Lappeenrannan teknillinen korkeakoulu
Tietotekniikan osasto
Tietoliikennetekniikan laitos
28.4.2002
010628000 Suojatut tietoyhteydet

Seminaarityö:

Langattomien lähiverkkojen tietoturva

Sami Seppänen 0067071
Tite N

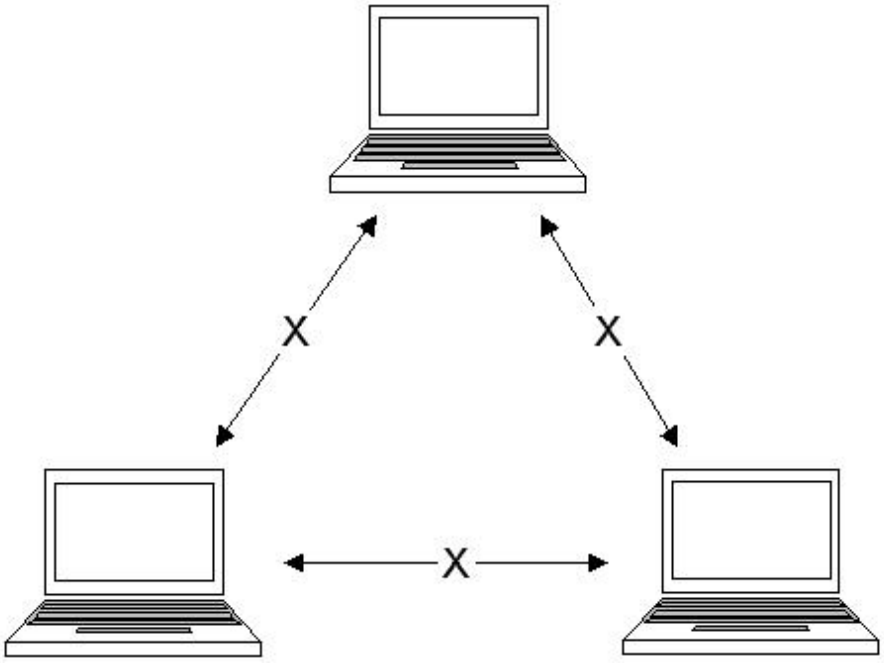
1 Langattoman lähiverkon perusteet

Lähiverkko (Local Area Network, LAN) yhdistää tietokonelaitteita ja mahdollistaa niiden välisen kommunikoinnin. Yleensä lähiverkko toimii pienellä maantieteellisellä alueella ja kattaa yhden rakennuksen tai organisaation. Lähiverkko ja siihen yhdistetyt laitteet ovat usein yhden organisaation omistuksessa. Lähiverkkojen sisäiset siirtonopeudet ovat yleensä huomattavasti suurempia kuin laajemmalla alueella toimivien verkkojen. [Sta97b]

Perinteisessä lähiverkossa laitteiden yhdistäminen tapahtuu kaapeloinnilla. Langattomassa lähiverkossa (Wireless LAN, WLAN), kuten nimikin jo kertoo, kaapelointi on korvattu langattomilla yhteyksillä. Joustavuuden ja liikkuvuuden ansiosta langattomat lähiverkot ovat houkuttelevia vaihtoehtoja langalliselle verkolle. Niitä voidaan käyttää laajentamaan perinteisiä verkkoja ja niillä on helppo kattaa paikkoja, joiden kaapeloiminen on hankalaa (esim. aukeat tehdashallit). Langattomien lähiverkkojen suosio on viime vuosina kasvanut rajusti sen ansiosta, että markkinoille on saatu standardoituja laitteita, joiden tiedonsiirtonopeus alkaa olemaan kilpailukykyinen langallisten verkkojen kanssa. Langaton lähiverkko tarjoaa kaiken langallisten verkkojen toiminnallisuuden ilman johtojen aiheuttamia fyysisiä rajoituksia. [Sta97a]

