempaa kaksi kertaa suuremman kaistanleveyden käyttäminen siirtotiellä. Toisena uutena, tiedonsiirtokapasiteettia suurentavana ominaisuutena esiteltiin useaa antennia hyödyntävät MIMO-tekniikat. Lähetystekniikaksi määritettiin OFDM; IEEE 802.11n -standardia tukevissa laitteissa on kuitenkin toimintatiloja, joilla on mahdollista saada tukiasema yhteensopivaksi aiempia standardeja tukevien laitteiden kanssa. (Molisch 2011, 739–740; Wrexler 2006.)

Standardia tukeva laite voi siirtää tietoa 20 MHz:n tai 40 MHz:n kaistanleveydellä tai kummallakin. 2,4 GHz:n taajuuskaistalla käytetään 20 MHz:n kaistanleveyttä, kun samanaikaisesti verrattain laajemmalla 5 GHz:n taajuuskaistalla voidaan käyttää 40 MHz:n kaistanleveyttä. Tiedonsiirtokapasiteettia kasvattaa myös IEEE 802.11a/g:hen verrattuna pienempi suojaväli; GI puolittuu 800 ns:sta 400 ns:iin. (Holt & Huang 2007, 66.)

IEEE 802.11n:ää tukevien laitteiden suorituskykyä nostaa myös valinnainen ominaisuus, beamforming-tekniikka, jonka tarkoitus on käytännössä muuttaa tukiaseman ympärisäteilevät antennit suunnatuiksi muuttamalla vähintään yhden niistä vaihetta tai amplitudia; näin signaalia voidaan vahvistaa vastaanottimen suuntaan ja vastaavasti heikentää mahdollisten häiriölähteiden suuntaan. (Holt & Huang 2007, 66, 72; Schulz 2011, 4–5.)

3.3.3 IEEE 802.11ac

IEEE 802.11ac -standardia tukevat laitteet käyttävät vain 5 GHz:n taajuuskaistaa. Standardin on tarkoitus on tarjota aiempia standardeja suurempi tiedonsiirtokapasiteetti; maksimissaan n. 3,5 Gb/s:iin yltävä tiedonsiirtonopeus mahdollistetaan suuremmilla kaistanleveyksillä, suurempaan tiedonsiirtokapasiteettiin tähtäävillä modulaatiomenetelmillä sekä yhä useammilla samanaikaisesti lähetettävillä signaaleilla. Standardi on

taaksepäin yhteensopiva standardien IEEE 802.11a/n kanssa, ja se tukee kaistanleveyksiä 20 MHz, 40 MHz, 80 MHz ja 160 MHz. Modulaatiomenetelmistä korkeimpaan mahdolliseen tiedonsiirtonopeuteen voidaan yltää 256QAM:llä. Samanaikaisesti voidaan lähettää korkeintaan kahdeksaa signaalia. Standardin kehitystyö on opinnäytteen kirjoittamishetkellä vielä kesken. (Institute of Electrical and Electronic Engineers 2012; Ward 2012, 4–5.)

3.3.4 IEEE 802.11e

IEEE 802.11e -standardi kehitettiin määrittämään QoS:ää (Quality of Service) eli palvelunlaatua. Taustana tälle on se, että lähiverkoissa käyttäjämäärän lisääntyessä myös kuormitus lisääntyy, jolloin syntyy tarve priorisoida liikennettä. Esimerkiksi videon ja äänen lähetys, kuten VoIP- (Voice over IP) eli IP-puhepalvelussa muun liikenteen aiheuttamien viiveiden ja hävinneiden pakettien vaikutukset vastaanottajan päässä ovat merkittävässä asemassa. Tämä korostuu erityisesti häiriöalttiissa langattomissa lähiverkoissa. (Adrio Communications 2012; Väärämäki 2007, 16.)

Standardi määrittelee ongelman ratkaisemiseksi kaksi tekniikkaa: EDCA:n (Enchanced DCF Channel Access) ja HCCA:n (HCF Controlled Channel Access), jotka sijoittuvat OSI-mallissa siirtokerroksen MAC-alikerrokseen ja laajentavat DCF- ja PCF-tekniikoita.

EDCA pohjautuu DCF-tekniikkaan, ja sen tarkoitus on luokitella liikenne CWmin- ja CWmax -arvojen avulla. Lähetettävä data voidaan luokitella neljään eri ryhmään: voice, video, background ja best effort. HCCA pohjautuu PCF:ään; kehykset jaetaan samoin tavoin kilpavarauksselliseen ja kilpavarauksettomaan osaan. Lähetettävä data jaetaan jonoihin, joiden pituudet määrittävät lähetysajat. Myös useiden pakettien lähettäminen peräkkäin on mahdollista. (Chien 2007, 4; Väärämäki 18, 24–25.)

3.4 Salaus- ja todennusmenetelmät

Tietoturvan lisäämiseksi on olemassa erilaisia menetelmiä, joilla langattoman dataliikenne voidaan salata verkon ulkopuolisilta käyttäjiltä ja todentaa tietoturvan lisäämiseksi.

3.4.1 WEP

WEP (Wired Equivalent Privacy) suunniteltiin nimensä mukaisesti langattomiin lähiverkkoihin vastaamaan langattoman siirtotien tietoturvaa päätelaitteen ja tukiaseman välille. Salaus voidaan toteuttaa pääosin joko ilman avainta, 64-bittisellä avaimella tai 128-bittisellä avaimella. Avaimen pituus vaikuttaa salausalgoritmin tekemään tiedon salauksen monimutkaisuuteen ja siten suojaustasoon. Loppukäyttäjä tunnistautuu tukiasemalle etukäteen sovitulla salasanalla; vaihtoehtoisesti tunnistautumisen. Vaikka liikenne saadaankin salattua, on WEP salausmenetelmänä helppo murtaa. (Thomas 2005, 305–306.)

3.4.2 WPA ja WPA2

WPA (Wi-Fi Protected Access) suunniteltiin paikkaamaan WEP:ssä ilmenneitä haavoittuvuuksia. Menetelmässä käytetty TKIP (Temporal Key Integrity Protocol) salaa siirrettävät paketit – WEP:stä ja siinä käytetystä staattisesta avaimesta poiketen – dynaamisesti luodulla avaimella. Salaus toteutetaan 128-bittisellä avaimella, ja pakettien kaappaamisen ja muokkaamisen varalta käytetään pakettien tarkistusmenetelmää, MIC:tä (Message Integrity Check). Todennus voidaan toteuttaa kahdella eri tavalla: PSK:lla (Pre-Shared Key) eli esijaetulla avaimella tai 802.1X:llä ja EAP:llä (Extensible Authentication Protocol). 802.1X/EAP -salaus perustuu porttikohtaiseen todennukseen. (Cisco Systems, Inc. 2008; Wi-Fi Alliance 2012.)

WPA2 on paranneltu versio WPA:sta ja osa IEEE 802.11i -standardia. Todennusmenetelmät ovat samat kuin WPA:ssa, mutta paketit salataan AES:ää (Advanced Encryption Standard) ja CCMP:tä (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) käyttäen. Tällä yhdistelmällä lähetettävä tieto salataan AES:llä

128 bitin lohkoissa ja 128-bittisellä avaimella. (Cisco Systems, Inc. 2008; Institute of Electrical and Electronics Engineers 2007, 197.)

4 LANGATTOMIEN LÄHIVERKKOJEN LAATU

Tässä luvussa käsitellään Cisco Systems, Inc.:n teettämään kyselyyn pohjautuen langattoman lähiverkon laatuun liittyviä käytännön ongelmia.

4.1 Laadun merkitys

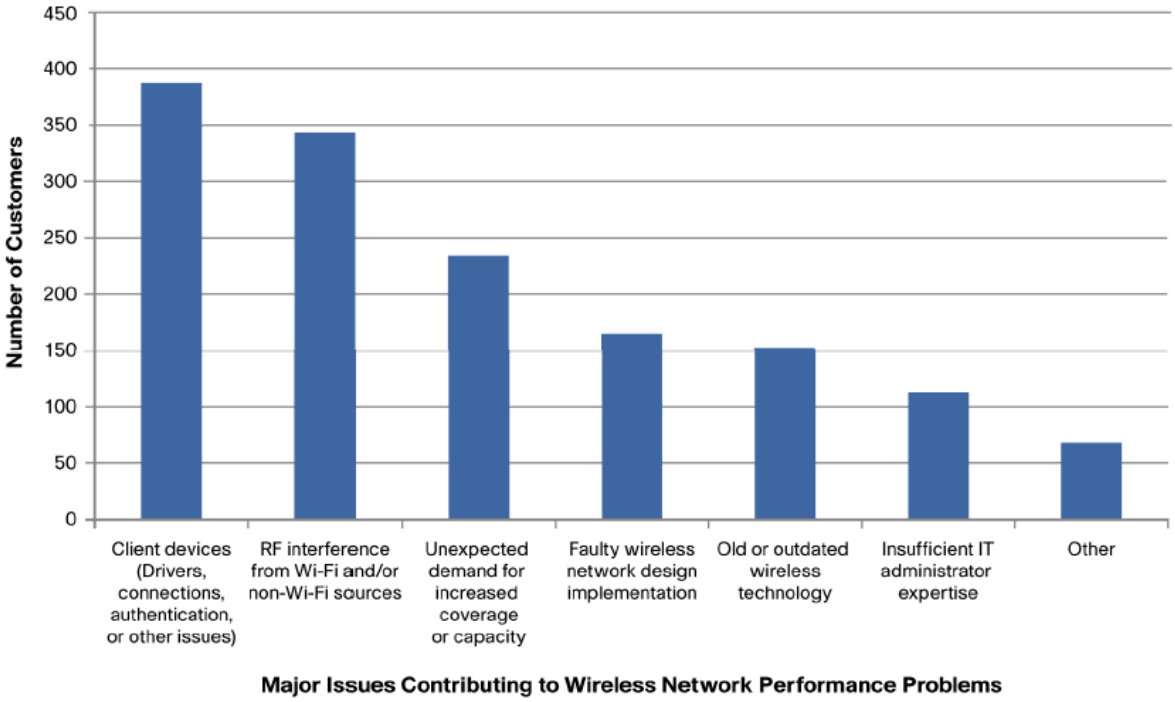
Langattoman lähiverkon suorituskyky on riippuvainen ensisijaisesti siirtotiestä. Siirtotiellä olevat erilaiset häiriölähteet ja esteet ovat verkon ylläpidon ja luotettavuuden kannalta suurin haaste. Signaalin etenemiseen merkittävimmin vaikuttavien fyysisten esteiden vaikutus otetaan tavallisesti huomioon jo verkon suunnitteluvaiheessa, mutta kaikkea ajan kuluessa siirtotielle tilapäisesti tai pysyvästi ilmaantuvaa sähkömagneettista häiriösäteilyä ei voida ennakoida. Suunnittelussa ei välttämättä voida varautua myöskään siihen, miltä verkon kattama ympäristö näyttää fyysisesti tulevaisuudessa, joten kaikkia esteitäkään ei voida ottaa etukäteen huomioon. Laadun heikentyminen tarkoittaa usein heikkoa signaalia ja sen myötä epäluotettavuutta tiedonsiirrossa. Kun signaali ei yllä teholtaan vaadittavaan herkkyystasoon, otetaan käyttöön toiminnallisuuden mahdollistava matalampi herkkyystaso, mikä tarkoittaa käytännössä alhaisempaa tiedonsiirtonopeutta, kuten liitteen 2 käytännön esimerkki osoittaa. Mikäli alin herkkyysraja jää saavuttamatta, yhteyttä ei voida muodostaa.

