TAMPEREEN
AMMATTIKORKEAKOULU

WLAN -mittaukset

Tomi Salonen

Opinnäytetyö
Marraskuu 2016
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka ja tietoverkot

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka ja tietoverkot

TOMI SALONEN:
WLAN-mittaukset

Opinnäytetyö 22 sivua, joista liitteitä 3 sivua
Marraskuu 2016

Opinnäytetyön tarkoituksena oli selvittää ja kokeilla käytännössä, mitä kaikkea WLAN-verkoista pystyy ja kannattaa mitata. Työssä käydään läpi WLAN-verkkojen ominaisuuksien osalta olennaisia teorioita, kuten 802.11-standardien erot toisiinsa ja WLAN-verkkojen tietoturvaprotokollat.

Teorioiden lisäksi työssä käydään läpi mittausohjelmien ominaisuuksia ja perusteellisemmin Site Survey –mittaus. Työssä on esitelty mittausohjelmina Acrylic WiFi Professional WLAN-verkkojen ominaisuuksien mittausta varten ja Site Survey –mittausta varten on käytetty Acrylic WiFi Heatmaps –ohjelmaa.

Asiasanat: WLAN, langaton lähiverkko, mittaukset, 802.11

ABSTRACT

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

TOMI SALONEN:
WLAN Analysis

Bachelor's thesis 22 pages, appendices 3 pages
November 2016

The aim for this thesis was to find out and to try in practice what can and is useful to analyze from a WLAN network using software designed for WLAN analysis. This thesis examines essential WLAN network feature theories, such as differences in 802.11 standards and WLAN network security protocols.

In addition to the theories, the thesis examines features found in WLAN analysis software and goes through how to perform a site survey analysis. The analysis software used in this thesis are Acrylic WiFi Professional for WLAN features and Acrylic WiFi Heatmaps for the site survey.

Key words: WLAN, wireless local area network, analysis, 802.11

SISÄLLYS

LYHENTEET JA TERMIT

AAD	Additional Authentication Data, ylimääräinen todennusdata
AES	Advanced Encryption Standard, lohkosalausmenetelmä
Airpcap	Pakettien monitorointiohjelma langattomissa verkoissa
CCMP	Counter Mode Cipher Block Chaining Message Authentication Code Protocol, salausprotokolla
CRC	Cyclic Redundancy Check, tiivistealgoritmi
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance, siirtotien varausmenetelmä
DSSS	Direct Sequence Spread Spectrum, suorasekventointi
EIRP	Effective Isotropic Radiated Power, suunnattu radiosignaali
FHSS	Frequency Hopping Spread Spectrum, taajuushyppely
IEEE	Institute of Electrical and Electronics Engineers, järjestö, joka mm. määrittelee standardeja
ISM	Industrial, Scientific and Medical radio, joukko radiotaajuuksia
MIC	Message Integrity Code, tekniikka, jolla varmistetaan että lähetettyä dataa ei ole muokattu
MPDU	MAC Protocol Data Unit, MAC-kerrokson datayksikkö
OSI-malli	Open Systems Interconnection Reference Model, kuvaa tiedonsiirtoprotokollien yhdistelmän seitsemässä kerroksessa
PN	Packet Number, data-paketin järjestysnumero
PSK	Pre Shared Key, ennalta määritetty avain, WLAN salasana
RADIUS	Remote Authentication Dial-In User Service, käyttäjäntodennusprotokolla
RC4	Rivest Cipher 4, salausalgoritmi
RF	Radio Frequency, radiotaajuus
Solmu	Verkkolaite, joka prosessoi dataa
SSID	Service Set Identifier, WLAN-verkon tunniste
TKIP	Temporal Key Integrity Protocol, tietoturvaprotokolla
WEP	Wired Ethernet Privacy, suojausalgoritmi
Wireshark	Verkkodatapakettien monitorointiohjelma
WLAN	Wireless Local Area Network, langaton lähiverkko
WPA	Wi-Fi Protected Access, salausprotokolla

1 JOHDANTO

WLAN-tekniikoiden kehittyessä ja yhä useamman laitteen ollessa WiFi –yhteensopiva tarve laajemmille ja paremmille WLAN-verkoille kasvaa. Teknologian levitessä tulee myös vikatiloja esiintymään suurentuvassa määrin ja sen takia on hyvä pystyä analysoimaan sellaiset ja välttämään ne jo ennalta.

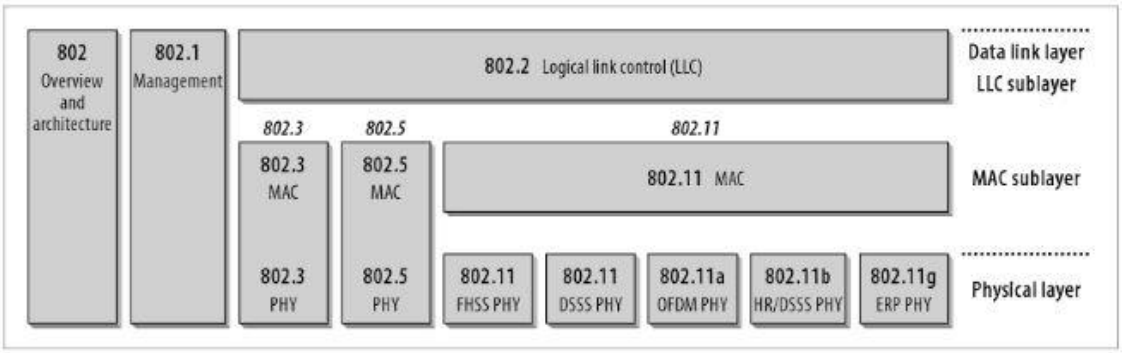
Tämän opinnäytetyön tarkoituksena on selvittää WLAN-verkkojen mittausten kannalta olennaiset perusteet ja tutustua joihinkin WLAN-verkkojen mittauksiin. Työssä käydään läpi ensin teoriat aiheista, jotka voivat tulla vastaan WLAN-verkkoja mitatessa ja sen jälkeen esitellään mittausohjelmien ominaisuuksia, tärkeitä mittauksia WLAN-verkoista sekä esitellään esimerkkimittaustuloksia kuuluvuuskartoituksesta.