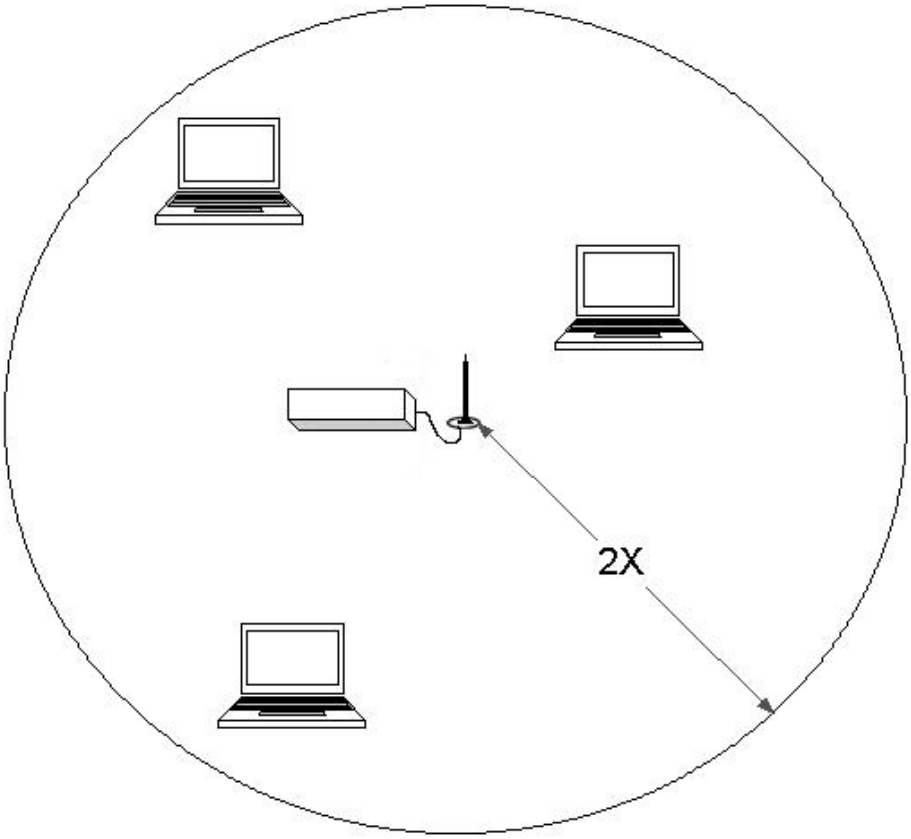
1.1 Ad hoc –verkko

Yksinkertaisimmillaan langaton lähiverkko on sellainen, jossa kaksi tai useampi langattomalla sovittimella (verkkokortilla) varustettua laitetta kommunikoivat suoraan keskenään (Ks. Kuva 1). Tällaista itsenäistä verkkoa kutsutaan ad hoc –verkoksi (tai peer-to-peer, eli vertaisverkoksi). Voidaan puhua myös ns. yhden solun verkosta. Ad hoc –verkon etuihin kuuluu, että sellainen voidaan järjestää vaivatta tarpeen vaatiessa. Mitään etukäteiskonfigurointia tai erillistä verkonhallintaa ei yleensä tarvita. [Gei99]



Kuva 1 Ad hoc –verkko.

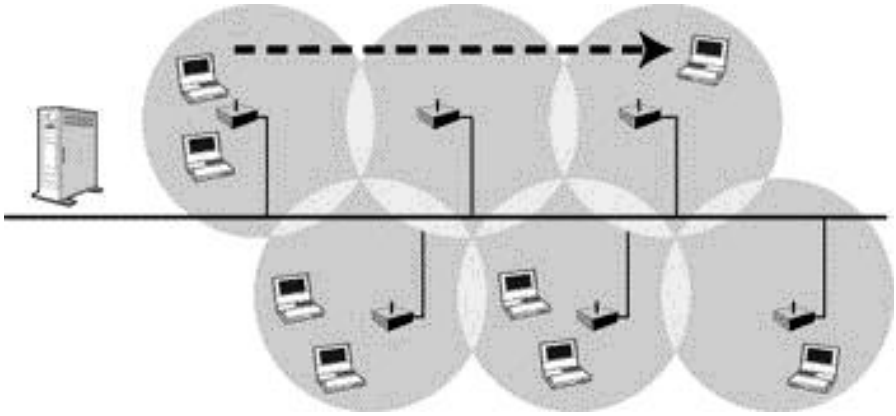
Verkon kantama voidaan kasvattaa jopa kaksinkertaiseksi lisäämällä verkkoon tukiasema, joka toimii toistimena. Kuva 2 esittää tätä ratkaisua, tosin lähteestä riippuen tällainen järjestely voidaan lukea jo infrastruktuuriverkoksi. Jos verkkoon kuuluu tukiasema, yleensä kaikki liikenne WLANissa kulkee tukiaseman kautta muille verkon langattomille laitteille. Tämä tosin riippuu kyseessä olevasta WLANin toteutuksesta joten myös yhtäaikainen peer-to-peer ja tukiasematoiminta on mahdollista. [WLANA]