Tietoturvan rooli langattoman lähiverkon laadun takaamisessa on estää verkkoon murtautuminen ja luvaton käyttö, joka varsinkin suuressa mittakaavassa vie resursseja muulta tiedonsiirrolta.

Vuonna 2010 markkinoiden johtava verkkolaitevalmistaja Cisco Systems, Inc. teetti verkossa langattomien lähiverkkojen suorituskykyä ja siihen liittyviä ongelmia kartoittavan kyselyn, johon osallistui 600 asiakasta. Vastaajakanta kattoi 28 eri toimialaa, ja vastaajat olivat pääosin yhdysvaltalaisia. Kyselyn tuloksista tärkeimpinä seikkoina ilmeni, että yrityksistä 78 % koki ainakin osan langattoman verkkonsa toiminnasta kriittiseksi yrityksen toiminnan kannalta. 54 %:ssa yrityksistä todettiin muun radioliikenteen häiritsevän yrityksen langattoman lähiverkon toimintaa, ja 18 % yrityksistä ei osannut

sanoa, vaikuttaako muu radioliikenne yrityksen langattoman verkon toimintaan. (Cisco Systems, Inc. 2010, 1.)

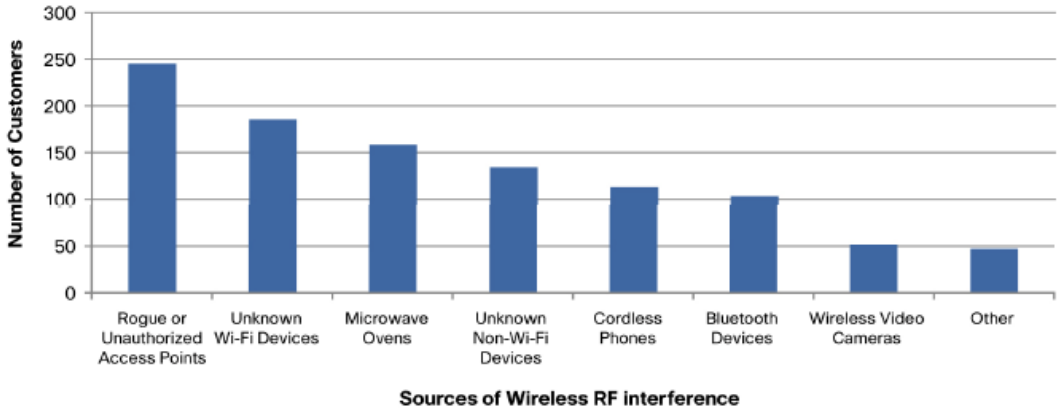
Kuviossa 16 on esitetty kyselytuloksiin pohjautuen graafisesti langattoman verkon toimintaa hankaloittavat asiat. Merkittävästi häiritseviksi tekijöiksi koettiin aiemmin mainitun ulkopuolisen radioliikenteen lisäksi verkkolaitteisiin liittyvät ongelmat, minkä lisäksi ongelmatilanteita olivat aiheuttaneet puutteet verkon suunnittelussa, vanhentuneiden verkkotekniikoiden käyttö sekä riittämätön asiantuntemus verkon ylläpidossa.



KUVIO 16: Yhteysongelmia aiheuttavat tekijät (Cisco Systems, Inc. 2010, 2.)

4.2 Laatuun vaikuttavat häiriölähteet

Samassa kyselyssä muusta radioliikenteestä aiheutuneista häiriöistä pyydettiin tarkempaa tietoa. Vastaukset on esitetty graafisesti kuviossa 17.



KUVIO 17. Muusta radioliikenteestä aiheutuneet häiriöt (Cisco Systems, Inc. 2010, 3.)

Vastanneiden keskuudessa merkittävimmäksi häiriölähteeksi koettiin valvomattomat tukiasemat. Muita mainittavia häiriölähteitä olivat muut tuntemattomat WLAN laitteet, mikroaaltouunit ja muut tuntemattomat laitteet, langattomat puhelimet, Bluetooth-laitteet ja langattomat videokamerat.

4.2.1 Valvomattomat langattomat tukiasemat

Valvomattomat langattomat tukiasemat ovat tukiasemia, jotka on asetettu samalle peittoalueelle, mutta jotka ovat jonkin muun tahon hallinnoimia. Ympäristöstä riippuen tällaiset tukiasemat voivat olla luvattomia tai pahimmassa tapauksessa asetettu vain häiritsemään alueen tietoliikennettä.

Kuten standardeihin keskittyneessä luvussa todettiin, erityisesti standardien IEEE 802.11b/g/n käyttämällä 2,4 GHz:n taajuusalueella voidaan helposti aiheuttaa häiriöitä, jos radiokanavaksi valitaan sama kanava kuin toisen verkon liikennöinnistä vastaavassa tukiasemassa. Häiriöitä aiheutuu myös, jos liikennöintiin valitaan sellainen kanava, joka ei täytä 25 MHz:n taajuusvälin ehtoa muiden samalla peittoalueella käytettyjen radiokanavien suhteen.

Useat langattomat tukiasemat tarkkailevat omatoimisesti ympäristöään ja signaalitasojaan, jolloin ne voidaan asettaa vaihtamaan kanavaa automaattisesti sen mukaan, millä kanavalla signaalin laatu on korkein. Tällöin voidaan teoriassa välttää pahimmat häiriötilanteet. Mikäli yhteisellä peittoalueella on yli kolme 2,4 GHz:n taajuusaluetta käyttävää tukiasemaa, jotka kaikki ylläpitävät eri lähiverkkoja, tilanne on jo huomattavasti haastavampi.

4.2.2 Tuntemattomat WLAN-laitteet

Tuntemattomat WLAN-laitteet ovat tavallisesti naapuriverkkojen laitteita, langattomia siltoja ja aiempien asukkaiden jättämiä langatonta lähiverkkoa hyödyntäviä laitteita (Cisco Systems, Inc. 2010, 3). Näihin laitteisiin pätevät pitkälti samat asiat kuin aiemmin käsiteltyihin valvomattomiin tukiasemiin. Nämä asiat erottaa oikeastaan se, että häiritsevän laitteen ei tarvitse olla tukiasema; esimerkiksi päätelaitteissa on yhtälailla lähetin-vastaanottimet, jotka voivat aiheuttaa häiriöitä.

4.2.3 Muut samaa taajuusaluetta käyttävät laitteet

Koska ISM-taajuusalueet ovat julkisesti käytettävissä, on olemassa myös muita langattoman tiedonsiirron tekniikoita, jotka hyödyntävät niitä. Eräs esimerkki tästä on WPAN-tekniikoihin (Wireless Personal Area Network) eli henkilökohtaisiin verkkoihin lukeutuva ja IEEE 802.15 -standardiperheeseen kuuluva Bluetooth, joka liikennöi 2,4 GHz:n taajuusalueella. Myös monet langattomat puhelimet ja peliohjaimet käyttävät tätä samaa taajuusaluetta. (Cisco Systems, Inc. 2010, 3; Porras 2009b, 8.)

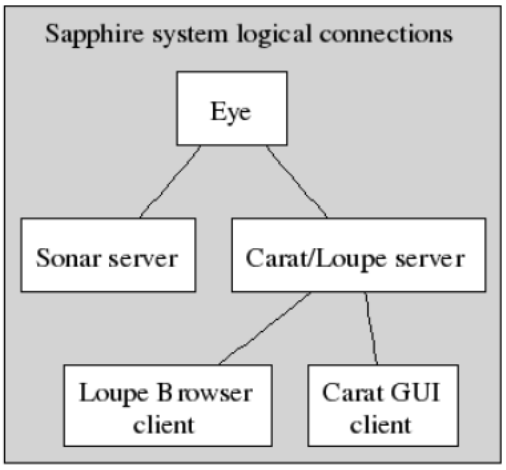
Langattomaan tiedonsiirtoon perustuvien laitteiden lisäksi on olemassa myös muita säteilylähteitä, joiden vaikutukset siirtotiellä voivat olla merkittäviä. Näistä esimerkkinä on kyselyssäkin esiin noussut mikroaaltouuni (Cisco Systems, Inc. 2010, 3).