2 WLAN-STANDARDIT

WLAN, eli langaton lähiverkko, on tekniikka, jolla yhdistetään kaksi tai useampi laite langattomasti toisiinsa. WLAN-tekniikalle on vuosien varrella kehitetty useita standardeja, mutta vallitsevaksi näistä on noussut IEEE:n kehittämä 802.11-standardi. WLAN-sanan sijaan käytetään yleisesti myös Wi-Fi –sanaa. Wi-Fi ei kuitenkaan ole synonyymi WLAN:ille vaan se on Wi-Fi Alliancen rekisteröity tavaramerkki, joka tarkoittaa WLAN-tuotetta, joka toimii 802.11 –standardeilla. Wi-Fi -sertifikaatti auttaa kuluttajia tunnistamaan monilta eri valmistajilta WLAN-laitteet, jotka ovat yhteensopivia keskenään.

2.1 802.11-standardi

WLAN-verkoissa on yleiseen käyttöön vakiintunut IEEE:n 802.11 –standardi, joka määrittelee OSI-mallin kaksi alinta kerrosta eli siirtokerroksen sekä fyysisen kerroksen langattomien lähiverkkojen toteuttamiseen. Alkuperäinen 802.11 –standardi julkaistiin vuonna 1997 ja parannettu versio vuonna 1999. (Geier 2000, 118) Kuvassa 1 on esitetty 802.11-standardin sijoittuminen OSI-malliin.



KUVA 1. IEEE 802-standardiperheen sijoittuminen OSI-malliin (Gast 2005)

Alkuperäinen 802.11-standardi määritteli kolme fyysisen kerroksen siirtomenetelmää: infrapunamenetelmän, joka toimii 1 Mbit/s nopeudella, FHSS (taajuushyppely) -menetelmän, joka toimii 1 ja 2 Mbit/s nopeudella ja DSSS (suorasekvenssi) -menetelmän, joka toimii 1 ja 2 Mbit/s nopeudella (Varshney 2003). FHSS- ja DSSS -menetelmät ovat RF (radio frequency) -menetelmiä, jotka toimivat 2,4 GHz:n ISM (Industrial Scientific Medical) taajuudella 5 MHz kanavavälein (Granlund 2007, 293-294).

802.11 -standardiperheenseen on myöhemmin julkaistu monia lisästandardeja, jotka voi tunnistaa niiden perään lisätyistä kirjaimista.

TAULUKKO 1. 802.11-Standardiperhe

Standardi	Toimintataajuus	Julkaisuvuosi
802.11	2,4 GHz	1997
802.11b	2,4 GHz	1999
802.11a	5 GHz	1999
802.11g	2,4 GHz	2003
802.11n	2,4 GHz ja 5 GHz	2009
802.11ac	5 GHz	2013
802.11ad	60 GHz	2012

2.1.1 FHSS-tekniikka

Taajuushyppelyhajaspektri on tekniikka, jossa datasignaalia moduloidaan kantoaallolla, joka hyppii eri taajuuksien välillä. 802.11-standardissa kantoaallon taajuus vaihtelee 2,4 GHz ja 2,483 GHz välisellä alueella. Signaali pysähtyy määritetyn mittaiseksi hetkeksi jokaisella taajuudella lähettämään dataa ja siirtyy sitten toiselle taajuudelle. FHSS kestää paremmin signaalihäiriöitä kuin DSSS, mutta se pystyy ainoastaan 2 Mbit/s tiedonsiirtonopeuteen ja toimii lyhyemmällä välimatkalla. (Geier 2000, 3)

2.1.2 DSSS-tekniikka

Suorasekvenssihajaspektrissä lähetettävään datasignaaliin yhdistetään korkeamman tiedonsiirtonopeuden omaava bittijono. 802.11-standardissa yhdistetty bittijono muuntaa lähetetyn signaalin bittimäärän vähintään 11-kertaiseksi alkuperäiseen datasignaaliin nähden. DSSS pystyy toimimaan FHSS:tä pidemmillä välimatkoilla johtuen sen pienemmästä signaali-kohinasuhteen tarpeesta, joka on DSSS:lle 12 dB ja FHSS:lle 18 dB. (Geier 2000, 4)

2.2 802.11b-standardi

Vuonna 1999 hyväksytty 802.11b-standardi oli ensimmäinen suuren suosion saavuttanut WLAN-standardi. 802.11b paransi enimmäistiedonsiirtonopeuden vanhasta 2 Mbit/s maksimissaan 11 Mbit/s. 802.11b käyttää tiedonsiirtoon CSMA/CA –tekniikkaa, joka oli määritelty jo alkuperäisessä 802.11-standardissa. CSMA/CS-tekniikka toimii siten, että kun solmu haluaa suorittaa datansiirron, se kuuntelee löytääkseen vapaan kanavan ja suorittaa sen jälkeen siirron. Solmu odottaa sen jälkeen vahvistusviestiä ja, jos ei saa sellaista, solmu odottaa satunnaisen ajan ja yrittää suorittaa siirron uudelleen. (Poole 2010)