Kuva 2 Ad hoc -verkon kantaman kasvattaminen tukiaseman avulla

1.2 Infrastruktuuriverkko

Kun verkkoon lisätään yksi tai useampia tukiasemia, jotka liitetään laajempaan verkkoinfrastruktuuriin, puhutaan infrastruktuuriverkosta. Tukiasemana voi toimia tavallinen tietokone tai erillinen tukiasemalaite. Useista tukiasemista, jotka ovat yhteydessä toisiinsa joko langattomasti tai lankojen välityksellä, muodostuu langaton lähiverkko (ks. Kuva 3). Yleensä verkko ei kuitenkaan ole täysin langaton, vaan tukiasemat liitetään perinteiseen langalliseen lähiverkkoon. Tukiasemat voidaan tarvittaessa liittää toisiinsa myös langattomasti. Tämä ei kuitenkaan ole järkevää, jos yhteys voidaan tehdä langallisesti, sillä radiotien kapasiteetti on rajallinen.



Kuva 3 Infrastruktuuriverkko ja roaming [WLANA]

Tukiasemat toimivat siltoina langallisen ja langattoman lähiverkon välillä. Langattomasta verkosta tuleva tietoliikenne kulkee tukiasemilta langallisen verkon kytkimille, jotka välittävät liikenteen eteenpäin. Vastaavasti tukiasemat välittävät langallisesta verkosta tulevan liikenteen langattoman verkon laitteille.

Langaton lähiverkko voidaan rakentaa siten, että tukiasemien peittoalueet ovat osittain limittäisiä. Tällöin käyttäjä voi liikkua niiden peittoalueella ilman yhteyden katkeamista. Yhteys verkkoon säilyy, vaikka käytettävä tukiasema vaihtuu käyttäjän sijainnin mukaan. Tukiaseman vaihdokset ovat käyttäjälle näkymättömiä. Tekniikasta käytetään nimitystä roaming. [WLANA]

1.3 Langattomat tekniikat

Ylivoimaisesti suosituin siirtotekniikka, eli fyysisen kerroksen ratkaisu, langattomissa lähiverkoissa on radioaallot. Muita langattomiin yhteyksiin käytettyjä tekniikoita ovat esimerkiksi infrapuna ja laser. Radioaaltojen hyvänä puolena on, että yhteyden saamiseksi ei tarvitse olla näköyhteyttä lähettimen ja vastaanottimen välillä. Radioaallot pystyvät läpäisemään jonkun verran esteitä, kuten seiniä, ja mahdollistavat kunnollisen liikkuvuuden lähiverkon käyttäjille. Radioaaltojen huonona puolena on, että ne ovat alttiita häiriöille. Jos langattoman lähiverkon käyttöalueella on laitteita, jotka käyttävät samoja taajuusalueita, saattaa syntyä interferenssiä, joka laskee verkon suorituskykyä tai estää sen toiminnan kokonaan (tämä pätee varsinkin perinteisille kapeakaistalähetyksille).

Suosituin radiotekniikka langattomissa lähiverkoissa on hajaspektritekniikka (Spread Spectrum, SS), joka on alun perin sotilaskäyttöön kehitetty laajakaistatekniikka. Hajaspektritekniikalla lähetettäessä alkuperäinen signaali hajautetaan laajalle taajuusalueelle, ja vastaanotettaessa kasataan alkuperäiseen muotoonsa. Hajautuksen ansiosta lähetystehon tiheys (mitattuna tehoyksikköä/hertsi) on paljon pienempi kuin samalla kokonaisteholla lähettävän kapeakaistaradiolla. Tämä mahdollistaa sen, että kapeakaista- ja hajaspektrilähetykset voivat jakaa saman taajuusalueen aiheuttamatta toisilleen juurikaan häiriöitä. Satunnaiselle vastaanottimelle hajaspektrisignaali näyttää