5 7SIGNAL SAPPHIRE -LAADUNVALVONTARATKAISU

7 Signal Sapphire -laadunvalvontaratkaisu koostuu useasta komponentista, ja sillä voidaan valvoa langattomia lähiverkkoja erilaisin suoritettavin mittauksin. Tässä luvussa käsitellään laadunvalvontaratkaisun sisältöä ja ominaisuuksia.

5.1 Toimintaperiaate

Sapphire on kokonaisuus, joka koostuu tietokantaa pyörittävästä Carat-hallintapalvelimesta ja siihen liittyvästä web-pohjaisesta Loupe-seurantasovelluksesta sekä yhdestä tai useammasta Eyeksi nimetystä valvonta-asemasta. Näiden lisäksi verkkoympäristöön tulee asentaa Sonar-testipalvelin, jota vasten voidaan tehdä aktiivisia mittauksia. Sapphire-järjestelmän looginen kytkentä on esitetty kuviossa 18.



KUVIO 18. Sapphire-järjestelmän looginen kytkentä (7signal 2010b.)

5.2 Komponentit

5.2.1 Valvonta-asema

Valvonta-asema toimii sekä lähettimenä että vastaanottimena, ja se sisältää seitsemän ympärisäteilevää antennia. Antenneista kuusi on asetettu pystysuuntaisesti ja yksi vaakasuuntaisesti. Laitteeseen kuuluu osana myös GPS-vastaanotin (Global Positioning System), jota voidaan tarvittaessa hyödyntää erillisen antennin avulla. Pohjana jokaisella yksittäisellä valvonta-asemalla on Linux-käyttöjärjestelmä. (7signal 2010b, 6.)

Valvonta-asemilla voidaan tehdä sekä passiivisia että aktiivisia testejä. Passiivisella testillä voidaan kerätä yleistä tietoa ympäröivistä langattomista lähiverkoista ja niitä ylläpitävien tukiasemien lähettämistä signaaleista. Kun laite assosioidaan johonkin tiettyyn lähiverkkoon, sillä voidaan tehdä sen verkon piirissä aktiivisia testejä, jolla tutkitaan yhteyttä pääosin loppukäyttäjän näkökulmasta. Jotta valvonta-asema voidaan liittää verkkoon, tulee sen – työasemien ja muiden päätelaitteiden tavoin – läpäistä verkkoon turvallisuussyistä asetettu mahdollinen salaus. Aktiivisten mittausten suorittamiseksi testipalvelimen tulee tavallisesti olla laitteen saavutettavissa.

Valvonta-asemasta luodaan yhteys hallintapalvelimeen Ethernet-rajapinnan kautta, ja itse mittauksissa hyödynnetään radiotekniikkaa ja käytetään laitteen WLAN-rajapintaa. Vuoden 2010 ohjelmistossa on tuki langattoman lähiverkon standardeille IEEE 802.11a/b/g, mutta tukea on myöhemmin laajennettu kattamaan myös IEEE 802.11n -standardi. Ohjelmistotuen lisäksi on oltava myös radioltaan standardin kanssa yhteensopiva valvonta-asema, jotta mittauksia voidaan tehdä.

Valvonta-asemien huolto- ja konfigurointitehtäviin käytetään pääasiassa hallintapalvelimen graafista käyttöliittymää, mutta myös SSH-etäyhteys (Secure Shell) on mahdollinen ja valvonta-aseman aktiivisen hallinnoinnin kannalta jopa välttämätön.

5.2.2 Hallintapalvelin

Hallintapalvelimen tehtävänä on ylläpitää tietokantaa ja mahdollistaa yhteydet sekä valvonta-asemalta että seurantasovellusta pyörittävältä työasemalta tietokantaan. Palvelimen käyttöjärjestelmäksi suositellaan Red Hat Linuxiin pohjautuvaa CentOS 5.4 -jakelupakettia. Palvelimelle asennettavan graafisen käyttöliittymän avulla voidaan myös määrittää verkosta mitattavia ominaisuuksia, joita käsitellään luvussa 5.3.

5.2.3 Seurantasovellus

Seurantasovellus asennetaan osaksi hallintapalvelinta, ja se on tiiviisti yhteydessä tietokantaan. Näin ollen kerätyn tiedon tarkkailuun ja prosessointiin tarkoitettua web-pohjaista asiakasohjelmaa voidaan käyttää lähiverkon yli tai mahdollisuuksien mukaan myös ulkoverkosta käsin etänä.

5.2.4 Testipalvelin

Aktiivisissa mittauksissa käytettävä testipalvelinohjelma voidaan asentaa Microsoft Windows- tai Linux-pohjaiselle työasemalle. Ohjelman tarkoitus on olla loppukäyttäjän roolissa, mittauksiin liittyvän tiedonsiirron toisena päätepisteenä. Testipalvelinohjelmaa suorittavan työaseman tulee olla päällä ja yhdistettynä verkkoon langallisesti.

5.3 Mittaaminen

Mittaukset voidaan tehdä joko automaattisesti tai manuaalisesti. Automaattisia mittauksia varten luodaan testiprofiili, johon voidaan valita mittausvaihtoehtoja niin passiivisten kuin aktiivistenkin mittausten valikoimista.

Valikoista voidaan valita joko aktiivisia tai passiivisia mittauksia. Aktiivisista mittauksista eri vaihtoehtoja on esitelty ja selitetty liitteessä 1. Aktiivisten mittausten toteuttaminen edellyttää asennettua testipalvelinsovellusta testin kohteessa. Joissakin mittauksissa voidaan hyödyntää IEEE 802.11e -standardin mukaisia laatukategorioita; esimer-

kiksi FTP:hen (File Transfer Protocol) perustuva lähetys- tai vastaanottotesti voidaan tehdä best effort-, background-, video- tai voice-asetuksella. Lataustesteissä myös lähetettävien tai vastaanotettavien pakettien kokoja voidaan säädellä tiedonsiirtonopeuksien tarkempaa tutkimista varten.

5.4 Hälytykset

Hallintapalvelimen graafinen käyttöliittymä mahdollistaa myös tilauksen verkkoon liittyvien ongelmien ilmaisemiseen hälytysten muodossa. Hälytyksiä voidaan hallinnoida Alarms-valikosta. Osa vaihtoehdoista perustuu passiiviin ja osa aktiivisiin testeihin; ohjelmisto voidaan asettaa hälyttämään esimerkiksi kanavalla ilmenevän häirinnän, alueelle ilmestyneen tuntemattoman tukiaseman tai päätelaitteeseen katkenneen yhteyden perusteella. Tarvittaessa hälytykset voidaan asettaa lähetettäviksi sähköpostitse ylläpitäjälle.

6 MITTAUKSET

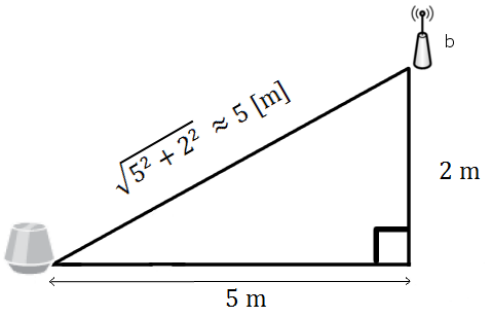
Tässä luvussa käsitellään esitellään 7signal Sapphire -laadunvalvontajärjestelmän käyttöönotto sekä järjestelmällä tehtyjä passiivisia mittauksia, joissa vertaillaan lähiverkon laatua häiriöttömässä ja häiriöllisessä tilassa. Käyttöönoton yhteydessä käsitellään myös testipalvelimen käyttöönotto, vaikka sitä ei hyödynnetty itse mittauksissa. Mittauksissa keskityttiin 2,4 GHz:n taajuusalueeseen ja IEEE 802.11g -standardiin.

6.1 Mittausten suunnittelu

Mittaukset toteutettiin käyttämällä 7signal Sapphire -järjestelmän ohjelmisto- ja laitekomponentteja. Hallintapalvelimessa käyttöjärjestelmänä käytettiin CentOS 5.4:ää ja testipalvelimessa Microsoft Windows 7:ää. Sapphiren ohjelmistokokonaisuudesta käytössä oli versio 2.2-0.2.

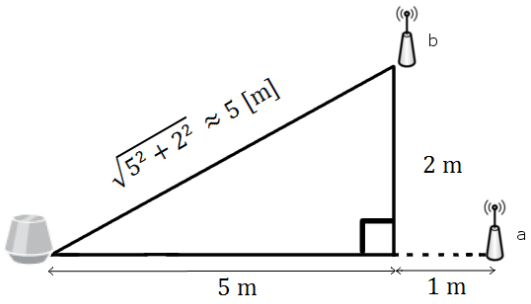
6.1.1 Mittausasetelmat

Mittausten lähtökohtana oli yrittää tarkoituksellisesti häiritä langattoman tukiaseman liikennöintiä. Häirinnän kohteeksi otettiin Tampereen ammattikorkeakoulun pääkampuksen syksyllä 2011 uusittu langaton verkko – ja käytännössä yksi verkkoa ylläpitävä langaton tukiasema –, ja häirintä toteutettiin 2,4 GHz:n taajuusalueella laboratoriotilassa muilla langattomilla tukiasemilla. Mittauksiin käytettiin yhtä valvonta-asemaa. Langatonta tiedonsiirtoa hyödyntävän laitteiston asettelu mittaustilanteeseen tehtiin aluksi kuvion 19 osoittamalla tavalla, jolla tarkoitus oli saada mahdollisimman vähähäiriöinen vertailukohta myöhemmille mittauksille. Kaikki laitteet olivat siis leveyssuunnassa suorassa linjassa toisiinsa nähden. Pystysuunnassa tarkasteltuna valvonta-asema oli samassa tasossa myöhemmissä vaiheissa asetelmaan lisättävien häiritsevien tukiasemien kanssa ja häirittävä tukiasema kahden metrin korkeudella tästä tasosta.