802.11b-standardi käyttää myös ARS (adaptive rate selection) -järjestelmää signaalin laadun takaamiseksi: jos signaalin taso laskee tai interferenssi nousee, systeemin on mahdollista pudottaa datansiirtonopeutta 11 Mbit/s:sta ensin 5,5 Mbit/s:een ja vielä uudelleen 2 tai 1 Mbit/s:een. Todellisuudessa 802.11b ei pysty saavuttamaan 11 Mbit/s enimmäistiedonsiirtonopeuttaan, vaan TCP-protokollaa käytettäessä todellinen maksimi nopeus on 5,9 Mbit/s, johtuen protokollan toiminnasta ja CSMA/CA-tekniikan odotusjaksoista. UDP-protokollaa käytettäessä on todellinen maksimi tiedonsiirtonopeus 7,1 Mbit/s luokkaa. (Poole 2010)

2.3 820.11a-standardi

Vuonna 1999 julkaistiin 802.11b:n lisäksi myös 802.11a-standardi, joka toimii 5 GHz taajuudella ja jonka maksimi tiedonsiirtonopeus on 54 Mbit/s, mutta käytännössä päästään noin puoleen maksimista. Huolimatta sen paremmasta tiedonsiirtonopeudesta ja vähemmän häiriötekijöitä sisältävästä taajuudesta, se ei noussut korkeammasta hinnastaan johtuen yhtä suosituksi kuin 802.11b. (Poole 2010)

Nopeamman 54 Mbit/s tiedonsiirtonopeuden mahdollisti OFDM-modulaation käyttö. 802.11a:ssa käytetyssä OFDM-signaalissa on 52 alikantoaaltoa, joista 48 käytetään tiedonsiirtoon ja 4 pilotti aaltoina. 12 alikantoaaltoa jää tyhjäksi varokaistaksi viereisiä kaistoja varten. Interferenssi eri alikantoaaltojen välillä estetään asettamalla ne suorakulmaisesti toisiinsa nähden. (Poole 2010)

2.4 802.11g-standardi

Vuonna 2003 julkaistiin uusi 802.11g-standardi. Sen tarkoituksena oli yhdistää 802.11a:n korkea tiedonsiirtonopeus ja 802.11b:n käyttämät halvemmat 2,4 GHz:in taajuudella toimivat sirut. Jo ennen 802.11g-standardin virallista hyväksymistä oli markkinoilla saatavissa sen mukaisia tuotteita. Uusi standardi tarjosi 54 Mbit/s enimmäistiedonsiirtonopeuden, jonka suoritusteho on tosin vain noin 24 Mbit/s. 802.11g käyttää 802.11a:n tavoin OFDM-modulaatiota yhdessä suorasekvenssitekniikan kanssa. (Poole 2010). 802.11g:n etuna on sen yhteensopivuus 802.11b-standardin kanssa, mikä helpotti yrityksien, joilla oli jo käytössä 802.11b-verkko, siirtymistä uuteen standardiin. 802.11b:tä käyttävät laitteet 802.11g–ympäristössä rajoittavat kuitenkin kokonaissuorituskykyä. (Geier 2000, 127)

2.5 802.11n-standardi

2004 vuonna IEEE ilmoitti perustaneensa uuden komitean kehittämään uutta suurinopeuksista 802.11n-standardia. Uusi standardi saatiin valmiiksi 2009 ja ominaisuudet oli paljastettu jo 2006, jolloin laitevalmistajat pystyivät aloittamaan suunnittelun ja kehityksen. (Poole 2010)

802.11g toimii sekä 2,4 GHz:in taajuudella, että 5 GHz:in taajuudella 20 tai 40 MHz:in kanavanleveydellä ja paljon edeltäjiään nopeammalla 600 Mbit/s tiedonsiirtonopeudella. 802.11n on taaksepäin yhteensopiva kaikkien aikaisempien 802.11-standardien kanssa. (Poole 2010). Saavuttaakseen paremman tiedonsiirtonopeuden 802.11n käyttää MIMO-teknologiaa. MIMO-teknologiassa käytetään useita lähetin- ja vastaanottoantenneja, jotta saadaan korkeampi tiedonsiirtonopeus. MIMO-teknologia hyödyntää myös monitie-etenemisilmiötä hyväkseen nostaakseen suorituskykyä ja etäisyyttä. (Intel 2016)

2.6 802.11ac-standardi

802.11ac-standardi parantaa edelleen 802.11-standardien tiedonsiirtonopeutta. 802.11ac käyttää lisensoimatonta 5,8 GHz:in ISM-taajuutta ja sen maksimi teoreettinen tiedonsiirtonopeus, kun kaikki ominaisuudet ovat käytössä on jopa 7 Gbit/s. 802.11ac

käyttää aikaisemmissa 802.11-standardeissa hyväksi todettuja tekniikoita, kuten OFDM, ja kehittää toisia, kuten MIMO, josta on nyt käytössä MU (multi-user) MIMO. 802.11ac pystyy myös käyttämään aikaisempia suurempia 80 ja 160 MHz:in kaistanleveyksiä. (Poole 2010)

2.7 802.11ad-standardi

Uusin markkinoille tuloa tekevä 802.11-standardi on vuonna 2012 julkaistu 802.11ad. Aikaisemmista versioista poiketen 802.11ad toimii 2,4 tai 5 GHz:in sijaan 60 GHz:in taajuudella ja sen kantama on tästä syystä vain muutamia metrejä. 60 GHz:in taajuus kuitenkin takaa tarpeeksi korkeat kaistanleveydet ja interferenssitason, jotta päästäisiin haluttuihin 7 Gbit/s:in suoritustehoihin. 802.11ad on suunnattu paljon dataa vaativille tiedonsiirroille, kuten 4K- ja 3D-elokuvien katsomiseen WLAN:in välityksellä. (Poole 2010)

2.8 U-NII-kaistat

5 GHz –taajuusalueella 802.11-standardit käyttävät U-NII –radiotaajuuskaistaa. U-NII jakautuu eri tasoille 5,15 – 5,85 GHz:in välille. U-NII 1 sijoittuu 5,150-5,250 GHz:in taajuusalueelle. Tehorajat U-NII 1:lle ovat 250 mW client-laitteelle ja 1 W master-laitteelle tai EIRP:iä, jossa signaali keskitetään yhteen suuntaan, käytettäessä 1 W client-laitteelle ja 4 W master-laitteelle tai 200 W point-to-point yhteydelle. (Nguyen 2014)

