KARELIA-AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

Teemu Pesonen

LANGATTOMAN LÄHIVERKON KATVEALUEIDEN KARTOITUS

Opinnäytetyö
Toukokuu 2014

Karelia AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Toukokuu 2014
Tietotekniikan koulutusohjelma

Karjalankatu 3
80200 JOENSUU
+358 50 260 6800

Tekijä
Teemu Pesonen

Nimeke
Langattoman lähiverkon katvealueiden kartoitus

Toimeksiantaja
John Deere Forestry Oy

Tiivistelmä

Tämän opinnäytetyön tehtävänä oli kartoittaa ja parantaa toimeksiantajan John Deere Forestry Oy:n tehdasalueen langattoman lähiverkon kuuluvuutta. Kuuluvuutta kartoitettiin tehdasalueen reunalla sijaitsevilla varastoalueilla ja lisäksi suunniteltiin sopivat sijoituspaikat verkkoon liitettäville tukiasemille.

Opinnäytetyö koostuu kahdesta osasta: teoriaosuudesta, jossa käsitellään langattoman verkon tekniikkaa, käsitteitä sekä tietoturvaa, ja raportista, jossa kartoitetaan toimeksiantajan langattoman lähiverkon katvealueet. Aihealueeseen perehdyttiin tutustumalla langattoman lähiverkon tekniikkaan ja kehitykseen. Teoriapohjan avulla toteutettiin toimeksiantajan langattoman lähiverkon katvealueiden kartoitus ja sopivien paikkojen suunnittelu uusille käyttöön otettaville tukiasemille.

Opinnäytetyön tuloksena toimeksiantajan langattoman lähiverkon katvealueet on poistettu. Lisäksi langattoman lähiverkkoyhteyden tila varastoalueilla on parantunut merkittävästi. Opinnäytetyön julkisesta versiosta on poistettu joitakin kuvia tai niissä esiintyvää tietoa luottamuksellisuuden vuoksi.

Kieli
suomi

Sivuja 48

Asiasanat
langaton lähiverkko, tietoturva, salaus

Karelia
UNIVERSITY OF APPLIED SCIENCES

THESIS
May 2014
Degree Programme in
Information Technology
Karjalankatu 3
FI 80200 JOENSUU
FINLAND
+358 50 260 6800

Author
Teemu Pesonen

Title
Mapping of the Dead Zones of Wireless Local Area Network

Commissioned by
John Deere Forestry Oy

Abstract

The purpose of this thesis was to map and improve the coverage of the wireless local area network of John Deere Forestry Oy's factory area. The coverage was mapped in the warehouse areas located in the edges of the factory area. In addition, suitable locations to network the access points were planned.

The thesis consists of two parts: the theoretical part which examines the technology, terms and security of wireless local area networks. The report examines the mapping of the dead zones of the customer's wireless local area network. The subject was approached by inspecting the technology and development of wireless local area networks. Through familiarity of the theoretical background the mapping of the dead zones of customer's wireless local area network was carried out as well as planning for the locations of the new access points.

The dead zones of the customer's wireless local area network have been removed as a result of the thesis. Furthermore, the status of the wireless network connection has improved significantly in the warehouse areas. From the public version of the thesis some figures or some information displayed in the figures have been removed due to confidentiality.

Language
Finnish

Pages 48

Keywords
wireless local area network, information security, encryption

Sisältö

1 Johdanto 6
1.1 Deere & Company 7
1.2 John Deere Forestry Oy 7
2 Langaton verkko 8
2.1 Langattoman lähiverkon signaalit 9
2.2 Signaalin eteneminen 9
2.3 Taajuusalueet 10
2.4 Langattoman lähiverkon tekniikka 12
2.4.1 Vuoronvaraus ja törmäyksen välttäminen (CSMA/CA) 12
2.4.2 Taajuushyppely (FHSS) 13
2.4.3 Suorasekvenssihajaspektri (DSSS) 14
2.4.4 Monikantoaaltomodulointi (OFDM) 14
2.5 OSI-malli 15
2.6 Langattoman verkon topologiat 17
2.6.1 BSS 18
2.6.2 IBSS 18
2.6.3 ESS 19
2.7 Langattoman verkon standardit 20
2.7.1 IEEE 802.11 20
2.7.2 802.11b 20
2.7.3 802.11a 21
2.7.4 802.11g 21
2.7.5 802.11n 22
2.7.6 802.11ac 22
2.7.7 Muut IEEE 802.11-standardilaajennukset 23
2.7.8 HiperLAN 24
2.8 Langattoman lähiverkon laitteet 25
2.8.1 WLAN-kortti 25
2.8.2 WLAN-tukiasema 26
2.8.3 WLAN-kytkin 27
3 Langattoman lähiverkon tietoturva 28
3.1 Tietoturvan tavoitteet ja perusmäärittelyt 28
3.2 Tietoturvauhat 29
3.2.1 Palvelunestohyökkäys 29
3.2.2 Välistävetohyökkäys 30
3.2.3 Passiivinen tarkkailu 31
3.3 Salausmenetelmät ja suojautuminen 31
3.3.1 WEP 31
3.3.2 WPA ja WPA2 32
3.3.3 TKIP 33
3.3.4 AES 33
3.3.5 MAC-suodatus 33
3.4 Todennusmenetelmät 34
3.4.1 802.1x-todennus 34
3.4.2 Todennus RADIUS-palvelimella 35
3.4.3 TACACS+ 36
4 John Deere Forestry Oy:n tehdasalueen langattoman verkon katvealueet 37

4.1 Lähtötilanne 37
4.2 Mittaukset katvealueilla 38
4.3 Uusien tukiasemien sijoituspaikat 41
4.4 Verkkokaappeihin tehdyt kytkennät 43
4.5 Mittaukset tukiasemien asennusten jälkeen 43
5 Pohdinta 45
Lähteet 47

1 Johdanto

Langattomat lähiverkot ovat yleistyneet merkittävästi viimeisen vuosikymmenen aikana. Kaupunkeihin on luotu monia kaikille avoimia liityntäpisteitä, joista on mahdollista ottaa yhteys internetiin. Laajemmassa mittakaavassa langattomien lähiverkkojen tekniikka on vielä rajallinen ja verkkojen toimintaan ongelmia aiheuttavat esimerkiksi muiden laitteiden interferenssi, rajoittunut kantoalue sekä kanavien päällekkäisyys.

Langattomuus on yksi tärkeimpiä asioita uusia laitteita suunnitellessa. Matkapuhelimet, kannettavat tietokoneet sekä muut viihdekäyttöön suunnitellut laitteet käyttävät langatonta verkkoa tiedonsiirtoon ja ohjelmistopäivitysten lataamiseen. Uusimmat televisiot on myös mahdollista yhdistää internetiin langattomasti. Langattomien verkkokorttien tuotekehityksen avulla langattomia verkkoja on mahdollista hyödyntää tulevaisuudessa entistä paremmin.

Tässä opinnäytetyössä on tavoitteena tutkia langattomien lähiverkkojen teoriaa ja tekniikkaa sekä parantaa opinnäytetyön toimeksiantajan John Deere Forestry Oy:n tehdasalueen langattoman verkon kuuluvuutta. Kuuluvuutta parannetaan lisäämällä katvealueille uusia langattoman verkon tukiasemia. Tukiasemien asennuspaikat suunnitellaan huomioiden asennuspaikan sijainti suhteutettuna parhaimman suorituskyvyn aikaansaamiseksi.

Opinnäytetyö on jaettu kahteen osaan: teoriaosaan ja toiminnalliseen osaan. Teoriaosassa käsitellään langattoman verkon tekniikkaa ja käsitteitä. Tarkoituksenani on esittää mahdollisimman ymmärrettävästi, miten langattomat lähiverkot toimivat. Teoriaosuudessa käsitellään sekä tekniikkaa että tietoturvaa. Tietoturva on etenkin yrityksille hyvin merkittävä huomioitava asia langatonta lähiverkkoa suunniteltaessa. Toiminnallisessa osuudessa on kerrottu tehdyt toimet langattoman lähiverkon kuuluvuuden parantamiseksi alkaen lähtötilanteen tarkastelusta lopputuloksiin.

Opinnäytetyöstä on tehty kaksi versiota: julkinen ja salainen versio. Julkisesta versiosta joidenkin kuvien tietoja on poistettu tietojen luottamuksellisuuden vuoksi.

1.1 Deere & Company

Seppä John Deere perusti vuonna 1837 yrityksen Illinoisissa, Yhdysvalloissa, minkä ainoana työntekijänä ryhtyi valmistamaan ja markkinoimaan uudentyyppisiä kyntöauroja. Yrityksen nimeksi vakiintui Deere & Company vuonna 1868. Nykyään Deere & Company on maailman johtava maatalous- ja metsäkoneiden valmistaja ja yksi johtavia maarakennus- ja nurmikonhoitokoneiden sekä peltojenkastelujärjestelmien toimittajia. Näiden ohessa yritys valmistaa koneisiinsa moottoreita ja voimansiirtolaitteita ja tarjoaa koneiden ostajille rahoituspalvelua. Deere & Company työllistää maailmanlaajuisesti yli 60 000 henkilöä. [1.]

1.2 John Deere Forestry Oy

John Deere Forestry Oy on maailman johtava metsäkonevalmistaja, joka tunnettiin aiemmin nimellä Timberjack Oy. Deere & Company osti Timberjack Oy:n Metso-konsernilta vuonna 2000. Yhtiön kotipaikka on Tampere, jossa sijaitsevat metsäkoneiden tuotekehitys sekä Euroopan markkinointikeskus. John Deere -metsäkoneet valmistetaan Joensuussa. John Deere Forestry Oy työllistää Suomessa noin 700 henkilöä. [1; 2.]

John Deeren Joensuun tehdas perustettiin vuonna 1972 ja siellä rakennettiin aluksi metsäkoneiden ohella kaivinkoneita, tiehöyliä ja täryjyriä. Vuodesta 1995 lähtien tehdas keskittyi ainoastaan metsäkoneiden, kuten harvesterien, kuormatraktorien ja kuormaimien valmistamiseen. Yhteistyökumppani Waratah-OM Oy valmistaa harvestereihin tulevat harvesteripäät. Joensuun tehtaan pinta-ala on noin 20 000 neliömetriä, josta tuotantokäytössä on noin 18 000 neliömetriä. Joensuun tehdas työllistää noin 400 henkilöä. [1; 2.]

2 Langaton verkko

Langattoman lähiverkon historia alkaa 1980-luvun puolivälistä, jolloin Motorola esitteli Altairin. Tämä oli ensimmäinen WLAN-tekniikkaa (Wireless Local Area Network) käyttävä tuote. Se, kuten monet muut 80- ja 90-luvun tuotteet olivat valmistajakohtaisia, eli käyttäjät joutuivat sitoutumaan yhteen valitsemaansa toimittajaan. IEEE-järjestön standardointiryhmä ryhtyi kehittämään langattoman lähiverkon standardikehystä vuonna 1990 ja työn tulos, 802.11-standardi, julkaistiin vuonna 1997. Standardin 1 ja 2 Mb/s-nopeudet olivat kuitenkin selvästi heikommat verrattuna Fast Ethernet -lähiverkkoon. Langaton lähiverkkotekniikka jatkoi kehittymistään ja pari vuotta myöhemmin julkaistiin uusi 802.11b-standardilaajennus, jonka nopeus kasvoi 11 Mb/s:iin. Tämän jälkeen on julkaistu neljä uutta standardilaajennusta: 802.11a, 802.11g, 802.11n ja 802.11ac. [3, s. 15.]

Nykyaikana langattomilla verkoilla on suuri merkitys ihmisten elämässä niin työkuin vapaa-aikanakin. Langattoman verkon avulla ihmiset voivat viestiä keskenään sekä olla yhteydessä tietoon tai sovelluksiin ilman fyysistä tietoverkkoa. Tämä mahdollistaa verkon palvelujen käyttämisen paikasta riippumatta. Kotona henkilö voi selata internetiä haluamassaan paikassa ja työpaikalla työntekijä pääsee samoihin tietoihin ja palveluihin käsiksi istuipa hän työpisteellään tai neuvotteluhuoneessa. Jo muutaman vuoden ajan langatonta verkkoa on myös ollut mahdollista käyttää lentokoneessa norjalaisen halpalentoyhtiön lennoilla [4]. Langattoman verkkotekniikan kehittyessä yhä useampi kotitalous käyttää pelkästään langatonta verkkoa viestintään. Yrityksien lähiverkkoa langaton verkko ei ole kokonaan korvannut, vaan se toimii langallisen lähiverkon vaihtoehtoisena yhteytenä. WLAN:a kutsutaan usein nimellä Wi-Fi (Wireless Fidelity), joka on Wi-Fi Alliancen tuotemerkki, johon on sisällytetty 802.11-standardin valikoituja toimintoja. [5, s. 8–9.]

Opinnäytetyössä tiedonsiirtonopeuksia käsiteltäessä on käytetty mittayksikköä Mb/s eli megabittiä sekunnissa. Kun tämä bittiluku jaetaan kahdeksalla, saadaan tiedonsiirtonopeus megatavuina. Esimerkiksi IEEE 802.11g:n maksimitiedonsiirtonopeus 54 Mb/s on 6,75 Mt/s eli megatavua sekunnissa. [6.]

2.1 Langattoman lähiverkon signaalit

Langattomissa lähiverkoissa kulkeva tieto, kuten sähköpostit, tiedostot, videot tai musiikki, kulkevat radioaaltojen avulla. Radioaallot ovat signaaleja, joiden amplitudi vaihtelee ajan suhteen jatkuvasti. Amplitudi on signaalin värähdysliikkeen taajuus. Radioaaltojen mittayksikkö on hertsi (Hz), jolla mitataan radioaaltojen tiheyttä sekunnissa. [5, s. 54–57.]

Tietokoneet käyttävät datan kuljettamiseen digitaalisia signaaleja. Nämä signaalit sisältävät binäärilukuja, jotka tulee vahvistaa ennen datan lähettämistä ilmateitse. Tietokoneen langaton verkkokortti muuntaa digitaalisen signaalin digitaaliseksi moduloiduksi signaaliksi. Modulaation jälkeen signaali vahvistetaan, jonka jälkeen se kulkee ilmatietä pitkin vastaanottavaan langattomaan verkkokorttiin, joka demoduloi sekä prosessoi vastaanotetun signaalin ja siirtää datan eteenpäin. [5, s. 54–55, 69.]