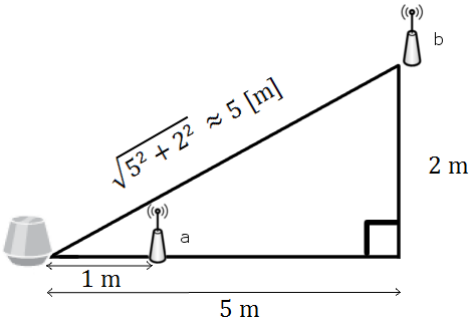
KUVIO 19. Mittausasetelmassa valvonta-asema ja häirittävä tukiasema (b)

Kuviossa 20 on esitetty muunneltu mittausasetelma, jossa tarkoituksena oli selvittää häiriöiden vaikutus tukiaseman signaaliin silloin kun häiriölähde on häirittävää asemaa kauempana päätelaitetta kuvastavasta valvonta-asemasta.



KUVIO 20. Mittausasetelmassa valvonta-asema, häiritsevä tukiasema (a) ja häirittävä tukiasema (b)

Viimeinen mittausasetelma on esitetty kuviossa 21. Häiritsevä tukiasema on siirretty lähemmäksi valvonta-asemaa, jolloin häirittävä tukiasema jää taka-alalle. Näin voidaan tutkia tilannetta, jossa häiriölähde on lähellä päätelaitetta.



KUVIO 21. Mittausasetelmassa valvonta-asema, häiritsevä tukiasema (a) ja häirittävä tukiasema (b)

Häirittävä tukiasema oli merkiltään ja malliltaan ZoneFlex 7363, jonka tiedettiin käyttävän tiedonsiirtoon IEEE 802.11n -standardia ja siten sekä 2,4 GHz:n että 5 GHz:n taajuusaluetta. Häiritsevänä tukiasemana käytettiin D-Link DI-524:ää ja ASUS RT-N56U:ta, joiden radioista otettiin käyttöön standardeja IEEE 802.11b/g käyttävä sekatila. Mittausten kannalta merkittävimpiä tietoja ja eroavaisuuksia näistä tukiasemista on kerätty taulukkoon 3 (Amazon 2012; D-Link Systems, Inc. 2012; Ruckus Wireless, Inc. 2012). Luvun 2.1 pohjalta voidaan ilmoitetuista arvoista ainakin maksimaalisiin lähetystehoihin suhtautua skeptisesti; todelliset arvot saavat olla Suomessa korkeintaan 20 dBm.

TAULUKKO 3. Tärkeimpiä tietoja laitteista

	ZoneFlex 7363	**D-Link DI-524**	**ASUS RT-N56U**
Lähetysteho, max (dBm)	29	15	19
Herkkyysraja, min (dBm)	-98	-89	?
Antennien lkm (2,4 GHz)	1	1	2
Antenni(e)n tyyppi	Sisäinen	Ulkoinen	Sisäinen
Beamforming	Kyllä	Ei	Ei

Tukiasemista ainoastaan D-Linkin valmistaman spesifikaatioissa mainittiin herkkyydet. Samoja arvoja arvioitiin voitavan käyttää ainakin viitteellisesti myös muiden tukiasemien signaaleja analysoitaessa. D-Link DI-524:n herkkyysrajat on esitetty liitteessä 2 (D-Link Systems, Inc. 2012).

Valvonta-asemalla tehtiin passiivisia mittauksia signaalien kartoittamiseksi. Testipalvelin jää näissä mittauksissa merkityksettömäksi, koska mittaukset toteutetaan vain passiivisin keinoin. Kuitenkin myös aktiivisia mittauksia valmistelevat käyttöönottovaiheet on esitelty.

6.1.2 Mittausverkon suunnittelu

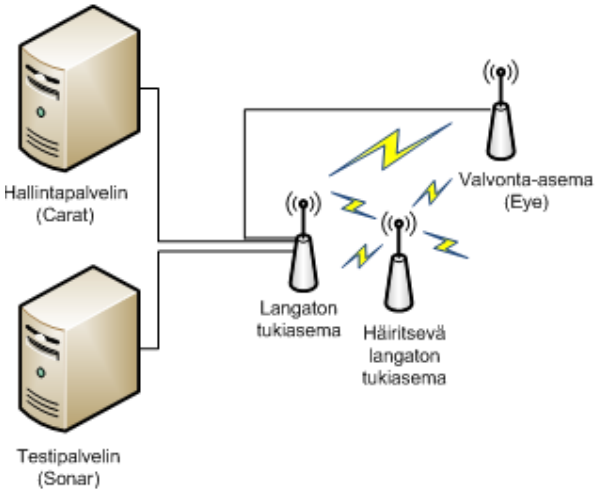
Mittauksia varten täytyi suunnitella lähiverkko, jotta tiedonsiirto laitteiden välillä olisi mahdollista. Koska mittauksissa käytettiin Tampereen ammattikorkeakoulun verkkoa, tietoturvasyistä alkuperäisiä IP-osoitteita ei tässä työssä voida julkaista. Taulukossa 4 on esitetty mittaukseen soveltuva vaihtoehtoinen verkko, jonka verkko-osoite on

192.168.0.0 /28. Aliverkkopeite 255.255.255.240 vastaa siis biteissä 28:aa, joka on osoitteen verkko-osa. 32 bitistä jää näin ollen neljä bittiä laiteosalle, ja aliverkon kooksi voidaan laskea 2^4 eli 16 osoitetta. Osoitteista ensimmäinen jää verkko-osoitteeksi ja viimeinen broadcast-osoitteeksi. Laitteita varten jäävät osoitteet väliltä 192.168.0.1-192.168.0.14, mikä riittää tämän mittakaavan mittausympäristöä varten.

TAULUKKO 4. Vaihtoehtoinen mittausverkko IP-osoitteineen

Laite	**IP-osoite (IPv4)**	**Aliverkkopeite**	**Rajapinta**
Langaton tukiasema	192.168.0.1	255.255.255.240	Ethernet/WLAN
Hallintapalvelin	192.168.0.2	255.255.255.240	Ethernet
Valvonta-asema	192.168.0.13	255.255.255.240	Ethernet/WLAN
Testipalvelin	192.168.0.5	255.255.255.240	Ethernet

Langattomissa tukiasemissa on usein valmiiksi sillattu WLAN- ja Ethernet-rajapinnat, jolloin ne ovat automaattisesti samassa lähiverkossa. Kuviossa 22 on esitetty mittauksissa käytetyn verkon topologia. Valvonta-asema on assosioitu myöhemmin luvussa 6.1 kuvaillulla tavalla langattomasti mittausverkkoon, ja häiritsevä tukiasema on verkon ulkopuolella.



KUVIO 22. Mittauksissa käytetyn verkon topologia

6.2 Järjestelmän käyttöönotto

Järjestelmän käyttöönotto aloitettiin asentamalla hallintapalvelin graafisine käyttöliittymineen ja siihen tietokanta sekä seurantasovellus. Yhteen työasemaan asennettiin testipalvelinohjelmisto aktiivisia mittauksia varten, ja kaikki laitteet liitettiin verkkoon. Valvonta-asema liitettiin hallintapalvelimeen graafisen käyttöliittymän esittämästä verkkotopologiasta. Laitteen on oltava verkossa ja saavutettavissa, joten mahdolliset palomuurisäännöt niin tukiasemissa kuin päätelaitteissakin oli myös huomioitava mittausverkkoa pystytettäessä. Assosiointi verkkoon aktiivisia mittauksia varten voitiin tehdä vasta ensimmäisen verkkohaun jälkeen varsinaisissa mittauksissa.

Mahdollisia myöhempiä aktiivisia mittauksia helpottamaan luotiin testiprofiili, jonka avulla voidaan suorittaa mittauksia automaattisesti. Testiprofiileja hallitaan graafisen käyttöliittymän Manage-välilehden takana olevasta Test Profiles -valinnasta. Valittavana on valmiita profiileja, mutta tässä yhteydessä haluttiin räätälöidä oma profiili. Testiprofiiliin saadaan valittua mittaus Elements-listasta valinnalla Copy Element, minkä jälkeen mittaus viedään testiprofiiliin Paste Test Profile Element -valinnalla. Verkkotopologiasta valitaan valvonta-asema, johon testiprofiilia halutaan käyttää ja sidotaan testiprofiili valinnalla Bind to Test Profile; tämä työvaihe toteutetaan loppuun asti, kun ensimmäinen verkkohaku on tehty ja assiosioitumisen kohteeksi soveltuva verkko löydetty. Testiprofiiliin valittiin tiedonsiirtonopeuden kartoittamiseksi FTP Download Test ja FTP Upload Test, joilla saadaan selville tiedonsiirtonopeus ylä- ja alavirtaan.