U-NII 2A toimii 5,250-5,350 GHz:in alueella ja U-NII 2C 5,470-5,725 GHz:in alueella. Niiden tehon enimmäisrajat ovat 250 mW tai EIRP käytettäessä 1 W. U-NII 2A- ja 2C-alueen kanavilla tulee käyttää dynaamista kaistan valintaa (DFS). (Nguyen 2014)

U-NII 3 toimii 5,725-5,850 GHz:in taajuusalueella. U-NII 3 alueella enimmäisteho on 1 W tai 4 W EIRP käytettäessä. Point-to-point EIRP käytettäessä ei ole enimmäistehorajaa. (Nguyen 2014)

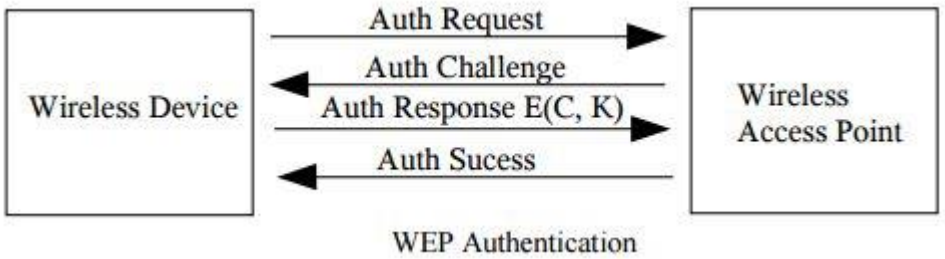
3 WLAN JA TIETOTURVA

WLAN-yhteyksien käyttö ei olisi kovin mielekästä, jos tiedonsiirto toteutettaisiin ilman suojausta ja datapaketit voisi kaapata radioaalloilta. Tietoturvan takaamiseksi on 802.11-standardeihin kehitetty erinäisiä suojausmetodeja kryptaamaan siirrettyä dataa.

3.1 WEP-salaustekniikka

Alkuperäisen 802.11-standardin osana 1997 vuonna määriteltiin sekä 64-bittinen WEP, että 128-bittinen WEP. WEP (Wired Equivalent Privacy) on MAC-tasolla tapahtuva kryptaus, joka suojaa datakehyksen MSDU hyötykuorman. WEP:n tarkoituksena on parantaa luottamuksellisuutta, kulunvalvontaa ja datan eheyttä. (Coleman, Westcott, Harkins & Jackman 2010, 38)

WEP-suojausta käyttävään verkkoon liittyessään päätelaite joutuu käymään läpi todennusprosessin (kuva 2), joka estää laitteita, jotka eivät tiedä WEP-avainta, liittymästä WEP-suojattuun verkkoon. Päätelaite lähettää todennuspyynnön tukiasemalle, joka vastaa pyyntöön 128-bittisellä haasteella. Päätelaite allekirjoittaa haasteen yhteisellä salausavaimella ja lähettää sen takaisin tukiasemalle, joka purkaa haasteviestin yhteisellä salausavaimella ja tarkistaa sen todenmukaisuuden. Todennuksen jälkeen salausavaimia ei enää käytetä, joten WEP suojaus on haavoittuvainen ”mies välissä”-hyökkäyksille. (Shivaputrappa 2005, 2)



KUVA 2. WEP-todennus (Shivaputrappa 2005)

Tiedonsiirron salaamiseksi päätelaitteen ja tukiaseman välillä WEP käyttää RC4-vuosalausta. 24-bittinen satunnaisen alustusvektorin (IV, initialization vector) ja salausavaimen avulla RC4 generoi avainjonon, joka yhdistetään XOR-operaattorilla hyötykuormaan ja CRC-kehystarkistussummaan. Saatuun kryptattuun viestiin

yhdistetään vielä käytetty alustusvektori ja se lähetetään eteenpäin ilmateitse. (Shivaputrappa 2005, 4)

3.2 WPA- ja WPA 2-salaustekniikat

Vuonna 2003 esitelty WPA (Wi-Fi Protected Access) kehitettiin korvaamaan WEP ja korjaamaan siinä todetut ongelmat. WPA:n avuksi kehitettiin TKIP (Temporal Key Integrity Protocol) -kryptausalgoritmi. WPA:sta on kaksi eri versiota: pienkäyttäjille tarkoitettu WPA Personal sekä suurille yrityksille suunnattu WPA Enterprise. Erona versioiden välillä on käytetty todennusmetodi; Personal käyttää PSK (pre-shared key) -todennusta ja Enterprise käyttää RADIUS-pohjaista todennusta. (Wi-Fi Alliance 2003)

WPA2 on jatkokehitetty WPA-luokituksesta. WPA2 tukee WPA:sta TKIP-kryptausta, EAP-todennusta sekä PSK-teknologiaa. Näiden lisäksi WPA2 tarjoaa uuden AES (Advanced Encryption Standard) -kryptauksen. (Wi-Fi Alliance 2003)