Antennien avulla lähetetään signaaleja ilmateitse. Antennit muuttavat sähköenergian sähkömagneettiseksi säteilyksi. Kaikkien antennien suuntakuvio on epäsymmetrinen eli signaalin lähetyskuvio on esimerkiksi suurempi vaakatasossa verrattuna pystytasoon nähden. Tavallisimpia antennityyppejä ovat esimerkiksi ympärisäteilevä antenni, suunta-antenni, laitteiden sisäinen antenni ja lautasantenni. Sisätilojen langattomissa lähiverkoissa käytetään tavallisesti ympärisäteileviä antenneja sekä laitteiden sisäisiä antenneja. Ulkotiloissa käytetään lautasantenneja tai sektoriantenneja. [3, s. 60, 63.]

2.2 Signaalin eteneminen

Sähkömagneettinen signaali etenee suoraviivaisesti ja vaimentumatta ainoastaan tyhjiössä. Käytännön ympäristössä signaalin etenemiseen vaikuttavat väliaine ja esteet. Signaalin edetessä ilmatiessä, sen amplitudi pienenee eksponentiaalisesti lähettäjän ja vastaanottajan etäisyyden kasvaessa. Avoimessa, esteettömässä tilassa signaaliin kohdistuu vapaan tilan matkavaimennus, jossa ilmakehän vaikutuksesta moduloitu signaali vaimenee eksponentiaalisesti sen edetessä antennista kauemmaksi. Signaalilla tuleekin olla riittävästi voimaa,

jotta se saavuttaisi tavoitellun etäisyyden vastaanottajan edellyttämällä tasolla. [3, s. 56; 5, s. 71].

Signaalin etenemiseen ja tehoon vaikuttavat useat eri tekijät kuten sade, lumi, kasvillisuus tai rakennukset. Signaalin etenemiseen vaikuttavat myös esineet, joista signaali voi heijastua. Heijastumisessa signaalin osat kulkevat eri reittejä kohdeasemaan. Osa signaalista kulkee suoraan kohteeseen ja toinen osa kimpoaa esineiden kautta kohteeseensa kulkien pidemmän matkan ja saapuen hieman myöhemmin perille. Heijastumisesta johtuvat viiveet aiheuttavat tiedon muuttumista, koska signaalin muoto välittää lähetettävän tiedon ja heijasteita sisältävää signaalia moduloidessaan vastaanottajan paketti saattaa sisältää bittivirheitä. [5, s. 74–75.]

Interferenssi häiritsee signaalin etenemistä silloin, kun vastaanottavassa asemassa on samanaikaisesti useita päällekkäisiä, samalla taajuudella olevia signaaleja. Yleisintä interferenssi on 2,4 GHz:n taajuusalueella kapeista ja päällekkäisistä kanavista johtuen. Lisäksi monet muut kuin langattomien lähiverkkojen laitteet, kuten mikroaaltouunit tai Bluetoothia käyttävät langattomat puhelimet, käyttävät samaa taajuusaluetta. Interferenssiä voidaan välttää esimerkiksi vaihtamalla langattomien lähiverkkojen laitteet 5 GHz:n taajuusalueelle. [5, s. 73–74, 129.]

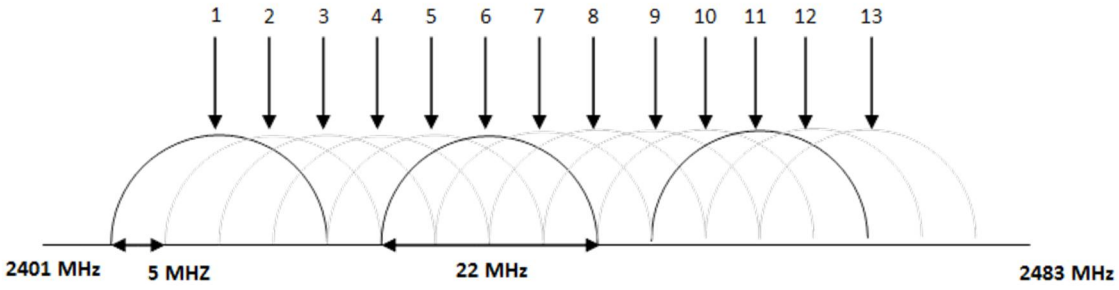
Muita signaalin etenemiseen vaikuttavia tekijöitä ovat taipuminen ja sironta. Taipumisessa signaali vuorovaikuttaa pienten alkeishiukkasten kanssa, jolloin signaali taipuu ja leviää osuessaan esteeseen. Sironnassa signaali hajaantuu osuessaan pieniin ilmakehän partikkeleihin hajaantuen erisuuntaisiksi aaltokimpuiksi. Taipuminen ja sironta ovat pienemmän mittakaavan ilmiöitä, jotka esiintyvät lähinnä ilmakehän ylemmissä kerroksissa. [3, s. 57–58.]

2.3 Taajuusalueet

ISM-taajuusalue on maailmanlaajuinen vapaassa käytössä oleva radiotaajuuskaista. Tietoliikenne käyttää ISM-taajuusalueita langattomaan tiedonsiirtoon. Langattomille lähiverkoille on annettu käyttöön ennalta määritellyt 2,4 GHz:n

sekä 5 GHz:n taajuusalueet sekä niille sovitut kaistanleveydet. Kaistat on puolestaan jaettu ennalta määrättyihin viestintään käytettäviin kanaviin. Samaa 2,4 GHz:n taajuusaluetta käyttävät Bluetooth-puhelimet tai mikroaaltouunit aiheuttavat hetkittäin interferenssiä heikentäen langattoman verkon suorituskykyä. [7.]

Yleisin langattomien lähiverkkojen käyttämä taajuusalue on 2,4 GHz. Taajuusalueet ja kaistanleveydet ovat erilaisia riippuen valtioiden maantieteellisestä sijainnista. Euroopassa 2,4 GHz:n taajuusalue on 2,401–2,483 GHz välillä ja se on jaettu 13 kanavaan, joista kukin on 22 MHz leveä (kuvio 1). Kanavat ovat toisistaan 5 MHz:n välein, eli vierekkäiset kanavat ovat osin päällekkäin toistensa kanssa. Toisistaan ei-päällekkäisiä kanavia ovat 1, 7 ja 13 (tai vaihtoehtoisesti 1, 6 ja 13 sekä 1, 8 ja 13). Yhdysvalloissa sallittuja kanavia ovat vain kanavat 1-11 ja ei-päällekkäisiä kanavia ovat ainoastaan 1, 6 ja 11. [3, s. 39.]



Kuvio 1. 2,4 GHz:n taajuusalueen kanavat.

Vaihtoehtoisella 5 GHz:n taajuusalueella on 12 ei-päällekkäistä kanavaa. Jokaisen kanavan kaistanleveys on 20 MHz. Tämä tarkoittaa huomattavasti parempaa suorituskykyä ja luotettavampaa yhteyttä 2,4 GHz:n taajuusalueeseen verrattuna. 5 GHz:n taajuusalueella on mahdollista toteuttaa lähestulkoon häiriötön langaton lähiverkko, sillä muut laitteet kuten mikroaaltouunit tai Bluetooth-laitteet eivät aiheuta interferenssiä. Korkeampi taajuusalue pienentää kuitenkin signaalin kantamaa, jolloin verkkoon sijoitettavien tukiasemien määrä kasvaa aiheuttaen suurempia kustannuksia. [5, s. 128–129.]

Nykyään monissa tukiasemissa on mahdollisuutena käyttää auto-channel-toimintoa. Tällöin tukiasema tarkkailee viereisten tukiasemien kanavia ja niiden signaalien vahvuuksia ja päättelee, mille kanavalle muiden tukiasemien aiheut-

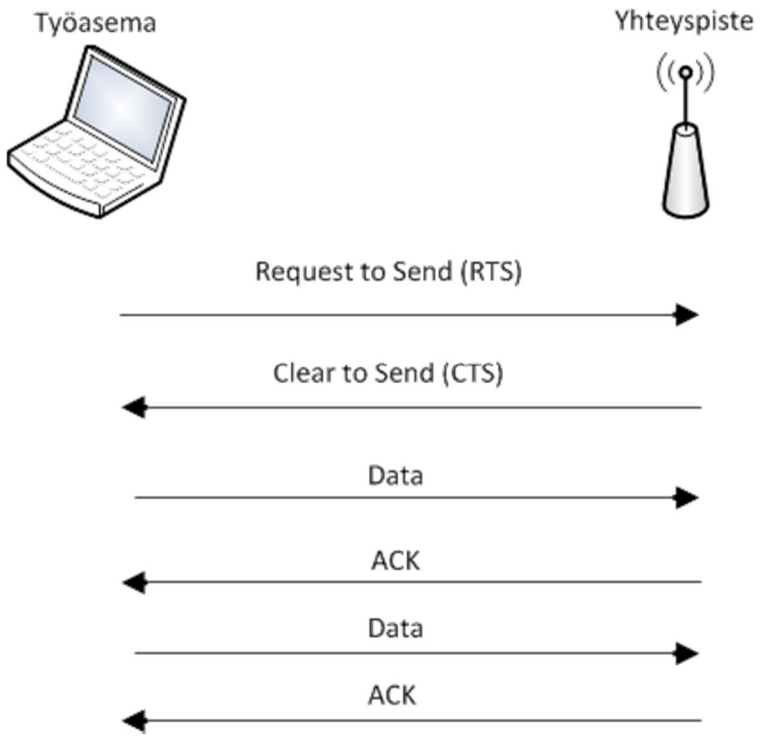
tama interferenssi vaikuttaa kaikista vähiten. Tukiasema valitsee vähiten muita kanavia häiritsevän kanavan oman käyttöönsä. [8.]

2.4 Langattoman lähiverkon tekniikka

2.4.1 Vuoronvaraus ja törmäyksen välttäminen (CSMA/CA)

Vuoronvaraus ja törmäyksen välttäminen (Carrier Sence Multiple Access with Collision Avoidance) on langattomissa lähiverkoissa käytettävä tiedonsiirron tekniikka. Sen tarkoituksena on estää datakehysten päällekkäiset lähetykset ja niistä aiheutuvat kehysten törmäykset. CSMA/CA muistuttaa paljon Ethernet-verkkojen CSMA/CD-tekniikkaa (Carrier Sence Multiple Access with Collision Detection), jonka tarkoituksena on havaita datakehysten törmäykset. [3, s. 29.]

CSMA/CA-tekniikka sisältää virtuaalisen kantoaallon kuuntelun (VCS, Virtual Carrier Sence), jonka avulla langattoman verkon yhteyspiste (tukiasema) voi kontrolloida alueensa verkkoliikennettä. VCS-tekniikassa (kuvio 2) langattoman verkon päätelaite, esimerkiksi työasema, pyytää aluksi datakehyksille lähetysluvan RTS-sanomalla (Request to Send). Kun verkko on vapaa liikenteelle, yhteyspiste vastaa CTS-sanomalla (Clear to Send) antaen päätelaitteelle luvan kehysten lähettämiselle. Saatuaan luvan päätelaite voi lähettää datansa joko yhdessä tai useammassa datakehyksessä. Jokainen lähetetty datakehys kuitataan erikseen ACK-sanomalla (Acknowledgement). [3, s. 29.]



Kuvio 2. Virtuaalinen kantoaallon kuuntelu ja datakehysten kuittaus.

VCS-tekniikan lisäksi CSMA/CA sisältää myös fyysisen kantoaallon kuuntelun eli PCS-tekniikan (Physical Carrier Sence). PCS-tekniikassa päätelaitteen pitää ennen datakehysten lähetystä varmistaa, onko verkko vapaa liikenteelle. Jos päätelaite havaitsee verkon olevan varattu, päätelaite odottaa hetken ennen kuin yrittää lähettää datakehyksensä uudelleen. [3, s. 29.]

2.4.2 Taajuushyppely (FHSS)

Taajuushyppely (Frequency Hopping Spread Spectrum) on sotilaselektroniikasta juurensa juontava tekniikka. Taajuushyppelyssä päätelaitteet hyppivät kanavilta toisille lähettäessään datapaketteja. Parhaimman hyödyn aikaan saamiseksi taajuushyppelyn tulisi tapahtua vähintään seitsemän kanavan päähän edellisestä kanavasta. Taajuushyppelyllä saavutetaan huomattava etu tietoturvaan, sillä taajuushyppely tekee salakuuntelusta erittäin vaikeaa. Salakuuntelijan tulisi tietää tarkasti hyppelyjärjestys liikenteen seuraamisen mahdollistamiseksi. Lisäksi taajuuksien välillä hyppely on niin nopeaa, ettei liikenteen seuraaminen normaalilla skannerilla onnistuisi, vaikka hyppelyjärjestys olisikin salakuuntelijan tiedossa. [9, s. 116–117.]

Taajuushyppelyn toimintaperiaatteeseen kuuluu kolme vaihetta. Siirtoaika jaetaan kiinteän mittaisiin aikaväleihin, käytettävissä oleva siirtokaista jaetaan alikanaviin ja sovitaan hyppelyjärjestyksestä lähettäjän ja vastaanottajan välillä. Tiedonsiirron aikana data paloitellaan purskeiksi ja jokainen purske siirretään hyppelyjärjestyksen mukaisesti omalla taajuudellaan. [9, s. 116–117.]

Taajuushyppely jaetaan hyppelynopeuden perusteella kahteen luokkaan, hitaaseen ja nopeaan taajuushyppelyyn. Hitaassa taajuushyppelyssä yksi tai useampia databittejä lähetetään yhdellä aikavälillä ja nopeassa taajuushyppelyssä yksi databitti jaetaan useammalle aikavälille. Hidas taajuushyppely on suosittu tekniikka langattomissa lähiverkoissa. [10.]

2.4.3 Suorasekvenssihajaspektri (DSSS)

Suorasekvenssihajaspektrissä (Direct Sequence Spread Spectrum) kapeakaistainen signaali levitetään laajemmalle taajuuskaistalle kertomalla lähetettävä signaali hajautusavaimella. Hajautusavain voi olla kiinteä tai ratkaisukohtainen, kuten IEEE:n 802.11b-standardissa. Hajautusavain koostuu lastuista, mikä esimerkiksi 802.11b-standardissa on 11-lastuinen. Hajautusavaimen taajuuden ollessa lähetettävän datan taajuutta suurempi, kertolaskun tulona on hajautusavaimen taajuuden omaama lähete. Lähetettä vastaanotettaessa vastaanotettu signaali kerrotaan hajautusavaimella, jolloin alkuperäinen signaali on palautettu entiselleen. [9, s. 117–118.]