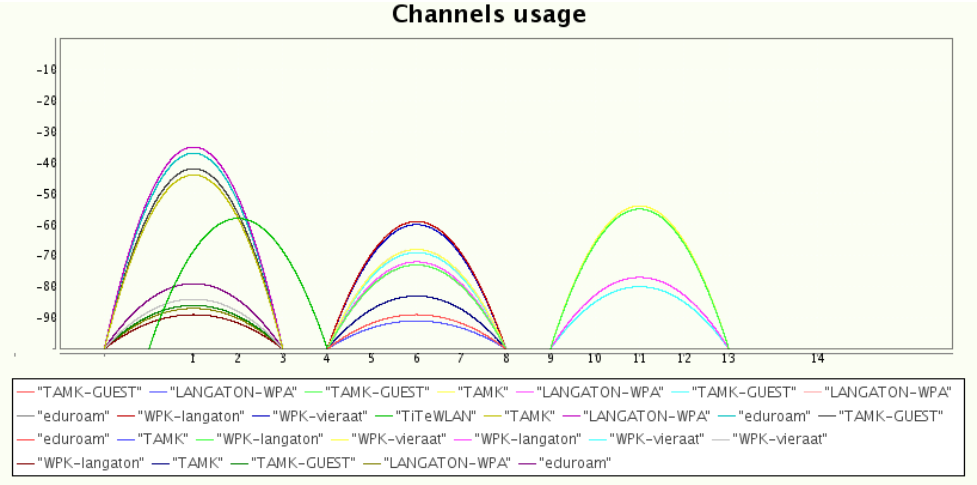
Aktiivisia mittauksia varten graafisen käyttöliittymän kautta luotiin myös valmis Sonar-profiili Manage-valikosta. Profiiliin liitettiin testipalvelimen IP-osoite. Työasemalla, jolle testipalvelinohjelmisto asennettiin, tulee käynnistää sovellus, jotta aktiivisia testejä voidaan suorittaa.

6.3 Mittaukset

Mittaukset koostuivat mahdollisimman häiriöttömään ympäristöön tähdänneestä alkutilanteesta sekä tilanteista, joissa pyrittiin häiritsemään alkutilanteessa käytettyä tukiasemaa. Mittausvaihtoehdoista käytettiin verkkohakua (Network Scan) ja siihen liittyviä kanavakäyttögraafeja (Channels Usage) sekä spektrianalysaattoria (Spectrum Analyzer).

6.3.1 Alkutilanne

Alkutilanteessa tehtiin verkkohaku, jonka perusteella havaittiin, että vahvin signaali saavutettiin radiokanavalla 1. Mittauksen pohjalta piirretty graafinen esitys kanavakäytöstä tuki tätä tulkintaa (kuvio 23). Kuviossa samat SSID:t (Service Set Identifier) toistuvat useaan kertaan, koska mittausympäristöön kantautuivat myös muiden samaa verkkoa ylläpitävien tukiasemia lähettämät signaalit.



KUVIO 23. Valvonta-aseman mittaama kanavakäyttö alkutilanteessa

Tärkeimmät mittaustulokset on esitetty liitteessä 3; liitteeseen on taulukoitu vahvimmat signaalin saavuttaneen tukiaseman rinnakkaiset SSID:t, jotka voitiin yhdistää samaan tukiasemaan sekä päättelemällä signaalitasojen voimakkuuksista että tukiaseman MAC-osoitteen perusteella. Mitattava tukiasema lähettää siis tietoa seuraavilla SSID:illä: eduroam, LANGATON-WPA, TAMK, TAMK-GUEST. Signaalin voimakkuus vaihteli -28 dBm:n ja -47 dBm:n välillä riippuen SSID:stä ja vastaanottavasta antennista.

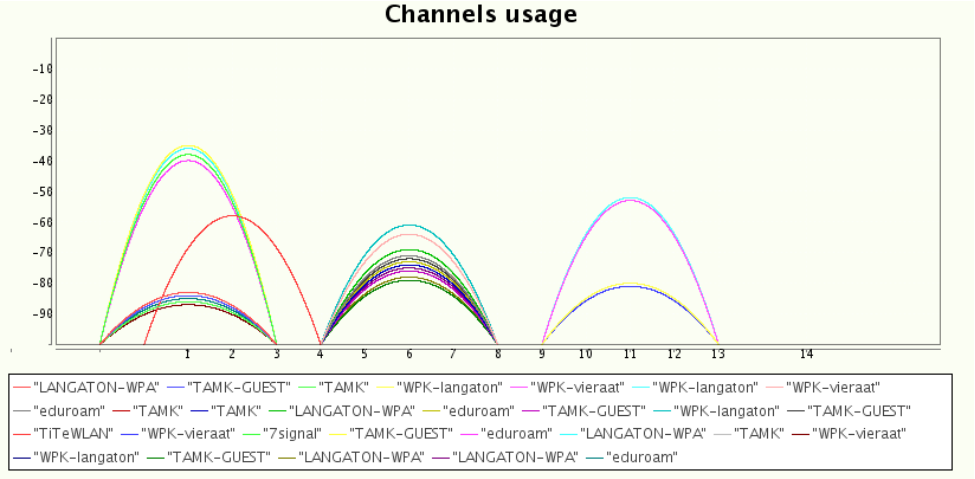
Verkkohaku tallennettiin mahdollisia myöhempiä aktiivisia testejä silmälläpitäen. Tallentamisen myötä verkkotopologiaan ilmestyivät kaikki havaitut langattomat lähiverkot, ja niistä hallinnoidut merkittiin Managed-statuksella. Jotta salattuun verkkoon voitiin assosioitua valvonta-asemalla, tuli Manage-valikon takaa määrittää verkon salauksen tyyppi ja salasana Network Keys -valinnasta. Kun verkkoavain oli luotu, se sidottiin mitattavaan verkkoon, minkä jälkeen assosioituminen oli mahdollista. Havaituista verkoista tähän valikoitui SSID:tä TAMK kantanut verkko, jota voitaisiin käyttää aktiivisissa testeissä myöhemmin.

Spektrianalysaattorilla tehdyssä testissä saatiin yleiskatsaus eri taajuuksien esiintymisestä taajuusalueella. Liitteessä 4 on esitetty spektrianalyysi alkutilanteesta. Myös spektrianalyysista havaitaan signaalin verrattain suuri voimakkuus radiokanavan 1 läheisyydessä. Koska spektrianalyysissa ei kuitenkaan eritellä signaalin voimakkuuden eri tekijöitä – eli tässä tapauksessa langattomia tukiasemia ja niiden SSID:itä –, ei toimintoa koettu näissä mittauksissa tarpeelliseksi.

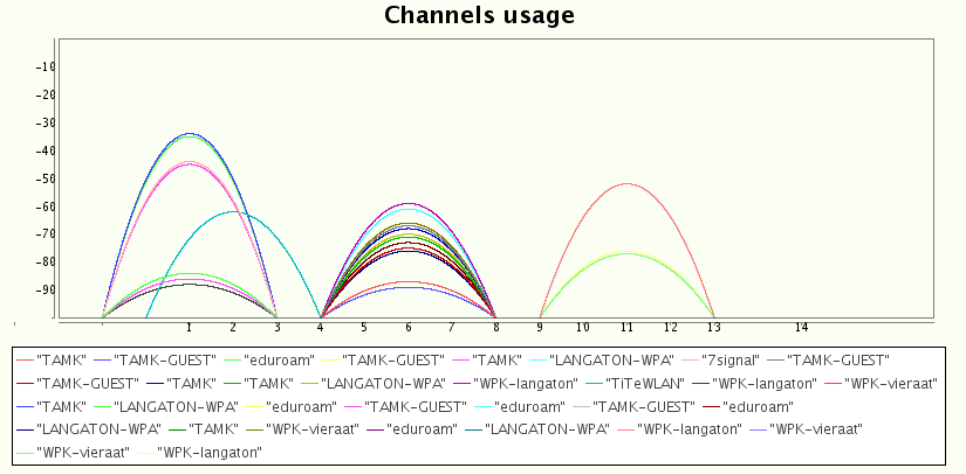
6.3.2 Häirintä ASUS RT-N56U:lla

Koska alkutilanteessa havaittiin lähimmän tukiaseman liikennöivän pääosin radiokanavalla 1, häiritsevä tukiasema pakotettiin käyttämään samaa kanavaa. Häirittävän tukiaseman mahdolliseen automaattiseen kanavanvaihtoon voitiin varautua tarkkailemalla verkkohaussa kanavakäyttöä ja alkutilanteessa selvinnyttä tukiaseman MAC-osoitetta suhteessa käytettävään kanavaan jatkossa.

Liitteessä 5 on esitetty vierekkäin tulokset mittauksista, joissa ASUS RT-N56U -tukiasema asetettiin SSID:llä 7signal ensin yhden metrin etäisyydelle valvonta-asemasta ja sen jälkeen kuuden metrin etäisyydelle valvonta-asemasta. Kuviossa 24 on esitetty graafi kanavakäytöstä, kun häiritsevä tukiasema on yhden metrin etäisyydellä ja kuviossa 25 kun tukiasema on kuuden metrin etäisyydellä mittaavasta valvonta-asemasta.



KUVIO 24. Kanavakäyttö häiritsevän tukiaseman ollessa yhden metrin etäisyydellä



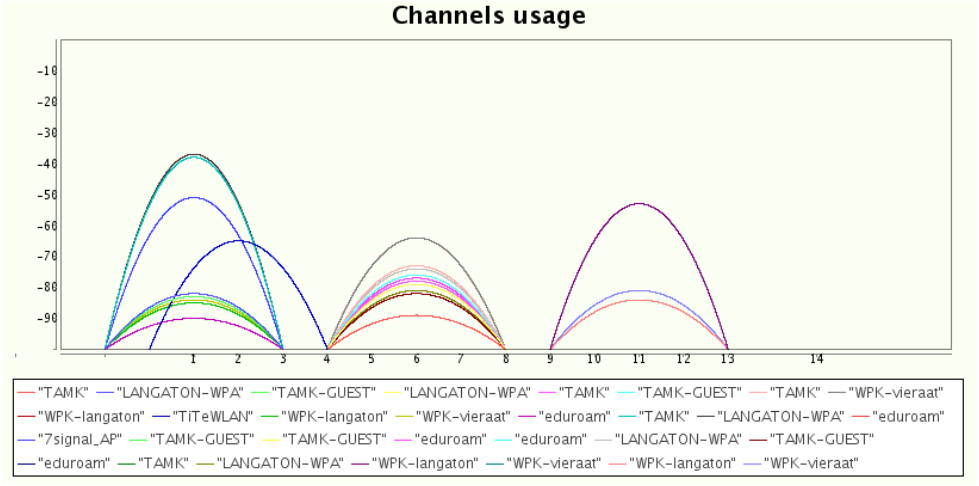
KUVIO 25. Kanavakäyttö häiritsevän tukiaseman ollessa kuuden metrin etäisyydellä

Häiritsevän tukiaseman lisääminen ympäristöön aiheutti hyvin pieniä muutoksia koulun tukiaseman lähettämiin signaaleihin. Muutokset olivat muutaman dBm:n suuruisia; kun häiritsevä tukiasema oli metrin etäisyydellä, signaalitaso vaihteli SSID:stä ja mitanneesta antennista riippuen -31 dBm:n ja -52 dBm:n välillä. Häiritsevän tukiaseman signaalitaso vaihteli -32 dBm:n ja -54 dBm:n mitanneesta antennista riippuen.