3.2.1 TKIP-salaustekniikka

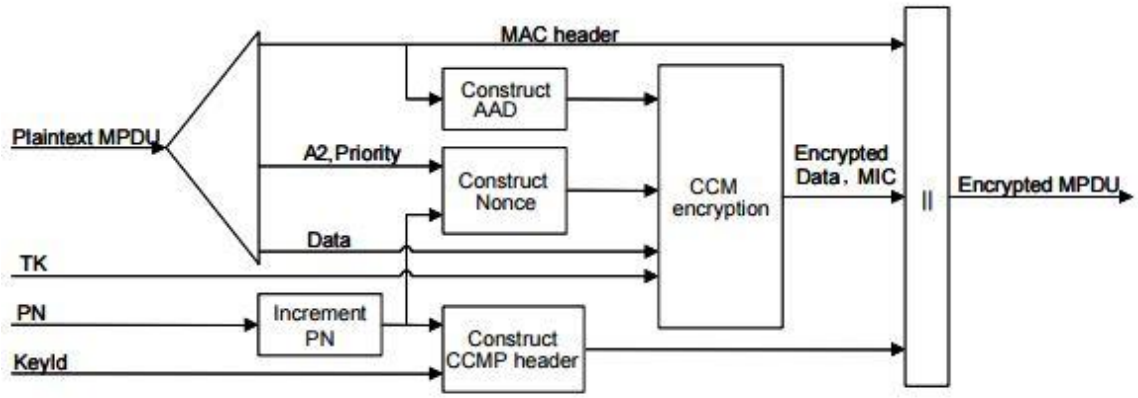
Temporal Key Integrity Protocol on salausprotokolla, joka kehitettiin paikkaamaan WEP-salauksen tietoturva-aukot. TKIP käyttää edelleen samaa RC4-jonosalausta kuin WEP, mutta käyttää sen yhteydessä vahvempia ominaisuuksia. Siinä missä WEP käyttää 40-bittistä salausavainta, TKIP parantaa tietoturvaa käyttämällä pidempää 128-bitin salausavainta, joka generoidaan kehyskohtaisesti, jolloin saadaan poistettua ongelmat liittyen avainten uudelleenkäyttöön. Myös alustusvektorin pituutta on nostettu entisestä 24-bitistä 48-bittiin. TKIP käyttää myös vahvaa MIC-eheydentarkistusta. MIC tunnistaa sanomien väärennysyritykset, kuten kohde- ja lähdeosoitteiden muutokset sekä bittien järjestyksen muuttumisen (bit flipping). (Puska 2005, 82)

TKIP-salaus suoritetaan ensin yhdistämällä yhteinen 128-bittinen väliaikainen avain päätelaitteen MAC-osoitteeseen sekä neljään eniten merkitsevään bittiin kehyksen järjestysnumerossa. Täten saatu avain ja järjestysnumeron kaksi alinta bittiä yhdistetään vielä keskenään, jolloin saadaan kehyskohtainen avain. MAC-osoitetta hyödynnettäessä jokainen asema käyttää uniikkia avainta, joka vielä vaihtuu jokaisen lähetetyn kehyksen

kohdalla. Jotta salauksesta saataisiin vielä varmempi, vaihdetaan salauksessa käytettävä 128-bittinen salausavain dynaamisesti joka 10 000 kehyksen välein. (Puska 2005, 82)

3.2.2 CCMP-salaustekniikka

CCMP on salaustekniikka jota voidaan käyttää WPA 2:ssa. CCMP on AES-krypausalgoritmin CCM-moodiin perustuva salaustekniikka. CCMP:n yhteydessä käytetty AES-prosessointi käyttää 128-bittistä avainta ja 128-bitin lohkokokoa. CCM-moodi käyttää uutta väliaikaista avainta jokaisessa sessiossa. Jokainen lähetetty kehys vaatii uniikin tunnistenumeron, jonka luontiin käytetään 48-bittistä paketin numeroa (PN). (IEEE 2007, 180)



KUVA 3. CCMP-kryptauksen lohkodiagrammi (lEEE 2007)

CCMP-kapseloinnissa luodaan ilmateitse lähetettävä datayksikkö yhdistämällä MAC-tunniste, CCMP-tunniste, kryptattu data ja MIC-eheydentarkistuskoodi. Alkuperäinen datayksikkö suurenee 16 oktetilla, näistä 8 oktettia on CCMP-tunnistetta ja toiset 8 oktettia MIC-eheydentarkistuskoodia. Kryptaus datalle saadaan yhdistämällä siihen väliaikainen avain ja paketin numeron avulla luotu uniikki tunniste. Kuvassa 3 on lohkodiagrammin avulla mallinnettu lähetettävän paketin kryptaus CCMP-tekniikalla. CCMP:n turvallisuus perustuu siihen, että yhden väliaikaisen avaimen kanssa ei koskaan käytetä samaa paketin numeroa yhtä kertaa enempää. (lEEE 2007, 181)

4 WLAN-MITTAUKSET

Langattomia verkkoja rakennettaessa ja ylläpidettäessä on tärkeää olla selvillä niiden ominaisuuksista ja toiminnasta. Usein helpoiten tähän tavoitteeseen päästään mittaamalla erinäisillä ohjelmilla WLAN-verkon toimintaa. WLAN-verkkojen mittaamiseen löytyy lukuisia ohjelmia, eikä yleensä yhdestä ohjelmasta löydy kaikkia mahdollisia ominaisuuksia.

4.1 WLAN-mittausohjelmat

WLAN-verkosta on nykyisin saatavilla olevilla ohjelmilla helppo mitata niiden ominaisuudet. Verkon ominaisuuksia mitatessa on tärkeä tietää WLAN-verkon käyttötarkoitus, jotta voidaan mittaustuloksia analysoida tarpeen mukaan. Kotiverkon, pienyritysverkon ja esimerkiksi suuren oppilaitoksen WLAN-verkkoilta odotetaan eri rajoitteita, jotka ovat mittaustulosten analysoinnin kannalta olennaisia.

Suurimmassa osassa WLAN-mittausohjelmia on samanlaiset perusominaisuudet. Ohjelmilla saa yleensä selville WLAN-verkossa käytettävän 802.11-standardin, verkon SSID-tunnisteen tai tiedon sen piilotuksesta, MAC-osoitteen, signaalin tehon mittauspisteessä, signaalin käyttämän kanavan, laitteen valmistajan ja tiedon siitä, mitä suojaustekniikkaa käytetään. Perusominaisuuksiin kuuluu yleensä myös graafinen esitys eri WLAN-verkkojen käyttämien kanavien päällekäisyydestä. Monipuolisemmista ohjelmista kuten Acrylic WiFi Professional (liite 1.) voi myös löytyä sisäänrakennettu tuki pakettien kaappaus –ohjelmille kuten Wireshark tai Airpcap.