Suorasekvenssihajaspektrin etuna on suuri häiriönsietokyky. Häiriönsietokyky kuitenkin riippuu lastunopeuden ja datanopeuden suhteesta toisiinsa. Verkon häiriönsietokyky on sitä parempi, mitä suurempi on nopeuksien keskinäinen suhde (lastua/s suhteessa bit/s). [9, s. 117–118.]

2.4.4 Monikantoaaltomodulointi (OFDM)

Monikantoaaltomoduloinnissa (Orthogonal Frequency Division Modulation) datan siirtoon tarkoitettu taajuusalue jaetaan itsenäisiin, toisistaan häiriöttömiin alikanaviin. Yhteyden osapuolet, lähettäjä ja vastaanottaja, tutkivat siirtotien

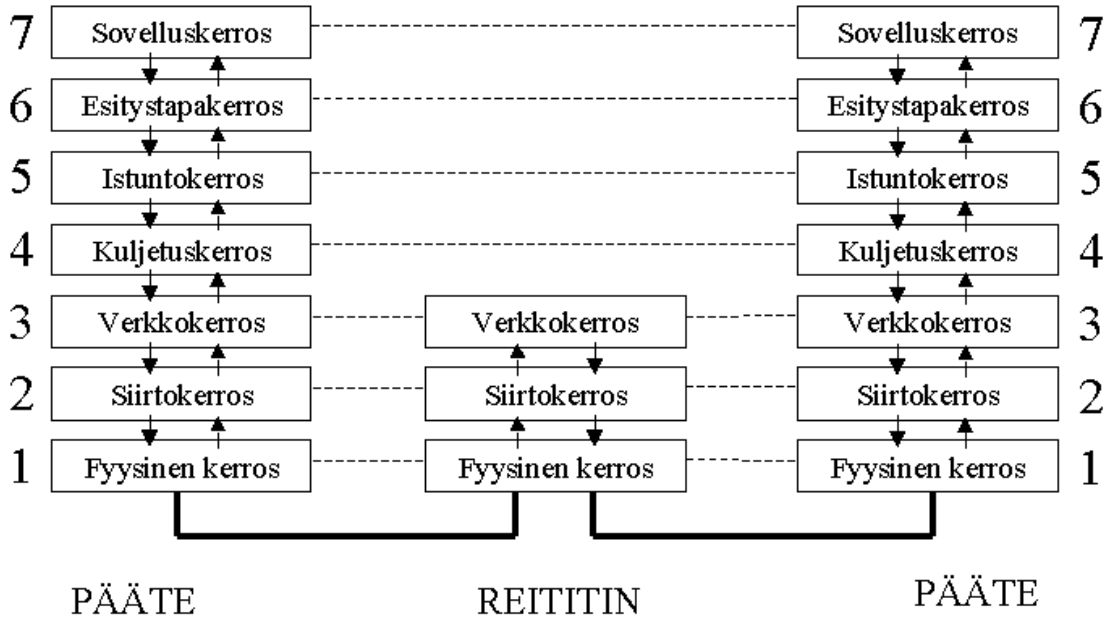
ominaisuuksia ja käyttömahdollisuuksia. Jos jokin taajuusalue havaitaan käyttökelvottomaksi, osapuolet hakevat signaali-kohinasuhteen perusteella jäljelle jääneiden alikanavien kantoaalloille sopivan modulointimenetelmän. OFDM:n avulla on mahdollista kasvattaa yksittäisen bitin kestoa, joka parantaa järjestelmän häiriönsietokykyä. [9, s. 112–113.]

2.5 OSI-malli

OSI-mallin (Open Systems Interconnect) kehitti ISO-järjestö (International Standards Organization) 1980-luvulla. OSI-malli määrittelee kattavasti verkon toiminnot. Mallissa on määritelty kehykset tietoliikenteen standardoinnille ja protokollien suunnittelulle. Se toimii perustana tietoliikennestandardoinnille ja tarjoaa tietoliikennejärjestelmien rakentamista varten peruskäsitteistön. OSI-malli on mahdollistanut eri valmistajien tietoliikennelaitteiden yhteistoiminnan eri tiedonsiirtoverkoissa ja -palveluissa. [11.]

Ennen OSI-mallia erilaisia verkkomalleja kehittivät pääasiassa tietotekniikkayritykset. Näissä verkkomalleissa ongelmana oli, etteivät ne olleet yhteensopivia muiden mallien kanssa. Yhteensopimattomuus olikin niin suuri ongelma, että tietotekniikkayritykset luopuivat valmistajakohtaisista malleistaan. [12.]

OSI-mallissa tietoliikenneverkon tehtävät jaetaan seitsemään toisistaan riippumattomaan kerrokseen, jotka kuitenkin tukeutuvat allaan olevan kerroksen tarjoamiin palveluihin. OSI-mallin (kuvio 3) toiminta alkaa ylimmästä kerroksesta jatkuen alempiin kerroksiin. Mallin avulla on myös helppoa tarkastella langattoman verkon toimintaa. [5, s. 52.]



Kuvio 3. OSI-malli. [12.]

Ensimmäinen OSI-mallin kerros on fyysinen kerros (Physical layer). Fyysiseen kerrokseen sisältyvät kaikki loogiset, sähköiset ja mekaaniset asiat. Kerros määrittelee fyysiset keinot tiedon siirtämiseksi paikasta toiseen. Kerroksen määrittelyihin kuuluvat esimerkiksi liittimet, signaalin jännitetasot ja kaapelityypit. Esimerkkejä standardeista ovat Bluetooth, Ethernet ja Wi-Fi. Fyysinen kerros on OSI-mallin kerroksista ainoa, joka sisältää konkreettisia nähtävissä olevia asioita, sillä muilla kerroksilla tiedon siirrosta huolehtivat ohjelmistot. [11.]

OSI-mallin toinen kerros on siirtoyhteyskerros (Data link layer). Sen tehtävänä on hoitaa yhteyden luominen ja purkaminen siirtotiehen tiedon kulkemista varten. Lisäksi tehtävänä on varmistaa, ettei tietoa lähetetä liian nopeasti, jolloin tiedon vastaanottaja ei pysty sitä käsittelemään. Siirtoyhteyskerros huolehtii myös siitä, että sen läpi kulkeva tieto ei sisällä virheitä. Virheettömyyden varmistaminen tapahtuu virheitä havaitsevia koodeja käyttämällä ja lähettämällä virheellinen data uudelleen. Siirtoyhteyskerrokseen kuuluvat esimerkiksi kytkimet, tukiasemat ja verkkokortit sekä 802.11-standardit. [13.]

Kolmas kerros on verkkokerros (Network layer), joka huolehtii pakettien reitityksen verkon sisällä lähteestä kohteeseen. Reitityksellä varmistetaan datapakettien lähteminen määrätyn kohteen kannalta oikeaan suuntaan ja valita, mitä reit-

tiä pitkin datapaketit kulkevat monihaaraisessa verkossa. Tähän kerrokseen kuuluu esimerkiksi IP-protokolla. [5, s. 53.]

Neljäs kerros on kuljetuskerros (Transport layer). Sen tehtävänä on tarjota datavirralle luotettava kuljetuspalvelu lähteen ja kohteen välillä. Kuljetuskerros huolehtii siitä, että verkossa yhteyden katketessa esimerkiksi johdon rikkoutumisen takia tietoliikenne verkossa ei katkeaisi, vaan ryhdytään käyttämään vaihtoehtoista reittiä tiedon perille viemiseksi. Kerrokseen kuuluu esimerkiksi TCP-protokolla (Transmission Control Protocol). [13.]

Viides kerros on istuntokerros (Session layer), joka muodostaa, hallinnoi ja purkaa sovellusten väliset istunnot. Lisäksi istuntokerros jaksottaa liikenteen yhteyden aikana loogisiin osiin. Langattomissa verkoissa väliohjelmistot ja pääsynvalvojat tarjoavat kyseiset toiminnot. Häiriön ilmetessä langattomassa verkossa istuntokerroksen toiminnot keskeyttävät yhteyden siihen saakka, kunnes häiriö poistuu. [5, s. 53.]

Kuudes kerros on esitystapakerros (Presentation layer). Kerros määrittelee yhtenäisen esitystavan datalle ja tarpeen mukaan suorittaa käännökset erilaisten datamuotojen välillä. Esitystapakerroksen tarkoituksena on saattaa tieto sellaiseen asuun, jonka tiedon vastaanottaja ymmärtää. [5, s. 52.]

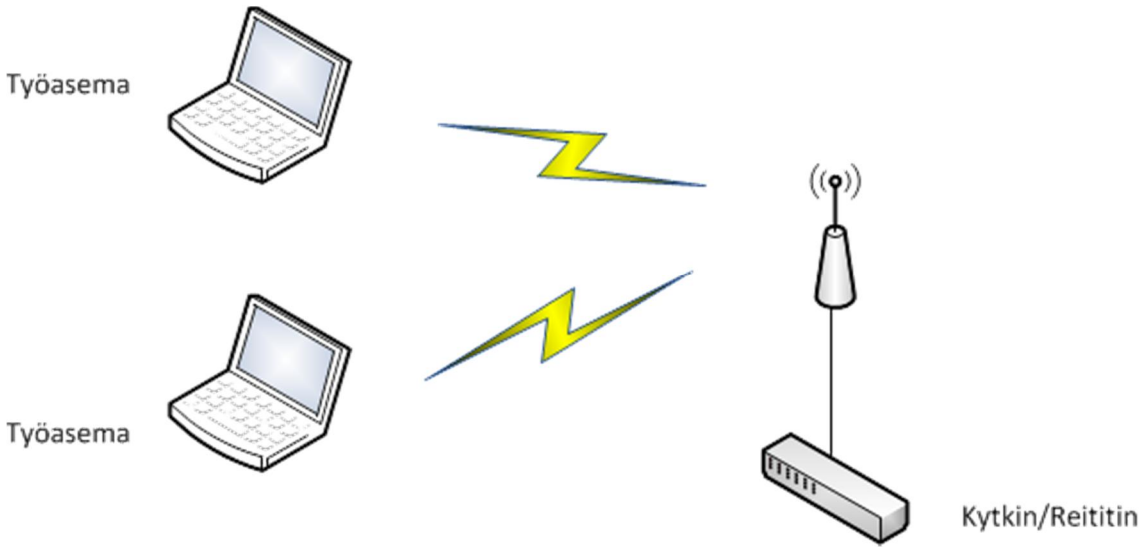
Seitsemäs ja ylin OSI-mallin kerros on sovelluskerros (Application layer). Sovelluskerros muodostaa käyttäjien väliset yhteydet ja tarjoaa perusviestintäpalvelut kuten sähköpostin tai tiedonsiirron palvelimelle. Kerrokseen kuuluvat esimerkiksi protokollat SMTP, http, ja FTP. [5, s. 52.]

2.6 Langattoman verkon topologiat

IEEE 802.11-standardin mukainen langaton lähiverkko mahdollistaa kolme erilaista tapaa kytkeä laitteita toisiinsa. Nämä kolme topologiaa ovat BSS, IBSS ja ESS. Topologiat määräytyvät sen mukaan, miten langatonta verkkoa halutaan käyttää.

2.6.1 BSS

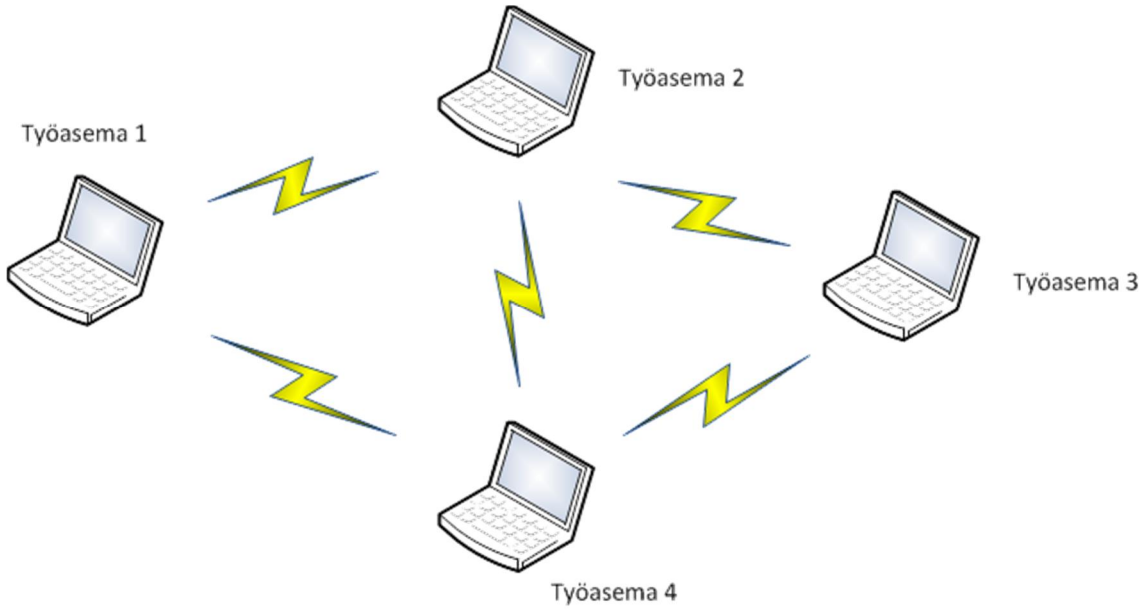
BSS eli Basic Service Set on verkko, joka muodostuu tukiasemista, joihin on langattomasti liitetty työasemia. Vastaavasti tukiasemat ovat yhteydessä pääverkkoon. BSS on yleisin langattoman verkon topologia sekä koti- että yritysympäristössä. BSS-topologiassa (kuvio 4) verkon liikenne kulkee aina tukiaseman kautta ja topologia on samankaltainen kytkimiin perustuvien kiinteiden lähiverkkojen kanssa. Jos tukiasema rikkoutuu tai sammuu, yhteys katkeaa ja BSS-topologian mukainen verkko ei ole enää käytössä. [9, s. 295.]



Kuvio 4. BSS-verkkotopologia.

2.6.2 IBSS

IBSS (Independent Basic Service Set) on verkko, jossa langatonta verkkoa käyttävät laitteet eivät kytkeydy mihinkään tukiasemaan, vaan laitteet keskustelevat keskenään langattoman verkon yli (kuvio 5). Esimerkkitilanne IBSS:tä on kokoustilanne, joissa osallistujien laitteet luovat kokoustilaan tilapäiseksi ajaksi oman verkkonsa ja keskustelevat kaikkien verkon laitteiden kanssa. Kun tarve verkosta päättyy esimerkiksi kokouksen päätyttyä, verkko puretaan. IBSS-verkkoa kutsutaan myös Ad-Hoc-verkoksi. Jos joidenkin laitteiden välille jää suurempi etäisyys, ne eivät välttämättä kuule toisiaan ja yhteys kyseisten laitteiden välillä ei ole mahdollinen. Kuviossa 5 työasemien 1 ja 4 etäisyys on liian suuri, joten ne eivät pysty keskinäiseen kommunikointiin. [9, s. 294–295.]