taustakohinalta, jos tiedossa ei ole hajaspektrisignaalin muodostamiseen käytetyt parametrit. Muut radiolähetykset ja elektroninen kohina, jotka ovat tyypillisesti luonteeltaan kapeakaistaisia, häiritsevät vain pientä osaa hajaspektrisignaalista. Hajaspektritekniikka uhraa tehokkuutta kaistanleveyden käytön suhteen, jotta saavutetaan luotettavat, eheät ja turvalliset tiedonsiirtoyhteydet. Kaksi tärkeintä hajaspektritekniikkaa ovat suorasekvenssihajaspektri (Direct Sequence Spread Spectrum, DSSS) ja taajuushyppelyhajaspektri (Frequency Hopping Spread Spectrum, FHSS). [WLANA, Gei99]

Taajuushyppelyhajaspektrissä käytetään kapeakaistaista kantoaaltoa, jonka taajuutta vaihdetaan tietyn kaavan mukaan lyhyin väliajoin. Eli signaali hyppii taajuudelta toiselle ajan funktiona ja yhdellä taajuudella viivytään kerrallaan vain lyhyt aika. Mikäli jollain taajuudella häiriö estää lähetyksen, tehdään uudelleenlähetys kun hypätään seuraavalle taajuudelle. Taajuushyppelyssä käytettävän modulaatiotekniikan toteutukseen tarvittavien komponenttien tekniset rajoitukset nykyisellään rajoittavat tiedonsiirtonopeuden kahteen megabittiin sekunnissa. Samoin rajoittavana tekijänä ovat ISM-kaistan määräykset FHSS:lle. [Sch90, Dea97]

Suorasekvenssihajaspektritekniikkaan perustuvissa lähetyksissä alkuperäinen signaali (eli lähetettävä tieto / informaatiokaista) moduloidaan sitä paljon laajakaistaisemmalla digitaalisella signaalilla. Eli alkuperäisen datan bitit muunnetaan ennen lähetystä esitettäväksi useammalla bitillä (redundanssi). Koodia, jonka mukaan tämä muunnos tehdään, sanotaan levityskoodiksi. Vastaanottajan on tiedettävä myös tämä koodi, jotta alkuperäisen datan kokoaminen on mahdollista. Suorasekvenssilähetyksen redundanttisuuden ansiosta on mahdollista selvittää alkuperäinen signaali, vaikka osa lähetyksestä kärsisikin häiriöistä. Suorasekvenssitekniikalla päästään huomattavasti suurempiin tiedonsiirtonopeuksiin kuin taajuushyppelytekniikalla. [Sch90, Dea97]

2 Langattomuuden vaikutus tietoturvaan

Radiotekniikkaan perustuvat langattomat lähiverkot (samoin kuin kaikki radiotekniikkaan perustuvat verkot) ovat luonnostaan turvattomampia kuin langalliset lähiverkot. Radioaallot läpäisevät fyysisiä esteitä ja leviävät joka puolelle lähettimen ympäristöön. Lähetetty, ja mahdollisesti luottamuksellinen data voidaan siis kuulla vaikkapa toimiston seinien ulkopuolelta, mikäli kuuntelijalla on käytettävissään sopiva vastaanotin. Langattoman verkon, jota ei ole suojattu millään keinoin, asentaminen merkitsee langallisen verkon termeillä kuvattuna tilannetta, jossa verkkoon pääsyyn tarvittavia pistokkeita asennetaan kaikkialle ympäristöön, mukaan lukien vaikkapa toimiston lähellä oleva parkkipaikka, avaten näin hyökkääjälle pääsyn organisaation verkon sisäisiin osiin [Cis01]. Langaton lähiverkko onkin erityisen altis salakuuntelulle, palvelunestolle ja verkon luvattomalle käytölle. Perinteisessä langallisessa verkossa turvallisuus saavutetaan fyysisesti rajoittamalla pääsyä verkon komponentteihin, eli kaapeloinnit sijoitetaan niin ettei niihin pääse helposti käsiksi, kytkimet ja palvelimet yms. sijaitsevat lukituissa tiloissa ja rakennuksen ovilla voi olla vartijat. Kun fyysinen turvaaminen ei ole mahdollista, on käytettävä kryptografisia menetelmiä avoimen verkon yhteyksien suojaamiseen [Aso95].