4.2 WLAN-mittaustulosten analysointi

WLAN-verkkoa mittamaalla saadaan helposti selville, mitä OSI-mallin fyysisen kerroksen 802.11-standardia verkko käyttää. 802.11-standardit ovat vanhempien ja samalla taajuudella toimivien 802.11-standardien kanssa takaperin yhteensopivia, mutta standardit sisältävät eri yhteensopivuustiloja, jotka voivat aiheuttaa ongelmia päätelaitteiden kanssa. Mittaamalla nähdään, mitä kaikkia 802.11-standardeja mikäkin verkko tukee.

Varsinkin uudemmat 802.11-standardit voivat toimia useilla eri tiedonsiirtonopeuksilla riippuen siitä montako lähetin- ja vastaanottoantennia on käytössä (MIMO). Mittausohjelmilla voidaan nähdä signaalin enimmäistiedonsiirtonopeus esimerkiksi tietämättä käytettävien laitteiden fyysisiä ominaisuuksia.

WLAN-verkossa käytössä oleva salaustekniikka on tietoturvan kannalta olennainen ja mitattavissa helposti. Koti- ja pienyrityskäytössä WPA2-PSK AES-pohjaisella CCMP-suojauksella on paras WLAN-verkon suojausmetodi. Suurempien yritysten ja laitosten käytössä olevat WLAN-verkot tulisi suojata WPA2-Enterprise:n avulla, jolloin lisäsuojauksena käytetään erillistä palvelimelle kirjautumista eikä kaikille käyttäjille tiedossa olevaa salasanaa (PSK).

WLAN-verkoille on käytössä melko pieni määrä kanavia varsinkin 2,4 GHz:ia käyttävillä 802.11-standardeilla. Päällekkäin osuvat WLAN-verkot voivat aiheuttaa häiriöitä toisilleen ja heikentää signaalin laatua. Mittaamalla on helppo selvittää verkkojen päällekkäisyydet ja asettaa oma verkko kuulumaan kanavalla, jolla on vähiten häiriötä.

4.3 Site Survey -kartoitus

Site Survey –kartoitus on suurenpien WLAN-verkkojen kannalta erittäin tärkeä mittausmenetelmä. Site Survey –kartoitus sisältää yleensä WLAN-verkon kuuluvuuskartoituksen ja RF-spektri –kartoituksen. Jo valmiille WLAN-verkolle voidaan suorittaa kuuluvuuskartoitus, jolloin saadaan selville verkon kuuluvuus ja mahdolliset katvealueet. Site survey:llä voidaan kartoittaa myös naapuriverkkojen kuuluvuus alueella, jonne ollaan asentamassa uutta WLAN-verkkoa, jolloin voidaan paremmin suunnitella WLAN-tukiasemien asennuspaikat.

Site Survey –kartoitusta varten löytyy markkinoilta monia ohjelmia, kuten Acrylic WiFi, NetSpot ja Ekahau. Site Survey –ohjelmalle syötetään aluksi pohjapiirros mitattavasta alueesta, jonka mittakaava sitten joko kalibroidaan manuaalisesti tai GPS-paikannuksen avulla. Mittaaja kartoittaa mitattavan alueen kulkemalla alueella mittalaitteiden kanssa samalla mitaten useita pisteitä alueelta ja merkiten ohjelmaan kuljetun reitin.

Liitteissä 2 ja 3 on Acrylic Wifi Heatmaps –ohjelman kokeiluversiolla suoritettu kuuluvuuskartoitus omakotitalon alakerrassa. Kartoitus on suoritettu 2,4 GHz:n 802.11n-verkolle (liite 2) ja 5 GHz 802.11ac-verkolle (liite 3). Kartoituksessa lähestyttäessä punaista väriä on kuuluvuus parempi ja lähestyttäessä mustaa on kuuluvuus huonompi, värittömässä kohdassa kartalla kuuluvuus ei ylitä asetettua -80 dBm:n rajaa. Liitteissä 2 ja 3 näkyy myös enimmäiskuuluvuus dBm:nä ”Plot options”:in alla. Pääteasema sijaitsee omakotitalon toisessa kerroksessa lähestulkoon kohdassa, johon kartoitus –ohjelma on sen arvannut (liite 3). Liitteistä 2 ja 3 nähdään selvästi, että 2,4 GHz:in signaali läpäisee rakennuksen seinät ja lattian paremmin kuin 5 GHz:n signaali. Liitteessä 3 on myös nähtävillä pisteet, joista verkot on mitattu.

Jos WLAN-verkon alueella on paljon mahdollisesti häiriöitä aiheuttavia laitteita on alueella hyvä myös suorittaa RF-spektri –kartoitus. RF-spektrin mittaamista ei voi suorittaa pelkällä WLAN-antennilla vaan sitä varten tarvitaan erillistä laitteistoa, jolla voidaan mitata RF-spektriä. Erityisesti 2,4 GHz:in taajuusalueella voi esiintyä paljon häiriöitä, koska se sijoittuu ISM-taajuuksille, jotka on tarkoitettu teollisille-, tieteellisille- ja lääketieteellisille laitteille, jotka aiheuttavat RF-säteilyä.

5 POHDINTA

Opinnäytetyössä oli tarkoituksena perehtyä WLAN-verkkojen mittaamiseen ja selvittää mitä kaikkea niistä voi mitata ja miksi. Työn teon edetessä ymmärrystä WLAN-standardeihin liittyvistä asioista karttui laajalti. Työtä tehtäessä tultiin siihen tulokseen, että WLAN-verkoista ei loppujen lopuksi löydy paljoa asioita, joita siitä voisi tai kannattaisi mitata Site Survey –kartoituksen ja kanavien päällekkäisyyden lisäksi. Mahdollisesti tukiasemien, joita on vaikeampi konfiguroida, verkkoja on myös kätevämpi mitata vikatilanteen sattuessa.