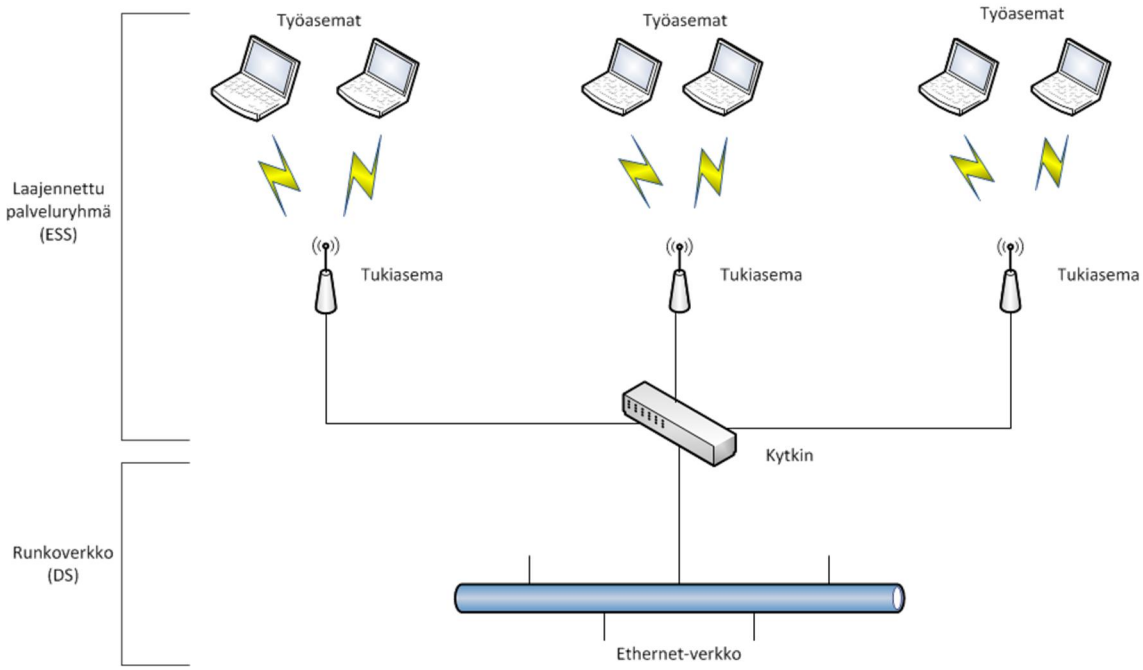


Kuvio 5. IBSS-verkkotopologia.

2.6.3 ESS

BSS-verkkoa on mahdollista laajentaa käyttämällä useampia samaan runkoverkkoon kytkettäviä tukiasemia. Tämä ratkaisu on nimeltään ESS (Extended Service Set). ESS on yleisin tapa muodostaa suurempia kuin yhden tukiaseman langattomia lähiverkkoja. Tällöin lähiverkko kattaa suuremman alueen kuin muutaman huoneen tai yhden kerroksen. [9, s. 296.]

ESS:n taustalla oleva runkoverkko DS (Distribution Set) mahdollistaa tietoliikenteen tukiasemien välillä ja edelleen liittymisen kiinteän verkon puoliseen lähiverkkoon (kuvio 6). Runkoverkko mahdollistaa autentikoinnin verkon työasemille. Tässä tapauksessa verkkoon oikeutettu työasema voi joko liittyä verkkoon tai vastaavasti poistua autentikointitilasta. Siirtotien suojauspalvelun avulla voidaan seurata autentikoituneiden työasemien liikennettä. Tiedonsiirtopalvelu välittää sanomia verkon osapuolten välillä ja reitityspalvelu reitittää sanomia runkoverkon kautta, mikäli vastaanottaja sijaitsee eri tukiaseman alueella kuin lähettäjä. [9, s. 296–297.]



Kuvio 6. ESS-verkkotopologia.

2.7 Langattoman verkon standardit

2.7.1 IEEE 802.11

IEEE (Institute of Electrical and Elecrtonics Engineers) julkaisi alkuperäisen 802.11-standardin vuonna 1997 ja siitä tuli yleisin käytetty langattoman verkon standardiperhe. 802.11-standardi määrittää pääasiassa OSI-mallin fyysisen kerroksen sekä alemman osan siirtokerroksesta. 802.11 toimii 2,4 GHz:n taajuusalueella. Standardin teoreettinen maksiminopeus on 2 Mb/s ja samalle alueelle on mahdollista asettaa toimimaan 15 tukiasemaa. 802.11-standardiperhettä on laajennettu monilla laajennuksilla, jotka ovat parantaneet langattoman verkon käyttönopeuksia ja sovellusten vaatimuksia. [5, s. 118, 124.]

2.7.2 802.11b

Heinäkuussa 1999 IEEE julkaisi 802.11b-standardilaajennuksen, sillä jatkuvasti kehittyvien verkkosovellusten ja kasvaneen langattomien verkkojen käytön myötä 802.11-standardin määrittämät nopeudet kävivät liian hitaiksi. Uusi 802.11b-standardi määritteli verkkoyhteyden nopeudeksi 11 Mb/s ja se toimi samalla 2,4

GHz:n taajuusalueella. 802.11b-standardin etuna on suuri, jopa sisätiloissa 100 metriin yltävä kantama, joka mahdollistaa langattomien lähiverkkojen suhteellisen pienellä tukiasemien määrällä. [5, s. 126–127.]

802.11b:n ongelmana on, että se mahdollistaa ainoastaan kolmen ei-päällekkäisen kanavan käytön 2,4 GHz:n taajuusalueella. Lisäksi 2,4 GHz:n taajuusaluetta käyttävät monet muut yleisesti käytetyt laitteet kuten langattomat puhelimet ja mikroaaltouunit. Nämä laitteet voivat heikentää verkon suorituskykyä merkittävästi. [5, s. 126–127.]

2.7.3 802.11a

Samaan aikaan 802.11b:n kanssa julkaistiin myös 802.11a-standardilaajennus. Merkittävänä erona edellisiin versioihin verrattuna 802.11a käyttää 5 GHz:n taajuusaluetta OFDM-tekniikkaa (Orthogonal Frequency Division Multiplexing) hyväksikäyttäen. 802.11a:n enimmäisnopeus kasvoi merkittävästi 54 Mb/s:iin asti. 802.11a-tekniikkaa käyttävät tukiasemat ja verkkokortit olivat kuitenkin saatavilla vasta vuoden 2001 lopulta, jolloin sen suosio jäi pienemmäksi verrattuna 802.11b:hen verrattuna. [5, s. 124–125.]

802.11a toimii neljällä häiriöttömällä kanavalla, joten sen kapasiteetti on suurempi 802.11b:hen nähden. Lisäksi 5 GHz:n taajuusalueella ei ole muita signaalia häiritseviä laitteita, jolloin häiriöiden todennäköisyys on pienempi. Kuitenkin ongelmana on 802.11a:n heikko kantama, joka on vain noin 30 metriä yhteyden nopeuden heiketessä nopeasti kuuluvuusalueen reunaa lähestyttäessä. 802.11a ei myöskään ole yhteensopiva 802.11b/g-standardien kanssa. Valmistajat ovat myöhemmin ratkaisseet toimittamalla markkinoille sekä 802.11a:ta että 802.11b:ta tukevia verkkokortteja. [5, s. 124–125.]

2.7.4 802.11g

802.11g julkaistiin vuonna 2003 ja se käyttää 2,4 GHz:n taajuusaluetta 802.11b:n tapaan ollen näin yhteensopiva kyseisen standardin kanssa. Kuitenkin, jos jokin verkossa oleva laite ei tue 802.11g:tä, vaan ainoastaan 802.11b:tä,

verkon nopeus putoaa 802.11b:n tasolle. 802.11b:tä käyttävien yritysten on helppo päivittää laitteensa yhteensopivaksi 802.11g:hen. Verkon maksiminopeus kasvoi samaan kuin 802.11a:ssa eli 54 Mb/s:iin. 802.11g:n ongelmat ovat pääosin samoja kuin 802.11b:n kanssa, eli 2,4 GHz:n taajuusaluetta käyttävät muut laitteet voivat aiheuttaa häiriöitä verkon signaaleihin. Käytössä on 802.11b:n tapaan kolme kanavaa, jotka eivät ole toistensa kanssa päällekkäisiä. [5, s. 127; 9, s. 305].

2.7.5 802.11n

802.11n-standardilaajennus julkaistiin vuonna 2009 tarkoituksena parantaa langattomien lähiverkkojen suorituskykyä aiempiin laajennuksiin verrattuna. 802.11n:n teoreettiseksi maksiminopeudeksi luvataan noin 600 Mb/s, todellisen nopeuden jäädessä noin 100–200 Mb/s välille. Merkittävä lisäys edellisiin laajennuksiin on MIMO-tekniikka (Multiple Input Multiple Output), joka mahdollistaa useampien antennien käytön samanaikaisesti. Tämä lisää huomattavasti verkon luotettavuutta sekä nopeutta. [14.]

Merkittävä uusi ominaisuus on myös mahdollisuus kaksinkertaistaa normaalin 20 MHz:n kaistanleveys 40 MHz:iin. Kaistanleveyden kaksinkertaistamisella mahdollistetaan tiedonsiirtonopeuden kasvaminen kaksinkertaiseksi. 802.11n-standardi voi käyttää sekä 2,4 GHz:n että 5 GHz:n taajuusalueita ja on näin ollen yhteensopiva aiempien standardien kanssa. Tällöin vanhemmista standardeista on helpompi siirtyä uuteen standardiin. [14.]

2.7.6 802.11ac

Uutta 802.11ac-standardilaajennusta ryhdyttiin kehittämään vuonna 2011 ja se hyväksyttiin lopullisesti vuoden 2014 tammikuussa. Laajennuksen tarkoituksena on parantaa langattoman lähiverkon tiedonsiirtonopeutta ja kaistanleveyttä, sillä langattomissa verkoissa käytettävien laitteiden määrä kasvaa jatkuvasti. 802.11ac:n teoreettiseksi tiedonsiirtonopeudeksi ilmoitetaan noin 7 Gb/s. 802.11n:n MIMO-tekniikkaa on parannettu MU-MIMO:ksi (Multi-User MIMO), joka mahdollistaa datan yhtäaikaisen lähettämisen usean antennin kautta useal-

le käyttäjälle. 802.11ac:ssä tiedonsiirtonopeutta on kasvatettu suurentamalla kaistanleveyttä. 802.11n:n 20 ja 40 MHz:n lisäksi 802.11ac tukee myös 80 MHz:n kaistanleveyttä sekä vaihtoehtoisen tuen 160 MHz:n kaistanleveydelle. [15.]

2.7.7 Muut IEEE 802.11-standardilaajennukset

IEEE kehittää tasaisin väliajoin uusia standardilaajennuksia, joista osa päätyy lopullisiksi standardeiksi. Oheisessa taulukossa tarkastellaan IEEE:n 802.11-standardilaajennuksia ja kerrotaan lyhyesti niiden ominaisuudet.

Taulukko 1. Luettelo IEEE 802.11 -standardilaajennuksista. [16. s. 7-12.]

Standardi	Ominaisuus
802.11d	Sisältää uusia kenttiä tukiasemien levitysviesteihin, joissa kerrotaan laitteen sijaintimaa. Pyrkimyksenä on, että langaton laite osaa valita itse oikean maakohtaisen taajuuskaistan.
802.11e	Sisältää toimintoja verkon suorituskyvyn ja palvelunlaadun kehittämiseksi. Pyrkimyksenä on minimoida verkon viiveitä. Suunnattu erityisesti multimedialiikennettä varten.
802.11h	Sisältää muutoksia Euroopassa 5 GHz:n taajuusalueella toimiville laitteille. Pyrkimyksenä vähentää häiriötekijöitä Euroopan asevoimien satelliitti- ja tutkakommunikoinnin kanssa. Sisältää lisäksi dynaamisen taajuuden valinnan (DFS) ja lähetystehon hallinnan (TPC).
802.11i	Sisältää parannuksia valmistajakohtaisiin tietoturvaominaisuuksiin määrittäen ne osaksi standardia. Mahdollistaa AES-salauksen ja 802.1x-todennuksen käyttämisen.
802.11j	Japaniin suunnattu aluepäivitys, joka lisää radiokanavia 4,9 ja 5 GHz:n välille.
802.11k	Mahdollistaa verkon tehokkuuden optimoinnin kanavavalintojen, roaming:n ja TCP:n kautta. Tarjoaa tiedot käyttäjälle etsiä paras saatavilla oleva tukiasema.

Jatkuu.

Taulukko 1. Luettelo IEEE 802.11 -standardilaajennuksista, jatkuu. [16. s. 7-12.]

Standardi	Ominaisuus
802.11p	Mahdollistaa liikkuvien ajoneuvojen välisen kommunikoinnin (WAVE). Lisäksi mahdollistaa kommunikoinnin liikkuvan ajoneuvon ja paikallaan olevan tukiaseman välillä käyttäen Intelligent Transportation System-tekniikkaa (ITS) 5,9 GHz:n taajuusalueella.
802.11r	Mahdollistaa mobiililaitteille nopean siirtymän BSS-verkkojen välillä, jonka ansiosta VoIP-puhelut ovat mahdollisia tukiasemien vaihdoksen yhteydessä.
802.11s	Mahdollistaa langattomien laitteiden välisen langattoman mesh-verkon muodostamisen.
802.11u	Mahdollistaa tiedonsiirron muiden kuin 802.11-standardien välillä.
802.11v	Sallii asiakaslaitteiden konfiguroinnin kun ne ovat yhteydessä langattomaan verkkoon.
802.11w	Datakehysten hallintaa parantava tietoturvapäivitys.
802.11y	Mahdollistaa 802.11-standardin laitteiden käytön Yhdysvalloissa 3,65 – 3,7 GHz:n taajuusalueella.
802.11z	Uusi DLS-tekniikan (Direct Link Setup) mekanismi, joka sallii operoinnin DLS:iin pystymättömän tukiaseman kanssa. Tarjoaa lisäksi uusia virransäästömahdollisuuksia.
802.11ad	Nopea taajuuden vaihtomahdollisuus 2,4 GHz:n ja 5 GHz:n taajuuksien välillä sekä uusi 60 GHz:n taajuusalue.
802.11af	Käyttää käyttämättömiä TV-taajuuksia.