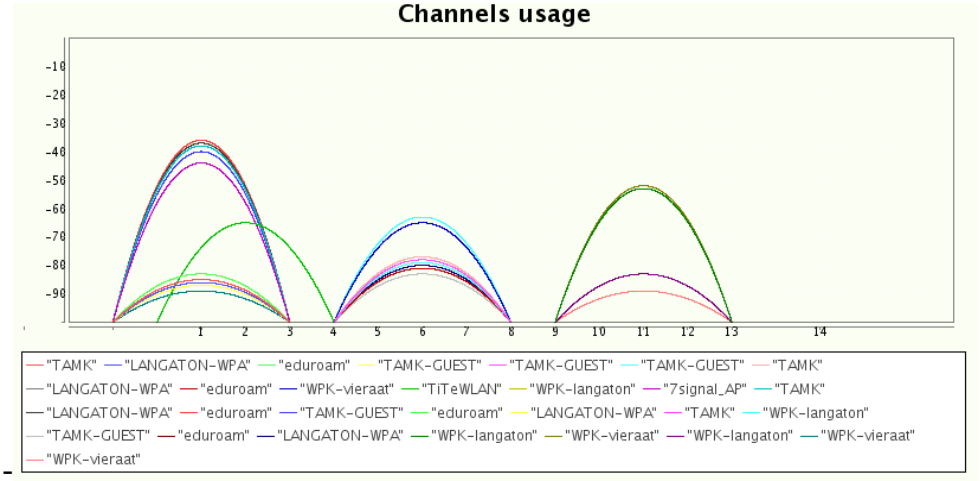
Kun häiritsevä tukiasema siirrettiin kuuden metrin päähän valvonta-asemasta, häiritsevän tukiaseman signaalitasot laskivat -38 dBm:n ja ja -54 dBm:n väliin. Koulun tukiaseman liikennöimän TAMK-GUEST-verkon signaalitasot nousivat merkittävästi saavuttaen parhaimmillaan signaalitason -26 dBm. Muutoin signaalitasot vaihtelivat -26 dBm:n ja -52 dBm:n välillä. Tässä mittauksessa valvonta-aseman antennilla 1 ei saatu mittaustuloksia kummallekaan näistä tukiasemista. Mittausten ulkopuolella olleiden tukiasemien signaaleista saatiin tuloksia kaikilla antenneilla.

6.3.3 Häirintä D-Link DI-524:llä

Häiritseväksi tukiasemaksi vaihdettiin D-Link DI-524, ja häiriömittaus toistettiin samoilla etäisyyksillä. Verkkohaun tulokset on esitetty liitteessä 6 ja kanavakäyttö kuvioissa 26 ja 27.



KUVIO 26. Kanavakäyttö häiritsevän tukiaseman ollessa yhden metrin etäisyydellä



KUVIO 27. Kanavakäyttö häiritsevän tukiaseman ollessa kuuden metrin etäisyydellä

Kun häiritsevä tukiasema asetettiin yhden metrin etäisyydelle mittaavasta valvonta-asemasta, koulun verkkojen signaalitasot vaihtelivat -31 dBm:n ja -54 dBm:n välillä. Häiritsevän tukiaseman signaalitasot vaihtelivat -39 dBm:n ja -53 dBm:n välillä.

Kun häiritsevä tukiasema siirrettiin kuuden metrin etäisyydelle valvonta-asemasta, koulun verkkojen signaalitasot nousivat kokonaisuudessaan hieman, jolloin arvot vaihtelivat -27 dBm:n ja -50 dBm:n välillä. Häiritsevän tukiaseman signaalitasot olivat -37 dBm:n ja -55 dBm:n väliltä; hajonta oli huomattavasti suurempaa kuin lyhyemmällä etäisyydellä.

7 POHDINTA

7.1 Mittaukset

Mittaukset sujuivat kaksijakoisesti. Passiiviset mittaukset onnistuivat hyvin, mutta aktiivisia mittauksia ei voitu toteuttaa yhteys- ja ohjelmistovirheiden vuoksi. Tavallisimmaksi ongelmaksi tässä suhteessa muodostui se, että vaikka kaiken voitiin todeta toimivan niin ping-testien kuin hallintapalvelimen ja valvonta-aseman sisältämien verify-terminaalikomentojen perusteella, varsinkin langallinen paluuyhteys valvonta-asemalta hallintapalvelimelle tuntui katkeavan kriittisissä vaiheissa.

Passiivisten mittausten tuloksissa odotettiin olevan mittausvaiheiden välillä suurempia eroavaisuuksia signaalien teholukemissa kuin mittaustuloksissa lopulta näkyi. Kuitenkin alkutilannetta ja häirintätilanteita verratessa voitiin havaita muutamien dBm:ien laskuja signaaliarvoissa. Häiritsevistä tukiasemista kahden antennin järjestelmässä signaalitaso vaikutti yltävän korkeampiin signaaliarvoihin kuin yhtä antennia hyödyntävä häiritsevä tukiasema. Herkkyysrajoihin joko viitteellisesti tai – jälkimmäisen häiritsevän tukiaseman kohdalla – suoraan verratessa voitiin kuitenkin todeta, että molemminpuolisesta häirinnästä huolimatta missään vaiheessa yksikään tukiasema ei ollut lähellä joutua laskemaan tiedonsiirtonopeuttaan yhteyden ylläpitämiseksi. Todelliset tiedonsiirtonopeudet olisi voinut saada selvitettyä esimerkiksi aktiivisilla FTP-mittauksilla. Huomionarvoista oli myös se, että häiritsevät tukiasemat kärsivät signaalitasojen perusteella häirintätilanteista enemmän kuin itse häirittävä tukiasema.

Mittausympäristö oli fyysisesti haastava, sillä laboratoriotila ei ollut kovin suuri ja ympäristössä olleet esteet tarjosivat tukiasemille monipuoliset mahdollisuudet hyödyntää monitie-etenemistä voimakkaamman signaalin saavuttamiseksi. Toisaalta myös häirittävä tukiasema oli haastava kohde, sillä sitä ei voitu hallinnoida ja sen käyttämä beamforming-tekniikka saattoi antaa sille huomattavan edun saavuttaa korkeampi signaalitaso.

Mittauksissa saatiin kuitenkin havainnollistettua jossain määrin häiriöiden vaikutusta langattomassa tiedonsiirrossa. Häiriöt ovat kuitenkin iso osa laatukysymystä langattomien lähiverkkojen kohdalla, kuten Cisco Systems, Inc.:n teettämä kyselykin osoitti.

7.2 Laadunvalvonnan sovelluskohteet

Esitellyn 7signal Sapphiren kaltaiset laadunvalvontajärjestelmät sopivat pitkällä aikajänteellä erityisesti sellaisiin ympäristöihin, joissa langaton lähiverkko on toiminnan kannalta kriittisessä asemassa; toimistot, tehdasympäristöt ja sairaalat ovat hyviä esimerkkejä tästä. Lyhyemmän aikajänteen käytössä sovelluskohteiksi voisivat sopia tilanteet, joissa jo olemassa olevaan langattomaan lähiverkkoon halutaan tehdä muutoksia. Laadunvalvontatyökaluilla voidaan tällöin tarkkailla muutoksen vaikutuksia mahdollisten suunnitteluvirheiden varalta. Jos suunnittelutyö aloitetaan puhtaalta pöydältä, on markkinoilla olemassa myös lukuisia yksinkertaisia site survey -työkaluja, joilla voidaan tutkia peittoalueita ja signaalitasoja.

Toisaalta tiedonsiirtotekniikoiden ja standardien kehittyessä laatuun vaikuttavat ongelmat vaikuttavat jäävän pienempään rooliin. Esimerkiksi tänä päivänä MIMO-tekniikoilla, 5 GHz:n taajuusalueen hyödyntämisellä ja beamforming-tekniikalla voidaan välttää useat häiritsevien radioaaltojen aiheuttamat ongelmat. Osansa on myös sillä, että uusien tiedonsiirtotekniikoiden ja standardien myötä on mahdollista saavuttaa vanhoihin standardeihin verrattuna samaa teholuokkaa olevilla signaalitasoilla myös korkeampia tiedonsiirtonopeuksia, jolloin häiriöiden vaikutus tiedonsiirtonopeuksissa ei välttämättä ole enää niin merkityksellinen.

7.3 Kehittämisehdotukset

Tässä työssä ei voitu tehdä aktiivisia mittauksia, joten jatkossa vastaavia mittauksia tehdessä olisi tärkeää saada tehtyä myös niitä. Tällöin saataisiin paremmin esiin se, miten häirintä vaikuttaa päätelaitteen toimintaan. Mielenkiintoista olisi myös vaihtaa langaton mittausympäristö standardista IEEE 802.11g standardiin IEEE 802.11n, joka on huomattavasti nykyaikaisempi ja monipuolisempi. Mittausten kannalta olisi oleellista, että mitattava verkko ja erityisesti tukiasema olisi hallittavissa, jolloin voitaisiin tutkia vastaavanlaista tilannetta esimerkiksi ilman beamformingin vaikutusta.