Mittausten suorittaminen on työssä jäänyt jokseenkin puutteelliseksi johtuen osittain budjetista. Paremmat mittausohjelmat ovat kaikki maksullisia ja niistä saatavat kokeiluversiot osoittautuivat paikoitellen puutteellisiksi. RF-spektri –mittauksia ei voitu työssä suorittaa ollenkaan, koska saatavilla ei ollut mittauksiin tarvittavia laitteita. Mittauksia olisi voinut myös suorittaa suuremmilla ja suurempikapasiteettisilla WLAN-verkoilla.

Yhdeksi suurimmista haasteista opinnäytetyö tehtäessä osoittautui luotettavien lähteiden löytäminen. Suurin osa teoriasta on pysynyt yli vuosikymmenen muuttumattomana ja on vakiintunut asioiksi, jotka vain tiedetään. Alkuperäisiä IEEE:n julkaisemia monituhatsivuisia standardeja on erittäin työlästä kahlata läpi jonkin tietyn informaationpalasen perässä.

LÄHTEET

Coleman, D., Westcott, D., Harkins, B & Jackman, S. 2010. Certified Wireless Security Professional Official Study Guide. Indianapolis: Wiley Publishing, Inc.

Gast, M. 2005. 802.11 Wireless networks the definitive guide. 2. painos. Sebastopol, USA: O'Reilly Media, Inc.

Geier, J. 2000. IEEE 802.11 Standard Overview. Julkaistu 29.11.2000. Luettu 13.11.2016. http://www.informit.com/articles/article.aspx?p=19825

Granlund, K. 2007. Tietoliikenne. 1. painos. Jyväskylä: Docendo.

IEEE. 2007. IEEE Std 802.11-2007. Julkaistu 12.06.2007. Luettu 21.11.2016. http://standards.ieee.org/getieee802/download/802.11-2007.pdf

Intel. Learn about Multiple-Input Multiple-Output (MIMO). Muokattu 15.7.2016. Luettu 11.11.2016. http://www.intel.com/content/www/us/en/support/network-and-i-o/wireless-networking/000005714.html

Nguyen, T. 2014. New Rules for Unlicensed National Information Infrastructure (U-NII) Bands KDB 789033, KDB 644545. Julkaistu 22.10.2014. Luettu 13.11.2016. https://transition.fcc.gov/bureaus/oet/ea/presentations/files/oct14/51-New-Rules-for-UNII-Bands,-Oct-2014-TN.pdf

Poole, I. 2010. IEEE 802.11 standards tutorial. Luettu 10.11.2016. http://www.radio-electronics.com/info/wireless/wi-fi/ieee-802-11-standards-tutorial.php

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

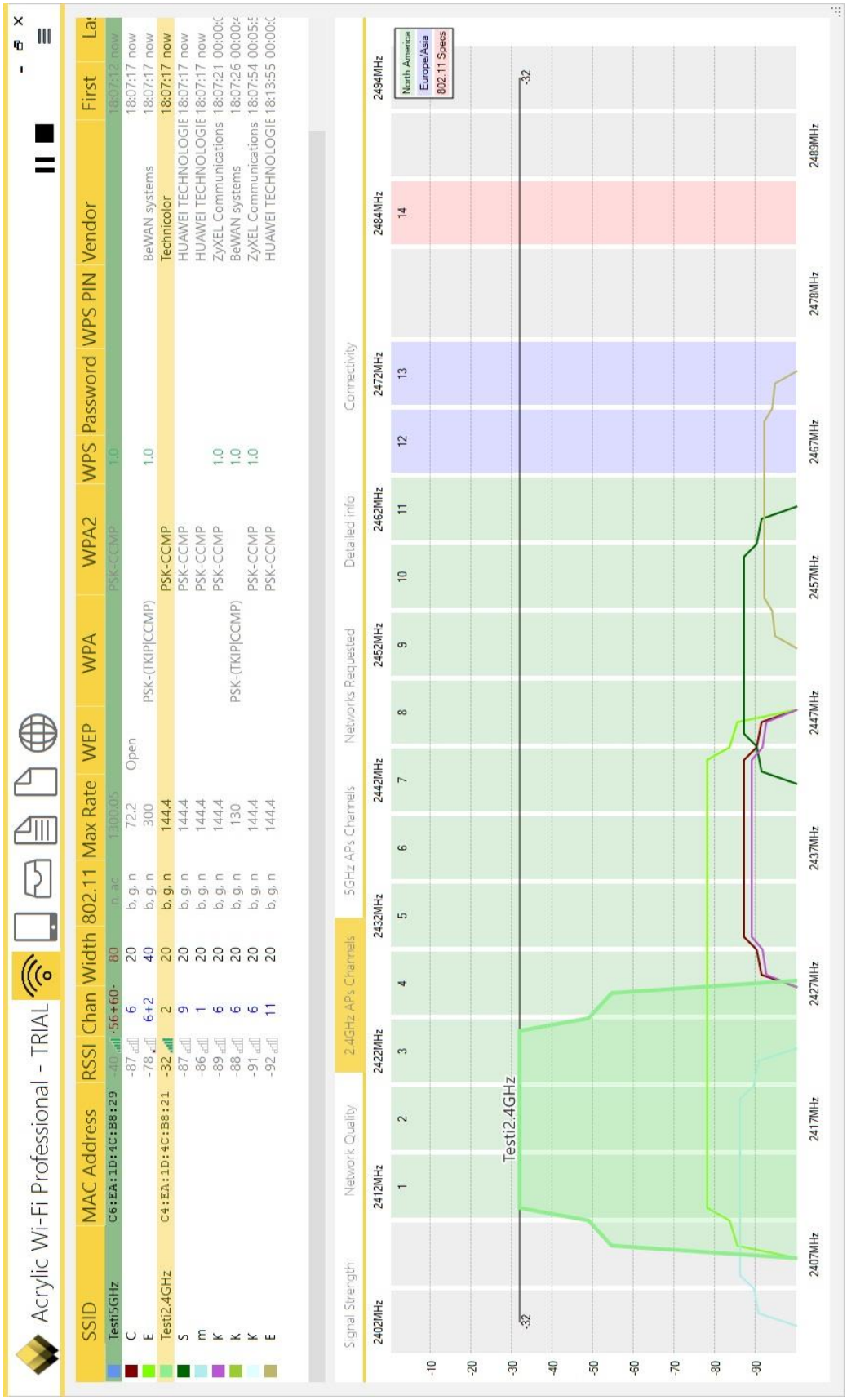
Shivaputrappa, V. 2005. IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability. Julkaistu 2005. Luettu 13.11.2016. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5189832