2.7.8 HiperLAN

HiperLAN:n (High Performance Radio LAN) kehitti ETSI (European Telecommunications Standards Institute). HiperLAN on eurooppalainen vastine IEEE 802.11-standardeille. Se käyttää 5 GHz:n taajuusaluetta verkkoyhteyden maksiminopeuden ollessa 20 Mb/s. Standardin seuraava versio HiperLAN/2 kasvatti teoreettisen nopeuden 54 Mb/s:iin. HiperLAN/2 keskittyi erityisesti verkkoliikenteen virheettömyyden varmistamiseen, joka omalta osaltaan hieman kasvatti

latenssiaikaa. Standardin kolmas versio HomeRF suunniteltiin ainoastaan kotikäyttöön, sillä se tarjosi vain varsin lyhyet yhteysvälit. HomeRF:a ei enää kehitetä eikä sitä käyttäviä laitteita ole saatavilla. [3, s. 47–48.]

802.11-standardien kehittyessä HiperLAN-standardi ei pystynyt haastamaan 802.11-standardia Euroopassa, joka oli HiperLAN:lle ainoa mahdollinen merkittävän markkinaosuuden alue. 802.11-standardit ovatkin tällä hetkellä käytännössä ainoat vaihtoehdot langattomien lähiverkkojen toteutuksiin. Lisäksi HiperLAN-tuotteiden saatavuus on nykyaikana hyvinkin vähäistä. [5, s. 133.]

2.8 Langattoman lähiverkon laitteet

2.8.1 WLAN-kortti

Jokainen laite, joka käyttää langatonta verkkoa, tarvitsee verkkokortin. Verkkokortin avulla laite tunnistaa alueella olevat langattomat verkot. Ilman verkkokorttia viestintä langattomien verkkojen välillä ei toimi. Verkkokorttien ulkomuodot ja liitäntävaihtoehdot (USB, PCI, Mini-PCI) vaihtelevat laitevalmistajista riippuen. Pöytätietokoneisiin liitettävissä verkkokorteissa on useimmiten ulkoinen antenni. Nykyään suurimmassa osassa myytävissä kannettavissa tietokoneissa ja älypuhelimissa on sisäisillä antenneilla oleva verkkokortti. Kuvassa 1 on esimerkki PCIe-väylään liitettävästä langattomasta verkkokortista.

Kuva 1. Asuksen valmistama PCIe-väylään liitettävä langaton verkkokortti. [17.]

2.8.2 WLAN-tukiasema

Yleinen osa langattoman verkon topologiaa on tukiasema. Tukiaseman avulla jaetaan langallinen Ethernet-verkko ilmateitse käyttöön. Tukiasema onkin yleensä fyysisesti kytkettynä langalliseen verkkoon parikaapeleilla. Lisäksi tukiasema voi toimia yhdyskäytävänä tarjoten palveluina esimerkiksi reitityksen, VPN:n, NAT:n ja DHCP:n. Nykyään monet tukiasemat tukevat Power over Ethernet -toimintoa (PoE), jolloin tukiasema saa käyttövirtansa suoraan parikaapelin kautta eikä tarvitse erillistä sähkökaapelia. Kuvassa 2 on esimerkki tukiasemasta.

Kuva 2. TP-LINK langaton tukiasema. [18.]

2.8.3 WLAN-ohjain

Suuren yrityksen verkkokokonaisuudessa voi olla käytössä useita kymmeniä tai jopa satoja tukiasemia. Jokaisen tukiaseman konfigurointi ja hallinnointi yksitellen olisi todella aikaa vievää. WLAN-ohjaimen avulla kaikkia verkon tukiasemia voidaan helposti hallita keskitetysti. WLAN-ohjain mahdollistaa tiheän tukiasemaverkkojen rakentamisen, joissa eri tukiasemien kuuluvuusalueet menevät osittain päällekkäin. Kun yhden tukiaseman alueella on paljon käyttäjiä, kytkin voi ohjata uusia käyttäjiä automaattisesti toiselle tukiasemalle pitäen verkolle tulevan kuormituksen tasaisena. [19.]

WLAN-ohjaimen avulla yritykset voivat käyttää langatonta verkkoa joustavasti erilaisiin tarpeisiin. WLAN-ohjaimen tukevat rinnakkaisten langattomien verkkojen luontia samoja tukiasemia käyttäen, joten erilaisten palveluiden luonti on yksinkertaista. Esimerkkinä palvelusta on yrityksen vierailijaverkko, johon pääsee yrityksen teknisen tuen tarjoamilla väliaikaistunnuksilla. Vierailijaverkon palvelut on voitu rajoittaa sähköpostin käyttöön ja internet-sivujen selaamiseen. Samoissa tukiasemissa on rinnalla yrityksen oma verkko, joista työntekijät pääsevät käyttämään yrityksen käyttämiin palveluihin tai tietojärjestelmiin. [19.]

3 Langattoman lähiverkon tietoturva

3.1 Tietoturvan tavoitteet ja perusmäärittelyt

Langattomille lähiverkoille tietoturva on elintärkeää, koska viestisignaalit etenevät ilmassa ollen näin kaikkien tavoitettavissa, varsinkin jos tietoturva ei ole riittävällä tasolla. IETF (Internet Engineering Task Force) on määritellyt kuusi toinen toistaan täydentäviä tietoturvan turvapalvelua, jotka sopivat hyvin myös langattomien lähiverkkojen tietoturvan tavoitteiksi. Turvapalvelut on koottu taulukkoon 2.

Taulukko 2. Tietoturvan turvapalvelut [3, s. 70.]

Tiedon luottamuksellisuus	Elektronista tietoa voi lukea ja välittää vain siihen oikeutetut henkilöt.
Tiedon eheys	Tietoa voi muuttaa tai poistaa vain tähän toimenpiteeseen etukäteen oikeutettu henkilö.
Todennus	Tehdyt toimenpiteet voidaan kiistatta todentaa jälkikäteen.
Kiistämättömyys	Varmistaa tiedon, henkilön ja toimenpiteiden aitouden-
Pääsynvalvonta	Varmistetaan, että vain oikeutetut henkilöt pääsevät tietoon käsiksi.
Käytettävyys	Tieto on kaikkien siihen oikeutettujen saatavilla sekä käytettävissä kaikissa olosuhteissa sovittuun aikaan.

Tietoturvan riittävä toteuttaminen vaatii toimiakseen järjestelmällisen suunnittelun, toteutuksen ja seurannan. Toteutus alkaa tietoturvapolitiikasta, johon on määritelty organisaation tietoturvan tavoitteet, turvattavat resurssit, verkkolaitteet, ja noudatettavat menettelytavat. Tietoturvapolitiikan perusteella on mahdollista toteuttaa tarvittavat turvatoimenpiteet, jotka sisältävät esimerkiksi ohjeita menettelytavoiksi. Turvatoimenpiteiden jälkeen järjestelmän ja verkon turvata-

soa seurataan hyökkäysten, väärinkäytösten tai muiden haitallisten toimintojen havaitsemiseksi. Seuranta varmistaa, että suunniteltu tietoturva toteutuu. Lisäksi erilaisia ratkaisuja ja toimenpiteitä tulee testata ajoittain turvallisuuden varmistamiseksi. Näiden perusteella turvallisuutta voidaan parantaa. Tietoturvan kanssa työskentely onkin jatkuvaa kehittymistä, sillä uusia turvallisuusuhkia kehittyy ja tietoturva on syytä pitää ajan hermolla (kuvio 7). [3, s. 70.]

Kuvio 7. Järjestelmällinen tietoturvapolitiikka. [3, s. 71.]

3.2 Tietoturvauhat

Langattomiin verkkoihin voi kohdistua monenlaisia tietoturvauhkia. Koska langattomassa verkossa viestisignaalit etenevät ilmassa, ne ovat avoimesti tavoitettavissa jos tietoturva ei ole riittävällä tasolla. Langattomien verkkojen laitteet tuleekin sijoittaa paikkoihin, joihin ulkopuolisten on hankalaa päästä. Verkkolaitteiden portteihin ei pidä pystyä liittämään ylimääräisiä laitteita ja laitteisiin on asetettava vahvat salasanat, jotka sisältävät sekä isoja että pieniä kirjaimia ja mieluusti myös erikoismerkkejä. Langattoman verkon yleisimpiä tietoturvauhkia ovat palvelunestohyökkäys, välistävetohyökkäys, liikenteen tarkkailu ja luvaton pääsy. [3, s. 70–71.]

3.2.1 Palvelunestohyökkäys

Palvelunestohyökkäyksellä (Denial of Service, DoS) voidaan aiheuttaa suurta haittaa langattomalle verkolle. Hyökkäyksellä on mahdollista jopa estää langattoman verkon käyttö kokonaan ja aiheuttaa näin ollen taloudellisiakin tappioita

yritykselle. Yksi palvelunestohyökkäyksen muodoista on väsytyshyökkäys. Tässä tapauksessa hyökättävään verkkoa kuormitetaan suurella määrällä paketteja. Verkossa pakettien liikennemäärä kuluttaa kaikki verkon resurssit, jonka seurauksena verkko kaatuu. [5, s. 176.]

Toinen palvelunestohyökkäyksen tyyli on käyttää voimakkaita radiosignaaleja, jotka hallitsevat ilmateitä ja häiritsevät langattomien verkkojen laitteiden lähettämiä signaaleja. Voimakkaiden signaalien käyttäminen hyökkäyksessä on kuitenkin riskialttiimpaa väsytyshyökkäykseen verrattuna, sillä hyökkäykseen tarvittavan lähettimen täytyy sijaita lähellä verkkoa, ja verkon haltijat voivat löytää lähettimen verkkoanalysaattorin paikannusvälineiden avulla. Kun verkkoa häiritsevä lähetin on löydetty, se on helppo poistaa ja se voi mahdollisesti johtaa hyökkääjien jäljille. Langatonta verkkoa voi myös häiritä tahattomasti radiosignaaleilla, sillä mikroaaltouunit ja langattomat puhelimet käyttävät samoja radiotaajuuksia. [5, s. 176–177.]

3.2.2 Välistävetohyökkäys

Välistävetohyökkäyksessä hakkeri laittaa luvattoman laitteen käyttäjän ja langattoman verkon väliin ARP-protokollaa hyväksikäyttäen. ARP-protokollan avulla hakkeri pystyy selvittämään kohdeverkkokortin fyysisen osoitteen. Tällä tavalla hakkeri pystyy ohjaamaan kaiken liikenteen käyttäjän ja kohdeaseman väliltä kulkemaan oman laitteensa kautta. Tällöin hakkerin on mahdollista saada tietoonsa yrityksessä käytettäviä salasanoja tai jopa saada muodostettua yhteyden yrityksen käyttämiin palvelimiin muiden sitä huomaamatta. [5, s. 174–175.]

Välistävetohyökkäyksiä vastaan voi suojautua Secure ARP -tekniikalla (SARP), joka on ARP:n laajennus. SARP muodostaa erityisen turvatunnelin asiakkaan ja tukiaseman välille ja jättää huomioimatta kaikki tunnelin ulkopuolelta tulevat pyynnöt. SARP vaatii kuitenkin erillisten ohjelmistojen asentamisen kaikkiin laitteisiin, joilla sitä haluttaisiin käyttää. [5, s. 175–176.]

3.2.3 Passiivinen tarkkailu

Hakkeri voi helposti tarkkailla suojaamatonta tai heikosti suojattua langattoman verkon verkkoliikennettä ilman, että ovat rakennuksen sisällä. Tätä kutsutaan passiiviseksi tarkkailuksi. Passiivisella tarkkailulla hakkeri voi saada tietoonsa käyttäjätunnuksia, salasanoja tai muuta arkaluontoista tietoa. Passiivista tarkkailua voi tapahtua pitkien matkojen päästä suunta-antennin avulla, jota ei pystytä havaitsemaan. Lisäksi internetistä on saatavilla erilaisia hakkerointityökaluja, joilla voi tarkkailla suojaamattomia langattomia datapaketteja tai purkaa heikkoja salausavaimia. Passiiviselta tarkkailulta voi suojautua käyttämällä tehokasta salausprotokollaa, jota on hankalaa ja hidasta purkaa. [5, s. 172.]

3.3 Salausmenetelmät ja suojautuminen

Langattomaan lähiverkkoon suuntautuvilta hyökkäyksiltä suojautuminen on moniosainen prosessi. Tehokas suojautumiskeino on pyrkiä rajoittamaan radiosignaalien leviämistä halutun alueen ulkopuolelle ja vastaavasti ei-toivottujen signaalien ulottuminen omalle langattoman verkon alueelle. Rakennukseen kohdistuvat tietoturvaratkaisut olisikin hyvä huomioida jo rakennuksen suunnitteluvaiheessa, sillä jälkikäteen tehtävät suojaukset voivat olla haasteellisia toteuttaa.

Rakennusten seinä- ja ikkunarakenteisiin tulee kiinnittää huomiota ja sisäseinien metalliset tukirakenteet on syytä maadoittaa. Lisäksi sisä- ja ulkoseinissä on suositeltavaa käyttää metallipohjaisia maaleja. Rakennusten ikkunoiden tulisi olla kuparilämpöeristettyjä tai metallikalvopohjaisia ja kaihtimien sijaan tulisi käyttää metalliväriäystä. Radiosignaalien vuotamista rakennuksen ulkopuolelle tulisi myös tutkia. Vuotoa pystytään vähentämään suuntaamalla tukiasemien antennit rakennuksen sisäosien suuntaan. [5, s. 177–178.]

3.3.1 WEP

WEP (Wired Equivalent Privacy) on IEEE:n 802.11-standardin suojaustekniikka, joka kehitettiin vastaamaan kaapeliverkon turvallisuutta. WEP-salauksessa kaikille laitteille jaetaan sama salausavain, jonka avulla voidaan liittyä verkkoon. Salausavaimena käytetään 64- tai 128-bittistä salausavainta ja salaus suorite-

taan RC4-salausalgoritmillä. WEP:ssä heikkoutena on ainoastaan käytettävän laitteen autentikointi, eikä käyttäjää itse autentikoida ollenkaan. Jos joku ulkopuolinen saa työaseman luvatta käyttöönsä, tämä voi päästä myös käyttämään salattua verkkoa luvattomasti. [9, s. 320.]