LÄHTEET

7signal 2010a. 7signal Sapphire Carat User Guide.

7signal. 2010b. 7signal Sapphire Deployment Guide.

Adrio Communications. 2012a. 802.11e for QoS. Luettu 2.12.2012.
http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11e.php

Adrio Communications. 2012b. Antennas and propagation. Electromagnetic waves and antenna basics. Luettu 18.10.2012.
http://www.radio-electronics.com/info/antennas/basics/emwaves.php

Adrio Communications. 2012c. Antennas and propagation. MIMO Formats - SISO, SIMO, MISO, MU-MIMO. Luettu 26.11.2012.
http://www.radio-electronics.com/info/antennas/mimo/formats-siso-simo-miso-mimo.php

Adrio Communications. 2012d. RF topics. OFDM Basics Tutorial. Luettu 26.11.2012.
http://www.radio-electronics.com/info/rf-technology-design/ofdm/ofdm-basics-tutorial.php

Adrio Communications. 2012e. Wireless technologies. Wi-Fi / WLAN channels, frequencies and bandwidth. Luettu 26.11.2012.
http://www.radio-electronics.com/info/wireless/wi-fi/80211-channels-number-frequencies-bandwidth.php

Agilent Technologies. 2009. Transforming MIMO Test With Fast, Accurate Signal Creation, Signal Analysis, and Protocol Development and Conformance. Luettu 7.11.2012.
http://www.agilent.com/about/newsroom/tmnews/background/N5106A/index.html

Armstrong, J. 2002. OFDM – Orthogonal Frequency Division Multiplexing. Luettu 28.10.2012.
http://www.ctie.monash.edu.au/ofdm/sample_files/armstrong_ofdm.pdf

Amazon. ASUS Black Diamond Dual-Band Wireless-N 600 Router (RT-N56U). Key Features. Luettu 8.12.2012.
http://www.amazon.com/Diamond-Dual-Band-Wireless-N-Router-RT-N56U/dp/B0049YQVHE

Chien, L.K. 2007. Resource Control for the EDCA and HCCA Mechanisms in IEEE 802.11e Networks. Luettu 2.12.2012.
http://mnet.cs.nthu.edu.tw/paper/9562616/070301.pdf

Cisco Systems, Inc. 2007. Omni Antenna vs. Directional Antenna. Luettu 7.11.2012.
http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a00807f34d3.shtml

Cisco Systems, Inc. 2008. Wi-Fi Protected Access (WPA) in a Cisco Unified Wireless Network Configuration Example. Luettu 4.12.2012.

http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a008095382f.shtml

Cisco Systems, Inc. 2010. Wireless RF Interference Customer Survey Results. Luettu 10.6.2012.
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps10981/white_paper_c11-609300.pdf

D-Link Systems, Inc. 2012. 802.11g Wireless Broadband Router, DI-524. Luettu 8.12.2012.
http://www.dlink.com/us/en/home-solutions/connect/routers/di-524-high-speed-2-4ghz-802-11g-wireless-router

Frenzel, L. 2006. Wi-Fi's Five Pronged Attack Alters The Wireless Landscape. Luettu 10.10.2012.
http://electronicdesign.com/article/communications/wi-fi-s-five-pronged-attack-alters-the-wireless-la

Haugdahl, J.S. 2007. Inside 802.11n Wireless LANs. Practical Insights and Analysis. Luettu 14.10.2012.
https://learningnetwork.cisco.com/servlet/JiveServlet/previewBody/3876-102-1-10914/Inside%20802.1s1n%20Wireless%20LANs%20-%20Practical%20insides%20and%20Analysis.pdf

Holt, A. & Huang C-Y. 2010. 802.11 Wireless Networks. Security and Analysis. Iso-Britannia: Springer.

Institute of Electrical and Electronics Engineers. 1996. Frequency Hopping Spread Spectrum PHY of the 802.11 Wireless LAN Standard. Luettu 22.10.2012.
http://grouper.ieee.org/groups/802/11/Tutorial/FH.pdf

Institute of Electrical and Electronics Engineers. 2007. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE 802®: Local and Metropolitan Area Network Standards. Luettu 4.12.2012.
http://standards.ieee.org/getieee802/download/802.11-2007.pdf

Institute of Electrical and Electronic Engineers. 2012. Official IEEE 802.11 Working Group Project Timelines - 2012-11-16. Luettu 28.11.2012.
http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

Gast, Matthew S. 2002. 802.11® Wireless Networks: The Definitive Guide. Yhdysvallat: O'Reilly Media.

Juutilainen, M. 2007a. Radiotekniikan perusteet: signaalien eteneminen. Luettu 22.10.2012.
http://www2.it.lut.fi/kurssit/06-07/Ti5312600/luentokalvot/luento03.pdf

Juutilainen, M. 2007b. Radiotekniikan perusteet: Yhteyden hallinta (MAC). Luettu 22.10.2012.
http://www2.it.lut.fi/kurssit/06-07/Ti5312600/luentokalvot/luento06.pdf

Juutilainen, M. 2007c. Radiotekniikan perusteet: Modulaatio. Luettu 22.10.2012. http://www2.it.lut.fi/kurssit/06-07/Ti5312600/luentokalvot/luento05.pdf

Masica, K. 2007. Securing WLANs using 802.11i. Luettu 2.9.2012. http://www.us-cert.gov/control_systems/practices/documents/Wireless%20802.11i%20Rec%20Practice.pdf

Matic, D. 1999. Mathematical description of OFDM. Luettu 28.10.2012. http://www.wirelesscommunication.nl/reference/chaptr05/ofdm/ofdmmath.htm

Molisch, A. 2011. Wireless Communications. 2. painos. Iso-Britannia: John Wiley & Sons Ltd.

Mäkelä, M., Soininen, L., Tuomola, S., Öistämö, J. 2005. Tekniikan kaavasto. 5. painos. Hämeenlinna: Karisto Oy.

Nobel, R., Lovison, F., Riesen, F., Vangrunderbeek, E., Ziliotto, F. 2012. Planning and Designing 802.11 Wireless Technologies. IEEE 802.11 Standards and Protocols. Luettu 14.10.2012. http://www.ciscopress.com/articles/article.asp?p=1873028&seqNum=3

Phoenix Contact. 2012. WLAN. Luettu 26.11.2012. http://www.phoenixcontact.fi/technologies/18699_18716.htm

Porras, J. 2009a. Luento 8 – WiFi (WLAN). Luettu 22.10.2012. http://www2.it.lut.fi/kurssit/08-09/CT30A2600/luennot/CT30A2600%20luento8%20WLAN.pdf

Porras, J. 2009a. Luento 8 - WPAN. Luettu 3.12.2012. http://www2.it.lut.fi/kurssit/08-09/CT30A2600/luennot/CT30A2600%20luento9%20WPAN.pdf

Prasad, R. 2004. OFDM for Wireless Communications Systems. Iso-Britannia: Artech House.

Rapidtables.com. 2012. dB to mW Conversion. Luettu 8.12.2012. http://www.rapidtables.com/convert/power/dBm_to_mW.htm

Ruckus Wireless, Inc. 2012. ZoneFlex™ 7300 Series. Luettu 8.12.2012. http://c541678.r78.cf2.rackcdn.com/datasheets/ds-zoneflex-7300-series.pdf

Schulz, B. 2011. Rohde & Schwarz. LTE Transmission Modes and Beamforming. Luettu 26.11.2012. http://www2.rohde-schwarz.com/file_17063/1MA186_0e.pdf

Thomas, T. 2005. Verkkojen tietoturva. Helsinki: Edita.

Toivonen, T. Säteilyturvakeskus. Väestön altistuminen radiotaajuisille kentille Suomessa. Luettu 8.12.2012. http://www.stuk.fi/julkaisut/tr/stuk-tr5.pdf

Väärämäki, T. 2007. WLAN ja Quality of Service. Luettu 2.12.2012.
http://users.jyu.fi/~timoh/kurssit/verkot/lecture5.pdf

Ward, L. 2012. Rohde & Schwarz. 802.11ac Technology Introduction. Luettu 27.11.2012.
http://www2.rohde-schwarz.com/file_18206/1MA192_7e.pdf

Wi-Fi Alliance. 2012. TKIP. Luettu 4.12.2012.
http://www.wi-fi.org/knowledge-center/glossary/tkip

Wrexler, J. How 802.11n backward compatibility works. Luettu 14.10.2012.
http://www.arnnet.com.au/article/147912/how_802_11n_backward_compatibility_works/

LIITTEET

Liite 1. 7signal Sapphire -järjestelmän aktiiviset mittausvaihtoehdot

Mittausvalinta	**Kuvaus**
Noise Monitor	Valvonta-asema tarkkailee tukiaseman lähettämän signaalin kohinaa.
Optimal Antenna Selection	Valvonta-asema mittaa signaalin voimakkuuden antenneissa, minkä perusteella voidaan todeta mittauksiin parhaiten soveltuva antenni.
UDP Download Test	Valinnalla mitataan tiedonsiirtonopeus testipalvelimelta valvonta-asemalle halutulla määrällä halutun kokoisia UDP-paketteja.
UDP Upload Test	Valinnalla mitataan tiedonsiirtonopeus valvonta-asemalta testipalvelimelle halutulla määrällä halutun kokoisia UDP-paketteja.
FTP Download Test	Valinnalla mitataan tiedonsiirtonopeus testipalvelimelta valvonta-asemalle halutulla määrällä halutun kokoisia FTP-paketteja.
FTP Upload Test	Valinnalla mitataan tiedonsiirtonopeus valvonta-asemalta testipalvelimelle halutulla määrällä halutun kokoisia FTP-paketteja.
Ping Test	Valinnalla mitataan ping-työkalua hyväksikäyttäen halutun kokoisten ICMP-pakettien lähetyksen ja sitä seuraavan vastauksen vastauksen välistä aikaa.
Traceroute Test	Valinnalla voidaan selvittää reitti lähdelaitteesta kohdelaitteeseen.
Access Point Traffic	Valinnalla voidaan tarkkailla tukiaseman tietoliikennettä.
Client Scan	Valinnalla voidaan kerätä tietoa siitä, mitkä laitteet siirtävät dataa tukiaseman kautta.
MOS Test	Valinnalla voidaan mitata verkon yli olevan puhe- tai kuvayhteyden laatua.
Air Utilization Test	Valinnalla voidaan tarkkailla langattoman yhteyden käyttöä ja verkossa käytettäviä tiedonsiirtonopeuksia.
HTTP URL (Intranet) Test	Valinnalla voidaan tarkkailla pääosin sitä, kuinka nopeasti yhteydellä voidaan avata WWW-sivu.
Internet Availability Test	Valinnalla voidaan tutkia pääsyä lähiverkosta Internetiin.
SIP Register Test	Valinnalla testataan SIP-protokollan toimivuutta verkon yli.