2.1 Salakuuntelu

Salakuuntelu on hyökkäys verkossa liikkuvan datan luottamuksellisuutta vastaan ja luultavasti yleisin uhka langattomille lähiverkoille. Radioliikennettä voidaan ottaa vastaan täysin passiivisesti, joten salakuuntelua ei pystytä havaitsemaan. Kuuntelemalla verkkoliikennettä voidaan saada selville käyttäjätunnuksia, niihin liittyviä salasanoja ja muuta tärkeää dataa. Salasanojen avulla voidaan saada edelleen parempi pääsy verkkoresursseihin ja dataan. Ratkaisu tähän on käyttää salausta ainakin silloin kun dataa siirretään radiotiellä.

Hajaspektritekniikkaan perustuvien langattomien lähiverkkojen on sanottu olevan turvallisia, koska hajaspektrilähetyksiä on vaikea havaita ja ottaa vastaan, jos hajautuksessa käytettävät parametrit eivät ole tiedossa. Tämä pitääkin paikkaansa tietyssä määrin, kun on kyse valmistajakohtaisista laitteista, joita ei ole yleisesti saatavilla, eikä myöskään tietoa niiden määrityksistä. Tosin riittävillä resursseilla ja taidoilla varustettu henkilö pystyy saamaan selville mitkä tahansa hajaspektritekniikkaan(kin) perustuvat lähetykset. [Sch90]

Kun on kyse yleiseen standardiin perustuvasta tekniikasta, ei voida missään tapauksessa luottaa hajaspektritekniikan tuovan yksityisyyttä langattoman verkon yli tehtäviin yhteyksiin. Standardin mukaisella, helposti kaupasta saatavalla langattomalla verkkokortilla voidaan ottaa vastaan kaikki liikenne, mitä verkossa lähetetään (esim. IEEE 802.11).

Salakuunteluun liittyy myös liikenneanalyysi. Koska radioliikenne on helppoa kuunnella, voidaan tehdä liikenneanalyysi vaikka verkossa liikkuvan pakettimuotoisen liikenteen hyötykuorma olisikin salattu pitävästi.

2.2 Palvelunesto

Vakava uhka langattomille lähiverkoille on myös mahdollinen palvelunestohyökkäys. Radiotekniikkaan perustuvan lähiverkon liikennöinti voidaan estää lähettämällä riittävästi häiriötä radiotielle. Hajaspektritekniikka auttaa selviämään suhteellisen pahoistakin häiriöistä niin, että verkko toimii vaikkakin tiedonsiirtonopeudet laskevat. Mutta verkon toiminnan kokonaan estävän laajakaistaisen häirintälaitteen rakentaminen on mahdollista ja onnistuu jopa kohtuullisen pienillä resursseilla. Radiotien häirinnästä on erittäin vaikeaa saada syyllistä kiinni ja vastuuseen teostaan. [Rus01]

2.3 Luvaton pääsy

Jos langattomassa lähiverkossa ei ole mitään menetelmiä joilla tunnistetaan ja todennetaan verkkoon liittyvät laitteet, ei myöskään ole mahdollista rajoittaa pääsyä verkkorajapintaan. Jos turvallista pääsynhallintaa ei ole järjestetty, on luvattomien tahojen mahdollista päästä käsiksi verkon resursseihin, koska radioverkko ei välttämättä rajoitu fyysisiin esteisiin. Luvaton pääsy voi johtaa laajempaankin murtoon, esimerkiksi verkossa oleville palvelimille. Luvaton pääsy verkkoresursseihin voi olla myös esimerkiksi Internet-yhteyden luvatonta käyttöä.

2.4 Muut hyökkäykset

Toisto ja väärentäminen voivat olla mahdollisia riippuen langattoman lähiverkkotekniikan ominaisuuksista. Nämä ovat monimutkaisempia hyökkäyksiä, joita saatetaan käyttää osana muita hyökkäyksiä tai itsenäisinä. Mikäli tietoturvaa ei ole otettu riittävässä määrin huomioon tekniikkaa määritellessä, voi verkko olla käytännössä turvaton kaikkia näitä hyökkäyksiä vastaan. Sama kyllä pätee tekniikan osalta myös langallisiin verkkoihin, mutta siellä pääsyä voidaan rajoittaa fyysisillä turvajärjestelyillä, kuten aiemmin jo todettiin.