Varshney, U. 2003. The Status and Future of 802.11-Based WLANs. Julkaistu 11.06.2003. Luettu 20.11.2016. http://paginadellatecnica.xoom.it/The%20Status%20and%20Future%20of%20802.11-Based%20WLANs.pdf

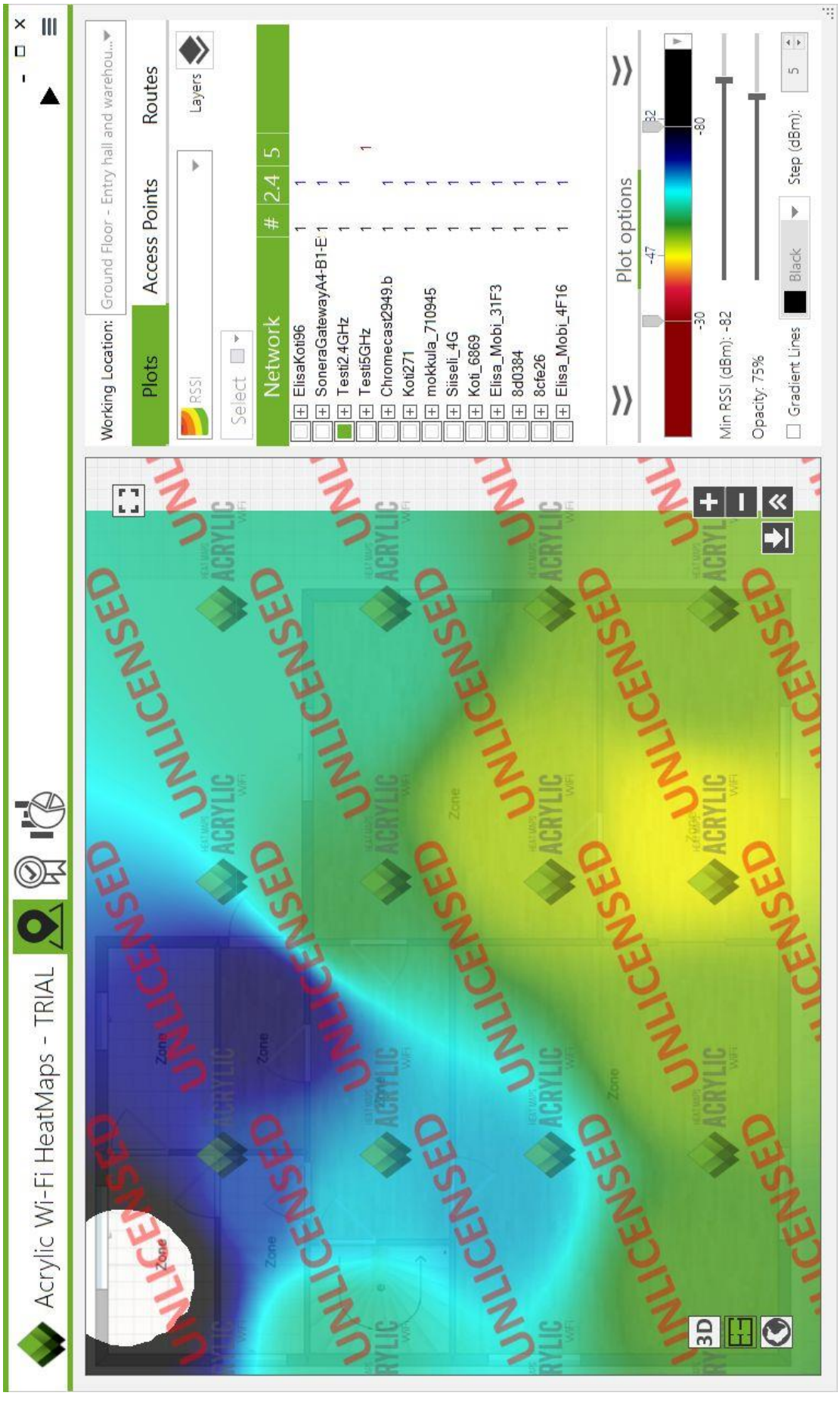
Wi-Fi Alliance. 2003. Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks. Julkaistu 29.04.2003. Luettu 13.11.2016. http://www.ans-vb.com/Docs/Whitepaper_Wi-Fi_Security4-29-03.pdf

LIITTEET

Liite 1. Testi2.4GHz-verkon ominaisuudet Acrylic WiFi Professional –ohjelmalla mitattuna



Liite 2. Testi2.4GHz-verkon kuuluvuuskartoitus Acrylic WiFi Heatmaps -ohjelmalla



Liite 3. Testi5GHz-verkon kuuluvuuskartoitus Acrylic WiFi Heatmaps -ohjelmalla