WEP-salauksen onnistuivat murtamaan tutkijat Fluher, Mantin ja Shamir vuonna 2001. He osoittivat, että julkisen RC4-salausalgoritmin ensimmäiset tavut paljastivat tietoja salausavaimen rakenteesta, jota hyväksikäyttäen langattoman verkon liikennettä pystyttiin analysoimaan. Analysoinnin avulla oli mahdollista paljastaa verkon käyttämä salausavain. Tehokkaampien salausmenetelmien myötä WEP:n käyttäminen salausmenetelmänä ei ole enää suositeltavaa. [9, s. 320.]

3.3.2 WPA ja WPA2

WPA (Wi-Fi Protected Access) kehitettiin korjaamaan WEP-salauksen puutteita. WPA suunniteltiin siten, että se on mahdollista ottaa käyttöön pelkällä ohjelmistopäivityksellä. WPA käyttää salausavaimen muodostamiseen TKIP-protokollaa (Temporal Key Integrity Protocol). [9, s. 320.]

WPA-salauksen kanssa on mahdollista käyttää 802.1x-autentikointia EAP-pakettisuodatuksen kanssa, joka mahdollistaa ulkopuolisen autentikointipalvelimen käytön autentikointiprosessissa. Toinen, kevyempi autentikointimahdollisuus WPA:ssa on käyttää PSK-salausavainta (Pre Shared Key), jolloin erillistä autentikointipalvelinta ei tarvita. PSK-salausavainta käytettäessä tukiasema ja verkkoon liittyvä työasema todentavat toisensa haaste-vastaus -tekniikalla (Challenge-response). Tässä menetelmässä käytetään kummankin osapuolen tuntemaa avainta (Master key). Menetelmä on nelivaiheinen, jolloin molemmat osapuolet autentikoituvat toisilleen. WPA:sta kehitettiin myös versio 2 (WPA2), jossa salausavainta hallitaan AES-salauksella (Advanced Encryption Standard). WPA2 on nykyään pakollinen suojaus kaikissa Wi-Fi-sertifioiduissa laitteissa. [9, s. 320.]

3.3.3 TKIP

TKIP (Temporal Key Integrity Protocol) kehitettiin alkuperäisen WEP:n tilalle korjaamaan WEP:n tietoturvapuutteita. TKIP jakaa asiakkaan ja tukiaseman kesken 128-bittisen väliaikaisen avaimen, joka yhdistetään asiakkaan MAC-osoitteen ja kehykseen järjestysnumeron neljän eniten merkitsevän bitin kanssa. Tästä saatu väliaikainen avain yhdistetään kahden alimman bitin kanssa, josta saadaan laitteelle uniikki kehyskohtainen avain. Lisäksi TKIP vaihtaa tilapäisiä avaimia 10 000 paketin välein tietoturvan vaatimuksista riippuen. Näin ollen salakuuntelijat eivät saa riittävästi dataa avaimen murtamiseen. [5, s. 183.]

3.3.4 AES

AES (Advanced Encryption Standard) on symmetrinen salausmenetelmä. Se on Yhdysvaltojen kauppaministeriön alaisen standardoimisviraston NIST:n standardoima ja sitä käytetään suojaamaan Yhdysvaltain hallinnon organisaatioiden arkaluontoista informaatiota. AES käsittelee tietoa 128 bitin lohkoina ja salausavaimet ovat 128-, 192- tai 256-bittisiä. AES:llä salattua tietoa on asiantuntijoiden mukaan mahdotonta murtaa. Brute force -hyökkäys, jossa käydään kaikki mahdolliset salausavaimet läpi, veisi supertietokoneelta noin triljoona vuotta (miljardi kertaa miljardi vuotta). [5, s. 184; 20].

3.3.5 MAC-suodatus

MAC-suodattimen avulla on mahdollista rajata langattoman verkon liikennettä. MAC-suodatuksessa tukiasemalle luodaan lista työasemien MAC-osoitteista, joilla on lupa liittyä langattomaan verkkoon. Jos tukiasema ei löydä laitteen MAC-osoitetta listastaan, se estää laitteen liittymisen verkkoon. Menetelmä ei ole järkevä yritysverkoissa, sillä MAC-osoitteiden pituuden takia niiden ylläpito ja syöttäminen jokaiseen tukiasemaan on raskasta ja aikaa vievää. MAC-suodatus toimiikin paremmin kotiverkoissa, joissa verkkoon liittyviä laitteita on vain vähän. [3, s. 73.]

MAC-suodatus ei kuitenkaan ole täysin turvallinen vaihtoehto. Verkkourkintaan tarkoitetuilla ohjelmilla on myös mahdollista nähdä verkkoon liittyneiden laittei-

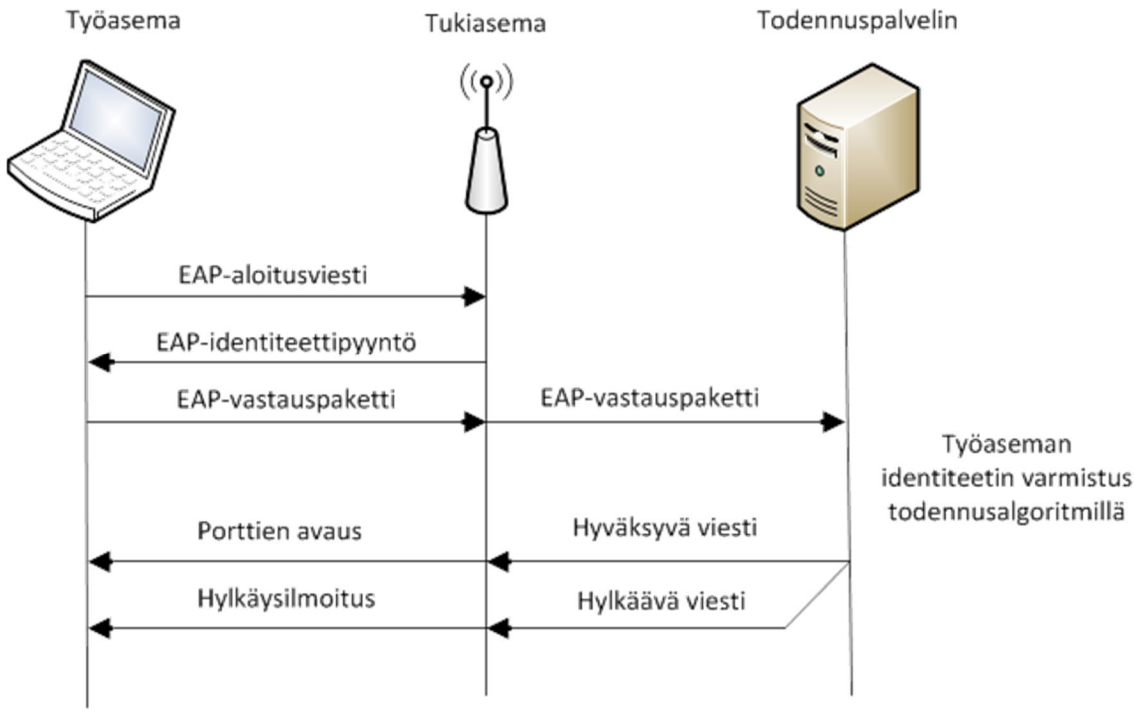
den MAC-osoitteet. Hakkeri voi näin ollen muuttaa oman laitteensa MAC-osoitteen vastaamaan luvallisen käyttäjän osoitetta ja huijaten tukiasemaa päästämään tämän verkkoon. [5, s. 187.]

3.4 Todennusmenetelmät

3.4.1 802.1x-todennus

802.1x-todennuksessa tunnistamaton langaton asiakaslaite pyrkii muodostamaan yhteyden langattomaan tukiasemaan. Tukiasema vastaa avaamalla asiakkaalle portin, jossa sallitaan ainoastaan EAP-pakettien (Extensible Authentication Protocol) lähettäminen asiakkaalta todennuspalvelimelle. Kun asiakas on tunnistettu, tukiasema avaa asiakkaan portit esimerkiksi http- ja DHCP-liikenteelle sekä POP3-paketeille todennuspalvelimen ilmoittamien oikeuksien mukaisesti. 802.1x tarjoaa tehokkaan todennuksen, vaikka verkossa ei olisi salausta ollenkaan. [5, s. 189–190.]

Kuviossa 8 on esitetty 802-1x-todennuksen vaiheet. Ensimmäisenä tukiasemaan yhdistyvä työasema lähettää tukiasemalle EAP-aloitusviestin, jossa työasema pyytää lupaa liittyä verkkoon. Tukiasema lähettää vastauksena EAP-identiteettipyynnön, johon työasema vastaa. Tukiasema välittää EAP-vastauspaketin todennuspalvelimelle. Todennuspalvelin varmistaa työaseman identiteetin ja hyväksyy tai hylkää työaseman kirjautumisen. Jos työasema on tunnistettu ja sen annetaan liittyä verkkoon, todennuspalvelin lähettää kirjautumisen sallivan viestin tukiasemalle, joka avaa työasemalle sen tarvitsemat portit. Vastaavasti, jos todennuspalvelin ei salli työaseman kirjautumista, se lähettää hylkäävän viestin tukiasemalle, joka ilmoittaa asiasta työasemalle.



Kuvio 8. 802.1x-todennuksen vaiheet.

3.4.2 Todennus RADIUS-palvelimella

Yleinen 802.1x-todennuksessa käytettävä todennuspalvelin on RADIUS (Remote Access Dial-In User Service). RADIUS-palvelin vastaanottaa verkon yhteyspisteen välittämät yhteydenottopyynnöt ja suorittaa käyttäjän tunnistamisen. Tämän jälkeen palvelin lähettää vastauksena viestin tunnistuksen hyväksymisestä tai hylkäämisestä. [3, s. 76–77.]

Liikenne asiakkaan ja RADIUS-palvelimen välillä alkaa aloitussanomalla, johon yhteyspiste vastaa kysyen käyttäjätietoja. Syötetyt käyttäjätiedot lähetetään yhteyspisteelle, joka muuttaa sanoman RADIUS-pyynnöksi palvelimelle. Palvelin lähettää haastepaketin, joka sisältää satunnaisen merkkijonon sekä salaisella avaimella salatun haasteen. Asiakkaan käyttämä laite lukee käyttäjän kirjoittaman salasanan ja salaa haastejonon ja lähettää viestin RADIUS-palvelimelle. Palvelin vertaa saamiaan tietoja tunnistetietoihin ja hyväksyy tai hylkää kirjautumispyynnön. [3, s. 76–77.]

3.4.3 TACACS+

TACACS+ (Terminal Access Controller Access-Control System Plus) on Cisco Systemsin kehittämä todennusmenetelmä. Se on vaihtoehtoinen todennusmenetelmä RADIUS-menetelmälle, tosin TACACS+ tukee ainoastaan Ciscon laitteita. TACACS+ salaa kaiken datan datapaketista otsikkokenttää lukuun ottamatta, kun kirjautumistietoja lähetetään asiakkaan ja todennuspalvelimen välillä. RADIUS puolestaan salaa vain käyttäjän salasanan. Kun RADIUS yhdistää todennuksen (authentication) ja valtuutuksen (authorization), TACACS+ käsittelee nämä erillisinä operaatioina. TACACS+ käyttää TCP-protokollaa UDP-protokollan sijaan. TCP-protokolla sopeutuu kasvaviin ja ruuhkaisiin verkkoihin UDP:tä paremmin ja kertoo tarkempia tietoja esimerkiksi kaatuneista tai epäkuntoisista palvelimista. [21.]

4 John Deere Forestry Oy:n tehdasalueen langattoman verkon katvealueet

John Deere Forestry Oy:n Joensuun tehdas on halunnut poistaa langattoman verkkonsa katvealueet. Katvealueet poistettiin lisäämällä tukiasemia paikkoihin, joissa langaton yhteys hidastuu tai katkeaa kokonaan. Lisättävien tukiasemien asennuspaikat suunniteltiin siten, että tukiasemien tarvitsemat kytkennät on helppo vetää voimassa oleviin rakenteisiin, josta tukiasema antaa parhaan mahdollisen signaalin tarvitulle alueelle. Tehdasalueen verkkoon tehtävät muutokset lisätään dokumentaatioon. Verkkokaappeihin tehdyt lisäkytkennät dokumentoidaan omaan järjestelmäänsä kuten myös lisätyt tukiasemat, joiden tiedot lisätään järjestelmään, joka sisältää kaikkien käytössä olevien laitteiden tiedot.

4.1 Lähtötilanne

John Deere Forestryn Joensuun tehtaalla on voimassa oleva langaton lähiverkko. Langaton lähiverkko kattaa tehdasalueen, toimistorakennuksen sekä myynti- ja huoltorakennuksen. Langattomassa lähiverkossa on tarjolla verkkoja työntekijöille, työntekijöiden henkilökohtaisille laitteille ja ulkopuolisille tarjolla oleva vierailijaverkko. Työntekijöiden verkkoon pääsevät liittymään ainoastaan yrityksen toimialueeseen liitetyt työasemat ja käyttäjät. Vierailijaverkko on varattu yrityksessä vierailijoille, joille yrityksen Help Desk luo väliaikaiset vierailijatunnukset.

Langattoman verkon katvealueita ovat tehdasalueen reuna, jossa sijaitsee metsäkoneiden hyttivarasto, sekä tehdasrakennuksesta erillisen lähettämörakennuksen vieressä sijaitseva rengasvarasto. Tehdasrakennuksessa ja sen ympäristössä langatonta verkkoa käyttävät eniten trukit, joissa kannettavat tietokoneet ovat yhteydessä yrityksen JMES-tuotannonohjausjärjestelmään, jota käytetään internetselaimella. Molemmilta varastoilta trukit kuljettavat osia rakennettaviin metsäkoneisiin, ja trukin saapuessa katvealueelle yhteys JMES-järjestelmään hidastuu merkittävästi tai katkeaa kokonaan.

Tarkoituksenani oli poistaa tehdasalueen katvealueet mittaamalla langattoman verkon signaalin kuuluvuutta katvealueilla. Kartoituksen jälkeen tehtäväni oli suunnitella tukiasemille sopivat asennuspaikat ja asentaa tukiasemat paikalleen tehtaan kunnossapidon ammattilaisten avulla. Lopuksi tarkastellaan, miten uusien tukiasemien lisääminen on parantanut tehdasalueen langattoman verkon kuuluvuutta.