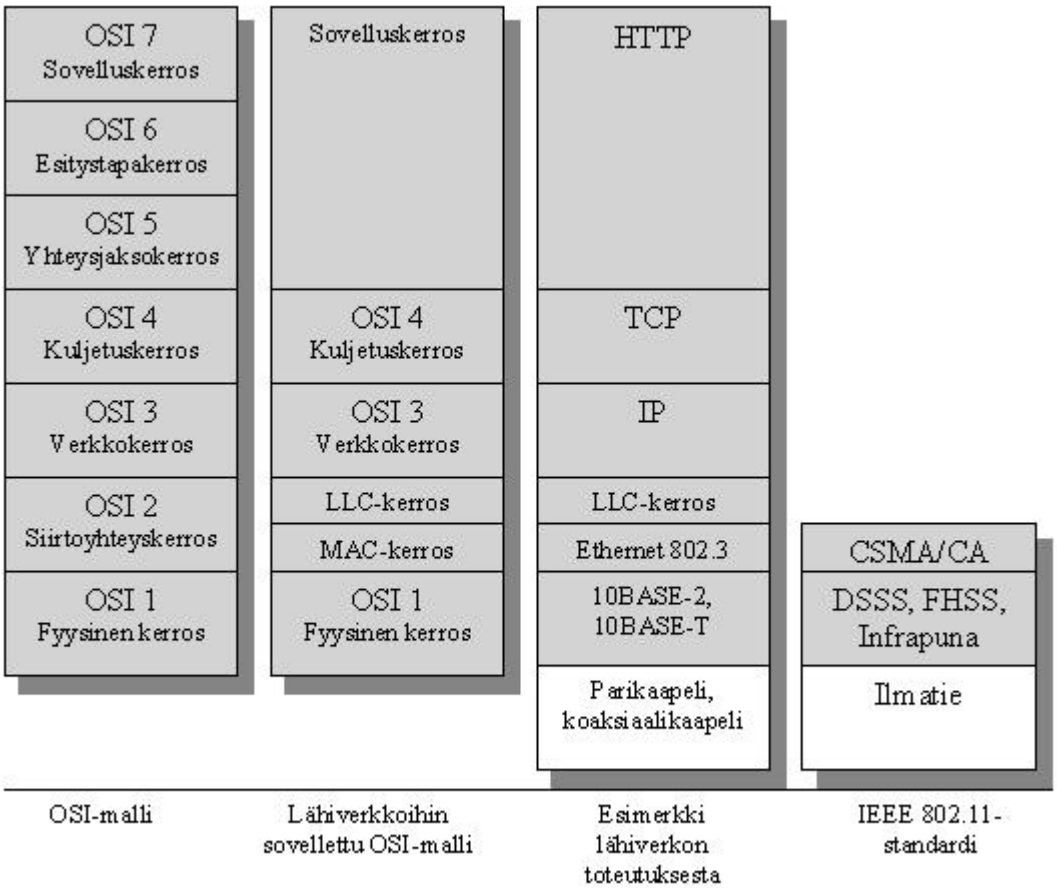
3 Langattomien lähiverkkojen standardointi

Tietokoneverkot ja radiotekniikka yhdistettiin ensimmäisen kerran jo vuonna 1971 ALOHANET-projektissa Havaijin yliopistossa. Radiotekniikkaan perustuvien lähiverkkokomponenttien kaupallisen kehittämisen mahdollisti Pohjois- ja Etelä-Amerikassa 1980-luvun puolivälissä tehty päätös vapauttaa niin sanotut ISM-kaistat (Industrial, Scientific and Medical bands) julkiseen käyttöön. Nämä taajuuskaistat ovat 902-928 MHz, 2.40-2.4835 GHz ja 5.725-5.850 GHz, eikä niitä käyttäville laitteille tarvitse hakea erillistä lupaa. Euroopassa ja Aasiassa 2.4 GHz ISM-kaista hyväksyttiin 1995 ja tämä kaista onkin ainoa maailmanlaajuisesti lisenssivapaa. Valmistajakohtaisia ratkaisuja alkoikin ilmestyä pian 1980-luvun päätöksen jälkeen (lähinnä Yhdysvalloissa ja 902 MHz kaistalle), mutta markkinoiden kiinnostus langattomia lähiverkkoja kohtaan pysyi vähäisenä vuoden 1997 loppuun saakka, jolloin ilmestyi ensimmäinen virallinen ja kansainvälisesti hyväksytty standardi langattomille lähiverkoille. Kyseessä oli IEEE:n (Institute for Electrical and Electronic Engineers) standardi 802.11. [Gei99] Muita langattomien lähiverkkojen standardeja ovat ETSI:n (European Telecommunications Standards Institute) HiperLAN (High Performance Radio LAN) ja HRFWG:n (HomeRF Working Group Inc.) HomeRF.