(7signal 2010a, 65–80.)

Liite 2. D-Link DI-524:n herkkyysrajat

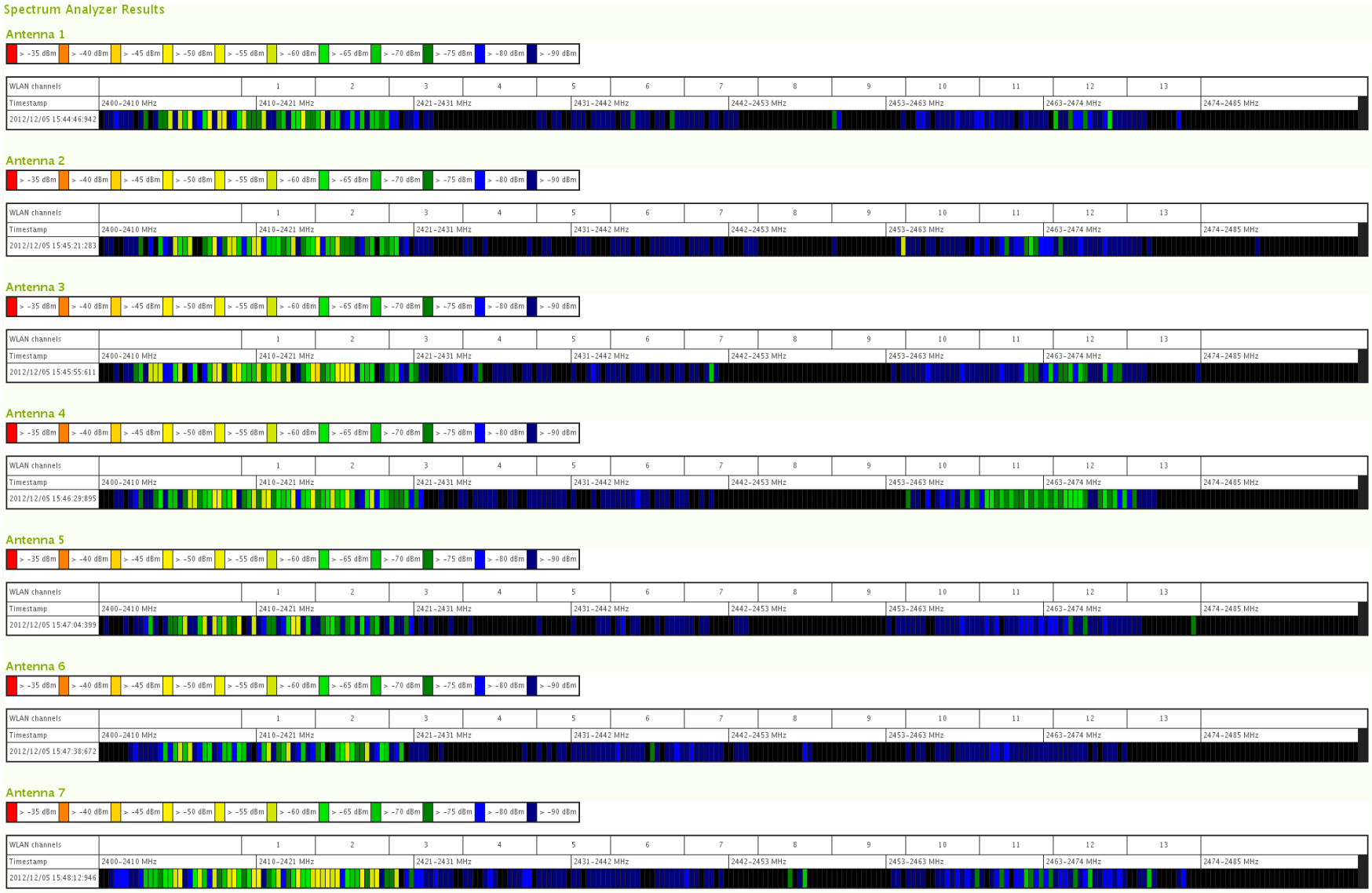
Tiedonsiirtonopeus (Mb/s)	Lähetystekniikka	Herkkyysraja (dBm)
54	OFDM	-68
48	OFDM	-68
36	OFDM	-75
24	OFDM	-79
18	OFDM	-82
12	OFDM	-84
11	CCK	-82
9	OFDM	-87
6	OFDM	-88
5,5	CCK	-85
2	QPSK	-86
1	BPSK	-89

(D-Link Systems, Inc. 2012.)

Liite 3. Valvonta-asemalla mitatut tukiasemien signaaliarvot (alkutilanne)

SSID	Antenni	Signaalitaso (dBm)	Kohinataso (dBm)
eduroam	1	-37	-93
	2	-35	-94
	3	-46	-94
	4	-48	-95
	5	-42	-95
	6	-33	-90
	7	-44	-94
LANGATON-WPA	1	-35	-93
	2	-40	-94
	3	-28	-94
	4	-46	-95
	5	-46	-94
	6	-35	-93
	7	-28	-94
TAMK	1	-44	-92
	2	-36	-94
	3	-47	-94
	4	-39	-95
	5	-48	-94
	6	-42	-90
	7	-37	-95
TAMK-GUEST	1	-42	-93
	2	-40	-95
	3	-44	-94
	4	-45	-95
	5	-44	-95
	6	-44	-90
	7	-44	-94

Liite 4. Spektrianalyysi alkutilanteesta



Liite 5. Valvonta-asemalla mitatut tukiasemien signaaliarvot (häiriötilanne 1)

		Etäisyys: 1 m		Etäisyys: 6 m	
SSID	**Antenni**	**Signaalitaso (dBm)**	**Kohinataso (dBm)**	**Signaalitaso (dBm)**	**Kohinataso (dBm)**
7signal (ASUS RT-N56U)	1	-32	-94	-	-
	2	-44	-95	-38	-95
	3	-36	-93	-40	-92
	4	-34	-95	-53	-95
	5	-54	-95	-54	-95
	6	-43	-95	-49	-95
	7	-42	-93	-43	-95
eduroam	1	-39	-94	-	-
	2	-39	-95	-40	-94
	3	-37	-92	-47	-92
	4	-34	-94	-36	-94
	5	-41	-95	-47	-95
	6	-52	-95	-48	-94
	7	-44	-92	-33	-94
LANGATON-WPA	1	-36	-94	-	-
	2	-36	-95	-36	-95
	3	-30	-94	-34	-92
	4	-41	-94	-37	-94
	5	-36	-95	-43	-95
	6	-46	-95	-49	-94
	7	-31	-92	-35	-94
TAMK	1	-36	-94	-	-
	2	-41	-95	-38	-95
	3	-40	-93	-40	-91
	4	-37	-94	-36	-94
	5	-37	-94	-37	-95
	6	-46	-95	-52	-95
	7	-32	-93	-37	-95
TAMK-GUEST	1	-36	-94	-	-
	2	-41	-95	-35	-92
	3	-47	-92	-24	-92
	4	-44	-94	-34	-94
	5	-44	-95	-39	-95
	6	-50	-95	-43	-94
	7	-39	-93	-26	-94

Liite 6. Valvonta-asemalla mitatut tukiasemien signaaliarvot (häiriötilanne 2)

		Etäisyys: 1 m		Etäisyys: 6 m	
SSID	**Antenni**	**Signaalitaso (dBm)**	**Kohinataso (dBm)**	**Signaalitaso (dBm)**	**Kohinataso (dBm)**
7signal_AP (D-Link DI-524)	1	-44	-93	-44	-89
	2	-46	-95	-44	-95
	3	-53	-93	-52	-94
	4	-39	-94	-37	-95
	5	-41	-95	-55	-95
	6	-43	-95	-56	-95
	7	-43	-94	-48	-94
eduroam	1	-36	-93	-31	-89
	2	-38	-95	-35	-95
	3	-39	-94	-34	-93
	4	-38	-94	-38	-95
	5	-37	-95	-38	-94
	6	-45	-95	-50	-95
	7	-47	-94	-33	-94
LANGATON-WPA	1	-37	-93	-36	-89
	2	-54	-95	-43	-95
	3	-35	-93	-35	-93
	4	-34	-94	-45	-95
	5	-36	-95	-40	-94
	6	-45	-95	-45	-95
	7	-42	-94	-27	-94
TAMK	1	-38	-93	-30	-89
	2	-51	-95	-41	-95
	3	-41	-93	-36	-93
	4	-32	-94	-39	-95
	5	-37	-94	-42	-94
	6	-44	-95	-39	-95
	7	-40	-94	-35	-93
TAMK-GUEST	1	-40	-93	-42	-89
	2	-56	-95	-50	-95
	3	-50	-93	-47	-93
	4	-48	-95	-41	-95
	5	-42	-95	-34	-94
	6	-54	-95	-50	-95
	7	-39	-94	-48	-94