4.2 Mittaukset katvealueilla

Langattoman verkon kuuluvuutta mitattiin inSSIDer-ohjelmalla. Ohjelma havaitsee tukiasemien radiosignaalien voimakkuudet ja esittää tulokset taulukkona, jossa näkyvät mac-osoite, verkon SSID, käytettävä kanava, signaalin herkkyys desibelimilliwatteina (dBm), verkon salaus ja maksiminopeus. Radiosignaalin voimakkuutta voi myös tarkastella graafisesta kuvaajasta tai kuvaajasta, joka sijoittaa signaalit käytettävien kanavien mukaan. Taulukossa 3 on esitetty tukiasemavalmistajan ilmoittamat signaalin voimakkuutta vastaavat tiedonsiirtonopeudet käytettäessä IEEE 802.11g-standardia.

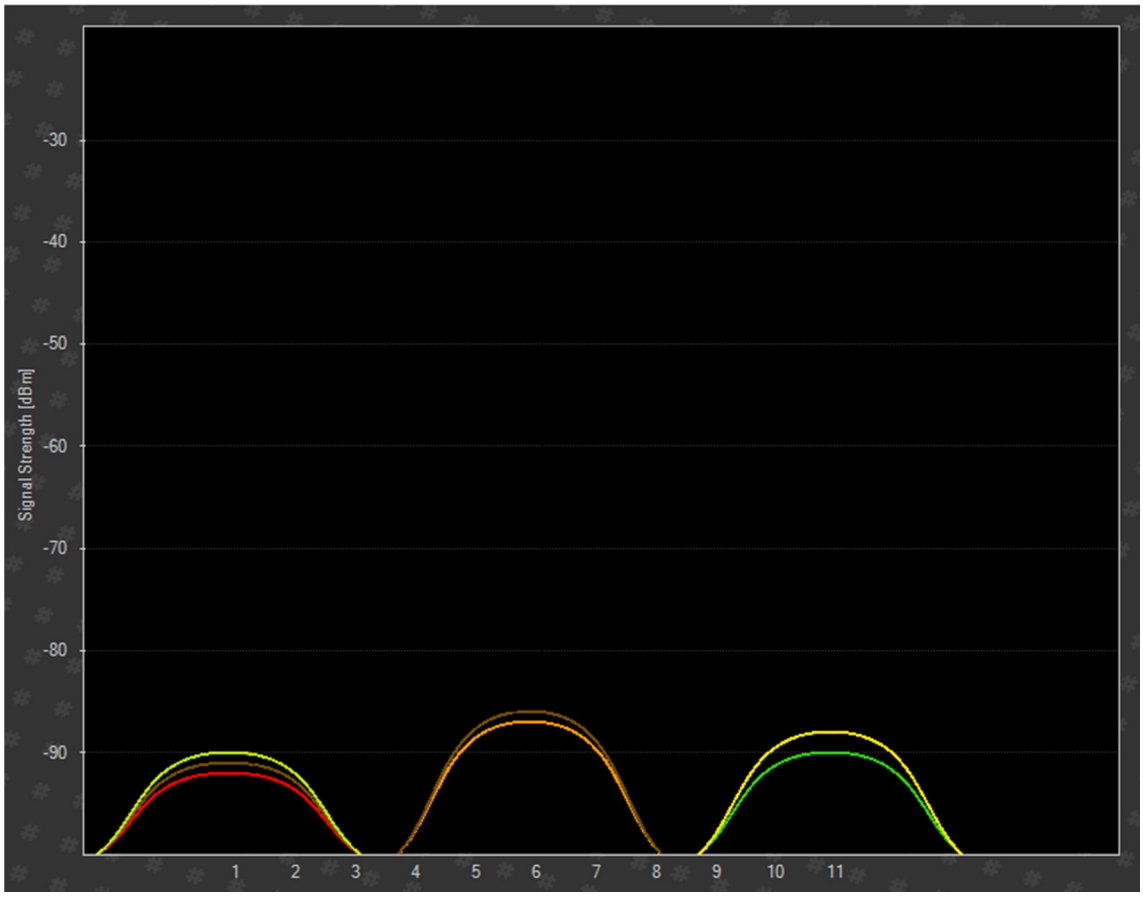
Taulukko 3. Signaalin voimakkuus suhteutettuna tiedonsiirtonopeuksiksi. [22.]

Signaalin voimakkuus (dBm)	Teoreettinen tiedonsiirtonopeus (Mb/s)
-73	54
-73	48
-74	36
-78	24
-81	18
-83	12
-88	11
-85	9
-91	6
-91	5,5
-93	2
-96	1

Taulukosta 3 voidaan havaita, että mitä pienempi negatiivinen signaalin voimakkuuden arvo on, sitä suurempi on teoreettinen tiedonsiirtonopeus.

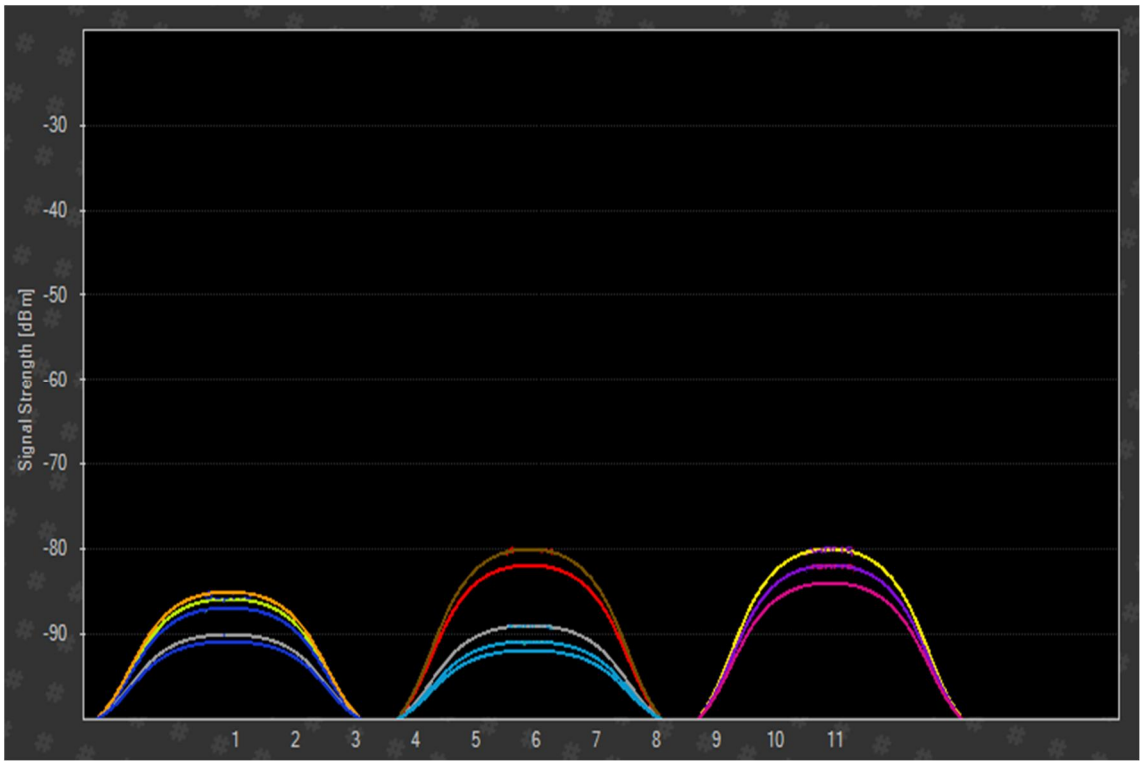
Mittaukset suoritettiin kulkemalla ennakkoon tiedetyillä katvealueilla eli hytti- ja rengasvarastolla inSSIDer-ohjelman mitatessa langattoman lähiverkon signaalin voimakkuutta. Langattoman lähiverkon signaalin voimakkuuden muuttuessa muutoskohdat merkittiin muistiin alueen pohjapiirroksiin. Mittausten lopuksi piirrettiin kartta signaalien voimakkuuksien vaihteluista varastoalueilla. Mittauksia suoritettiin kummallakin katvealueella useaan kertaan, jolloin mittaustulosten todenmukaisuudesta voitiin varmistua.

Hyttivarastolla kuljettaessa kohti varaston päätyä verkon signaali heikentyy nopeasti arvosta -60 dBm lukemaan -80 dBm, minimiarvon ollessa -86 dBm (kuvio 9). Tämä tarkoittaa noin 6 Mb/s:n teoreettista nopeutta, mutta todellisuudessa siirtonopeus on noin 40 % tästä eli noin 2,4 Mb/s. Siirtonopeuteen vaikuttavat etäisyyden ja esteiden lisäksi muiden laitteiden aiheuttama interferenssi ja mahdolliset muut käyttäjät samalla tukiasemalla. Samalla yhteys JMES-järjestelmään heikkenee merkittävästi ja selaimen sivun päivittyminen hidastuu, tai yhteys katkeaa kokonaan. Signaalin heikkenemiseen vaikuttavat tukiaseman kaukaisen sijainnin lisäksi tukiaseman ja hyttivaraston välillä olevat kaksi aaltopellistä tehtyä seinää sekä varastohyllyrivit, joilla voi välillä olla paljonkin suuria osia. Lisäksi hyttivaraston viereisellä ulkovarastolla signaalin voimakkuus heikkenee lukemaan -80 dBm kuljettaessa kohti alueen reunaa. Kuviossa 9 eri väreillä merkityt kuvaajat kuvaavat havaittuja tukiasemia näyttäen jokaisen tukiaseman signaalin voimakkuuden ja tukiaseman käyttämän kanavan. Tarkka pohjapiirros langattoman verkon signaalien voimakkuuksien mittaustuloksista hyttivarastolla ja viereisellä ulkovarastoalueella on poistettu luottamuksellisuuden vuoksi.



Kuvio 9. Signaalien voimakkuus hyttivaraston alueella.

Rengasvaraston alueella verkon signaali hidastuu arvoon -80 dBm asti (Kuvio 10). Verkon teoreettinen maksiminopeus on tällöin noin 20 Mpbs, eli todelliseksi maksiminopeudeksi jää noin 8 Mb/s. Yhteys JMES-järjestelmään ei katkea, mutta se selvästi heikkenee verrattuna tehtaan piha-alueen muihin alueisiin, joissa signaalin arvo pysyy -60 dBm ja -70 dBm:n välillä. Yksi tukiasema sijaitsee lähettämörakennuksessa toisella puolen rengasvarastoa ja signaali heikkenee sen kulkiessa rakennuksen seinien läpi aiheuttaen katvealueen lähettämörakennuksen toiselle puolelle. Lisäksi signaalia heikentävät varastohyllyriveissä varastoidut tavarat. Signaali on heikoimmillaan lähettämörakennuksen vieressä rakennuksen keskiosassa pituussuunnassa katsottuna. Kuviossa 10 eri väreillä merkitty kuvaaja kuvaa havaittua tukiasemaa näyttäen kyseisen tukiaseman signaalin voimakkuuden ja tukiaseman käyttävän kanavan. Tarkka pohjapiirros langattoman verkon signaalien voimakkuuksien mittaustuloksista rengasvarastolla on poistettu luottamuksellisuuden vuoksi.



Kuvio 10. Signaalien voimakkuus rengasvaraston alueella.

4.3 Uusien tukiasemien sijoituspaikat

Verkkoon lisättävät tukiasemat ovat mallia Cisco Aironet 1240AG Series 802.11a/b/g (kuva 3). Kyseinen tukiasema on suunniteltu haasteellisiin RF-ympäristöihin, kuten tehtaisiin, varastoihin tai suuriin vähittäistavaraliikkeisiin, jotka tarvitsevat laajan käyttölämpötila-alueen. Tukiasema tukee myös Power over Ethernet -toimintoa (PoE), jolloin tukiasema saa tarvitsevansa käyttövirran suoraan Ethernet-kaapelin kautta eikä erillistä sähkökaapelia tarvita. Tuettuja salaustekniikoita ovat WPA, WPA2, EAP, TKIP ja AES. Tukiasemassa on keskusmuistia 32 megatavua ja flash-muistia 16 megatavua. Tukiaseman toimintalämpötila on -20 °C:sta 55 °C:een. [22.]

Kuva 3. Cisco Aironet 1240AG – tukiasema. [22.]

Uusien tukiasemien sijoituspaikat suunnitellaan siten, että ne voidaan liittää olemassa olevaan verkkoon mahdollisimman helposti, mutta parantavat silti langattoman verkon katvealueiden kuuluvuutta suunnitellusti. Tukiasemia ei sijoiteta paikkoihin, joihin verkkokaapelit jouduttaisiin vetämään siten, että ne esimerkiksi roikkuisivat välillä ilmassa, tai paikkoihin, joihin täytyisi sijoittaa uusia rakenteita pelkästään tukiasemaa varten.

Hyttivarastolle tukiasema sijoitetaan teräksiseen tolppaan hyttivaraston läheisyyteen. Tukiaseman signaali kattaa näin sijoitettuna hyttivaraston alueen sekä viereisen ulkovarastoalueen, joka on myös aiemmin kärsinyt signaalin heikkoudesta. Tukiaseman sijoituspaikka mahdollistaa signaalin ulottuvuuden ulkovaraston etäisimpään nurkkaan esteettömästi. Tukiasemien sijoituspaikkaa esittävät kuvat on poistettu luottamuksellisten tietojen vuoksi.

Rengasvarastolle tukiasema sijoitetaan lähettämörakennuksen ulkoseinään asennuksen kannalta helposti soveltuvaan kohtaan. Tukiaseman sijoitus ulkoilmaan ei aiheuta ongelmia, sillä tukiasema sekä sen antennit asetetaan erillisen suojakotelon sisään. Tukiaseman signaali kattaa lähettämörakennuksen vieressä sijaitsevan rengasvaraston alueen, joka aiemmin jäi katveeseen lähettämörakennuksen taakse.

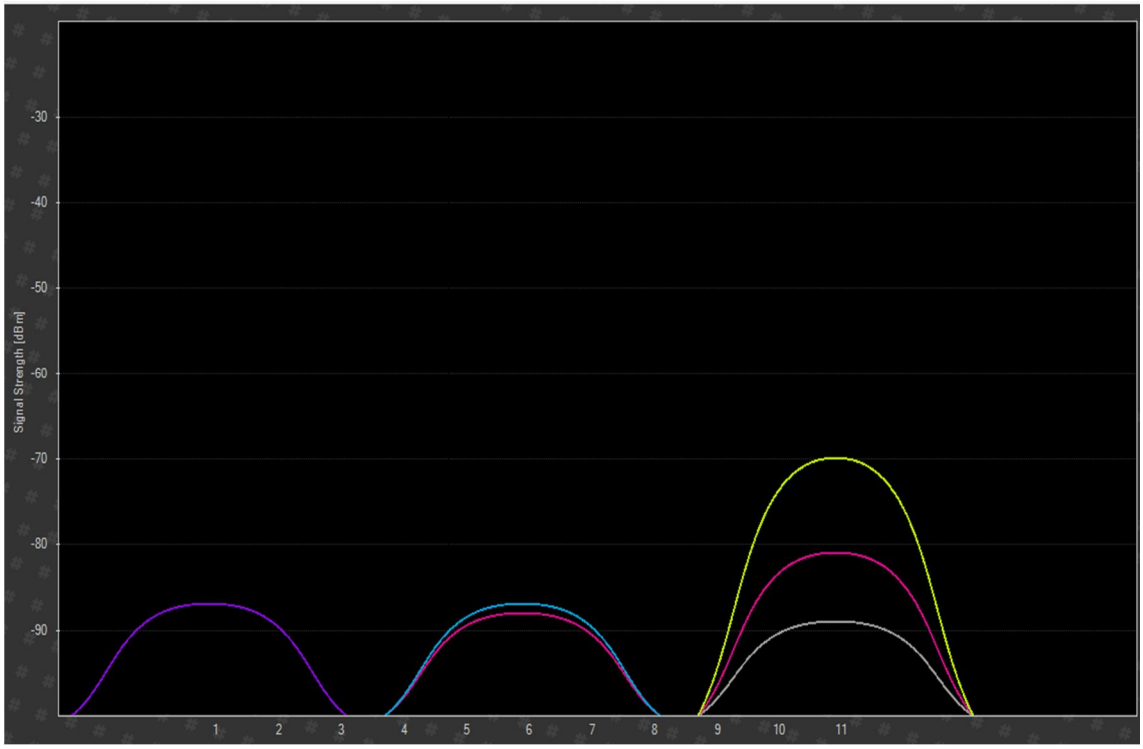
4.4 Verkkokaappeihin tehdyt kytkennät

Kahteen verkkokaappiin tarvitsi tehdä kytkentöjä uusia tukiasemia varten. Kytkentöjen jälkeen verkkokaapeista otettiin valokuvat, joihin merkittiin tehtyjen kytkentöjen paikat. Verkkokaappien kuvat on poistettu niissä olevien luottamuksellisten tietojen vuoksi.

4.5 Mittaukset tukiasemien asennusten jälkeen

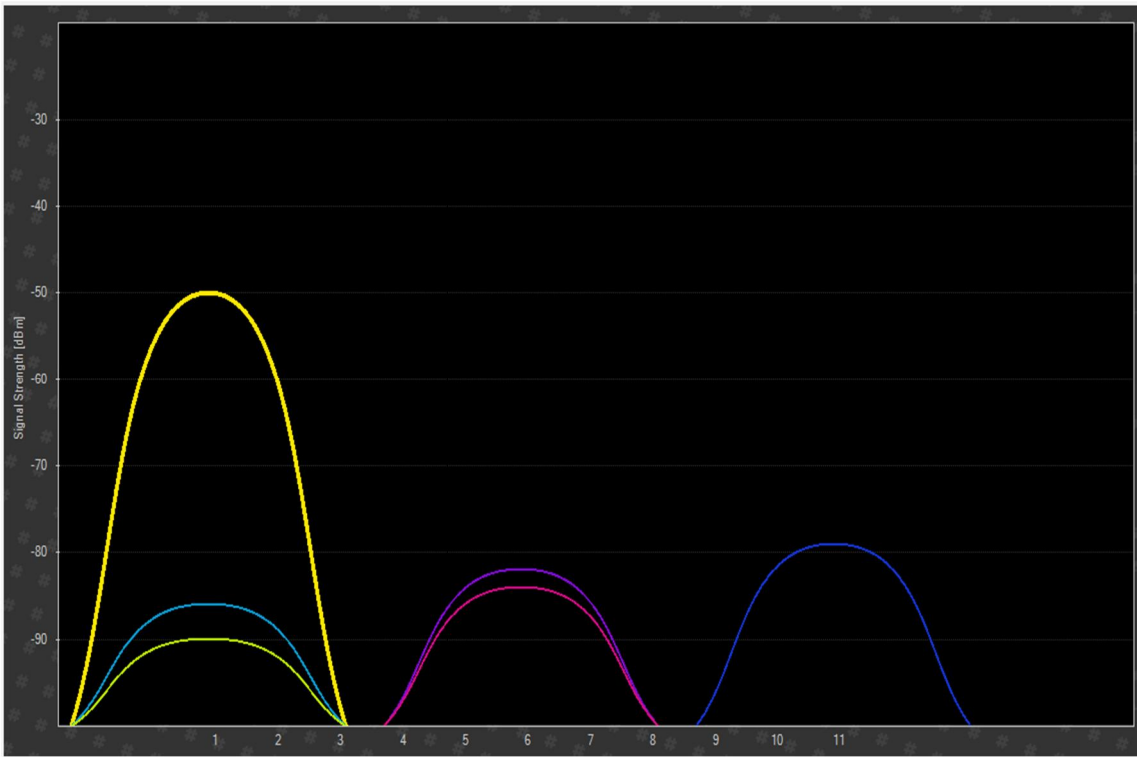
Uusien tukiasemien asennuksen jälkeen langattoman verkon signaalin kuuluvuutta mitattiin uudelleen inSSIDer-ohjelmalla ja verrattiin, miten signaalin voimakkuuden arvot ovat muuttuneet.

Hyttivarastolla signaalin voimakkuus pysyy pitkään arvossa -60 dBm ja hyttivaraston perimmäiseen nurkkaan mennessä vahvuus heikentyy arvoon -70 dBm, jota heikommaksi signaali ei heikkene (kuvio 11). Tässä tapauksessa verkon maksimitiedonsiirtonopeus on edelleen 54 Mb/s, eli todellinen nopeus on noin 21 Mb/s. Etäisyys tukiasemaan sekä varaston ja tukiaseman aaltopeltiseinä heikentävät hieman signaalia, mutta yhteys ei katkea missään vaiheessa. Ulkovaraston alueella signaali ei juuri heikkene arvosta -50 dBm huonommaksi. Uusi tukiasema näkyy kuviossa 11 keltaisella värillä. Tarkka pohjapiirros tukiaseman sijainnista varastoalueisiin nähden ja kuvaus signaalien voimakkuuksien tilasta on poistettu luottamuksellisuuden vuoksi.



Kuvio 11. Signaalien voimakkuus hyttivarastolla.

Rengasvarastolla signaalin voimakkuus pysyy lähes koko ajan arvossa -50 dBm (kuvio 12). Uutta tukiasemaa kuvaava viiva on väriltään keltainen. Hyllyrivistöjen välissä kulkiessa signaalin voimakkuus voi kuitenkin heiketä välillä nopeastikin johtuen suurista varastoiduista osista hyllyrivistöissä. Tällöin signaalin voimakkuuden arvo ei kuitenkaan laske -70 dBm:iä huonommaksi kuin hetkeksi. Uusi tukiasema näkyy kuviossa 12 keltaisella värillä. Tarkka pohjapiirros tukiaseman sijainnista ja signaalien voimakkuuksien tilasta rengasvarastolla on poistettu luottamuksellisuuden vuoksi.



Kuvio 12. Signaalien voimakkuus rengasvarastolla.

5 Pohdinta

Langattomien lähiverkkojen tekniikka on kehittynyt suuresti viimeisten vuosien aikana. Kehitystä on tullut niin laitteissa ja niiden käytettävyydessä sekä langattomien verkkojen standardeissa. Langattomien laitteiden liikuteltavuus tarjoaa laitteille käytännöllisyyttä. Langattomissa verkoissa on kuitenkin vieläkin heikkouksia sekä tietoturvapuutteita, minkä takia langattomat verkot eivät yksinään ole paras ratkaisu yritysten verkkoratkaisuiksi. Langaton verkko kuitenkin täydentää hyvin langallista verkkoa.

Opinnäytetyön tekeminen oli sekä mielenkiintoista että opettavaista. Aikaisempi kokemukseni langattomista lähiverkoista täydentyi merkittävästi langattomien verkkojen teoriaa opiskellessani sekä varsinaista työtä tehdessä. Lähdekirjallisuus ja internet tarjosivat tietoa langattomien lähiverkkojen teoriasta. Osittain turvauduin myös englanninkieliseen lähdemateriaaliin.

Opinnäytetyölle asetetut tavoitteet ja aikataulu olivat realistiset ja ne saavutettiin suunnitellun aikataulun puitteissa. Opinnäytetyön tekemisessä ei ilmennyt suuria ongelmia. Uudet tukiasemat ovat parantaneet langattoman verkkoyhteyden tasoa merkittävästi tehdasalueen osissa, joissa aiemmin yhteys on ollut hidas tai katkeillut kokonaan.

Opinnäytetyössä esitetyt tulokset langattoman lähiverkon voimakkuuksien mittauksista ovat luotettavia. Mittaukset on suoritettu kummallakin varastoalueella useaan kertaan mahdollisten häiriöiden tai muiden virhetuloksia aiheuttavien asioiden poissulkemiseksi. Mittaukset on suoritettu useaan kertaan ennen uusien tukiasemien asennusta ja myös tukiasemien asennusten jälkeen. Useaan kertaan suoritetuissa mittauksissa tulokset olivat samanlaisia, joiden perusteella tulosten luotettavuus on varmistettu.

Lähteet

1. Deere & Company. John Deere investoi Joensuun tehtaan valmistuskapasiteetin kasvattamiseen. 2012. [Viitattu 25.2.2014.] Saatavissa: http://www.deere.fi/wps/dcom/fi_FI/our_company/news_and_media/press_releases/2012/february/joe_investment/joe_investment.page
2. Deere & Company. John Deere juhlii Joensuun tehtaan 40. ja yhtiön 175. toimintavuotta. 2012. [Viitattu 25.2.2014.] Saatavissa: http://www.deere.fi/wps/dcom/fi_FI/our_company/news_and_media/press_releases/2012/june/175_40/175_40.page
3. Puska, M. Langattomat lähiverkot. Helsinki. Talentum. 2005.
4. Norwegian Air Shuttle ASA. WiFi-yhteys lennon aikana. 2014. [Viitattu 3.4.2014.] Saatavissa: https://www.norwegian.com/fi/matkapalvelut/travel-services-fi/wifi/
5. Geier, J. Langattomat verkot: perusteet. Helsinki. Edita Publishing Oy. 2005.
6. Media Road. Online Units Conversion. 2010. [Viitattu 25.3.2014.] Saatavissa: http://www.mediaroad.com/products/speedcheck/free_tools/unit_convert/
7. Honkanen, H. Lyhyen kantaman langattomat siirtotavat. Kajaanin ammattikorkeakoulu. Tietotekniikan koulutusohjelma. Oppimateriaali. 2011. [Viitattu 4.3.2014.] Saatavissa: http://gallia.kajak.fi/opmateriaalit/yleinen/honHar/ma/ELE_Langaton%20l%C3%A4hisiirto.pdf
8. Nguyen, H. Wireless access point (AP) automatic channel selection. Colubris Networks. 2006. [Viitattu 11.3.2014.] Saatavissa: https://www.google.com/patents/US20060094371
9. Granlund, K. Tietoliikenne. Jyväskylä. WSOYpro/Docendo. 2007.
10. Glas, J. Frequency Hopping. JPL's Wireless Communication Reference Website. 1999. [Viitattu 27.2.2014.] Saatavissa: http://www.wirelesscommunication.nl/reference/chaptr05/spreadsp/fh.htm
11. OSI-malli. Raahen tekniikan ja talouden yksikkö. 2014. [Viitattu 10.2.2014.] Saatavissa: http://www.ratol.fi/opensource/lahiverkot/fin/yleista/osi_malli.htm
12. Colliander, A. ISOn OSI-mallin rakenne ja käyttö. 1999. [Viitattu 10.2.2014.] Saatavissa: http://www.tml.tkk.fi/Studies/Tik-110.300/1999/Essays/essee_OSI.html
13. Tampereen teknillinen yliopisto. OSI-malli. Tampereen teknillinen yliopisto. Tieto- ja sähkötekniikan tiedekunta. Etäopetusmateriaali. 2002. [Viitattu 10.2.2014.] Saatavissa: http://www.cs.tut.fi/etaopetus/titepk/luku19/OSI.html
14. Poole, I. IEEE 802.11n Standard. Radio Electronics. 2014. [Viitattu 13.2.2014.] Saatavissa: http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11n.php
15. Kelly, V. New IEEE 802.11ac™ Specification Driven By Evolving Market Need For Higher, Multi-User Throughput in Wireless LANs. IEEE Standards Association. 2014. [Viitattu 14.2.2014.] Saatavissa: http://standards.ieee.org/news/2014/ieee_802_11ac_ballot.html
16. Banerji, S. On IEEE 802.11: Wireless LAN Technology. RCC-Institute of Information Technology. 2013. [Viitattu 18.2.2014.] Saatavissa: http://arxiv.org/ftp/arxiv/papers/1307/1307.2661.pdf

17. Verkkokauppa.com. Asus PCE-N53 kaksitaajuuksinen N600 PCIe -langaton verkkosovitin. 2014. [Viitattu 19.2.2014.] Saatavissa: http://www.verkkokauppa.com/fi/product/6004/dhhxr/Asus-PCE-N53-kaksitaajuuksinen-N600-PCIe-langaton-verkkosovi#product-q
18. Tietokonekauppa.fi. TP-LINK langaton tukiasema. 2014. [Viitattu 19.2.2014.] Saatavissa: http://www.tietokonekauppa.fi/product/30383/wlan+access+point/TP-LINK/langaton+tukiasema+300Mb/s+80211b+g+n+pass+PoE/
19. Hämäläinen, P. Wlan-kytkimet. Tietokone.fi. 2006. [Viitattu 20.2.2014.] Saatavissa: http://www.tietokone.fi/artikkelit/wlan_kytkimet
20. Arora, M. How secure is AES against brute force attacks? Electronic Engineering Times. 2012. [Viitattu 11.3.2014.] Saatavissa: http://www.eetimes.com/document.asp?doc_id=1279619
21. Cisco Systems. TACACS+ and RADIUS Comparison. Cisco Systems. 2008. [Viitattu 2.4.2014.] Saatavissa: http://www.cisco.com/c/en/us/support/docs/security-vpn/remote-authentication-dial-user-service-radius/13838-10.html
22. Cisco Systems. Cisco Aironet 1240AG Series 802.11A/B/G Access Point Data Sheet. Cisco Systems. 2014. [Viitattu 18.2.2014] Saatavissa: http://www.cisco.com/c/en/us/products/collateral/collaboration-endpoints/unified-ip-phone-7900-series/product_data_sheet0900aecd8031c844.html