Edes saman standardin mukaiset langattoman lähiverkon laitteet eivät välttämättä ole yhteensopivia keskenään. Tähän on käytännössä kolme syytä. Ensinnäkin standardissa voi olla määriteltynä useampi protokolla jonkun asian toteuttamiseen, ja eri protokollat eivät toimi yhdessä. Esimerkiksi 802.11 standardissa on fyysisen kerroksen protokollavaihtoehtoina suorasekvenssi- ja hajaspektritekniikat, jotka ovat toteutustavoiltaan erilaisia. Toiseksi eri taajuuskaistaa käyttävät ratkaisut eivät toimi keskenään vaikka käyttäisivätkin samaa tekniikkaa ja protokollia. Kolmanneksi eri valmistajien laitteet eivät välttämättä toimi keskenään vaikka käyttäisivätkin samaa tekniikkaa ja taajuuskaistaa. Eri valmistajien toteutustavoissa voi olla eroavaisuuksia, jotka estävät yhteentoimivuuden. [Sep00]

3.1 IEEE 802.11

IEEE 802 LAN/MAN standardointikomitea kehittää lähi- ja kaupunkiverkkojen (Metropolitan Area Network, MAN) standardeja. 802-standardiperheestä tunnetuin lienee 802.3 eli Ethernet. 802.11 määrittelee langattoman lähiverkon tekniikan. OSI-mallista (Open Systems Interconnections) puhuttaessa lähiverkon standardissa määritellään fyysinen kerros ja MAC-kerros (Media Access Control), joka on osa siirtoyhteyskerrosta (ks. Kuva 4). Alkuperäinen standardi valmistui 1997 ja siinä määritellään kolme erilaista vaihtoehtoista fyysistä kerrosta, jotka ovat 2.4 GHz ISM-alueella toimivat FHSS ja DSSS, sekä infrapuna. Tiedonsiirtonopeuksien vaihtoehtoina olivat 1 ja 2 Mbit/s (Nämä ovat fyysisen kerroksen signalointinopeuksia, usein korkeammille protokollatasoille näkyvä hyötykuorman läpäisy on noin puolet signalointinopeudesta).



Kuva 4 Erilaisten protokollapinojen suhtautuminen OSI-malliin [Sep00]

802.11-standardi tukee kahta erilaista verkkotopologiaa, joista käytetään standardissa nimitystä IBSS (Independent Basic Service Set) ja ESS (Extended Service Set). IBSS on ad hoc –verkko, jossa on vain keskenään keskustelevia langattomia liikkuvia asemia, eikä yhteyttä langalliseen verkkoon. ESS on infrastruktuuriverkko, johon kuuluu tukiasemia ja niitä yhdistävä siirtojärjestelmä (distribution system, joka usein on perinteinen langallinen verkko). Mikäli verkossa on mukana tukiasema, kaikki eri asemien välinen liikenne kulkee tukiaseman kautta. Liikkuva asema assosioituu yhteen tukiasemaan kerrallaan ja kaikki liikenne kulkee sen tukiaseman kautta johon asema on assosioitunut. Roaming ESS:n sisällä on myös määritelty. [Oha99] Perusstandardin MAC-määritys sisältää tietoturvaominaisuudet, jotka ovat autentikointi ja pakettien hyötykuorman salaus. Autentikointi yhdistettynä kerroshallinnan (layer management) kanssa mahdollistaa myös pääsynvalvonnan. [IEEE97]

Siirtoyhteyskerroksella toteutettu salaus on ns. linkkitason salaus, koska siinä salaus on tietoliikennelinkkikohtainen ja puretaan aina jokaisen linkin päässä. Näin ollen salaus on myöskin ylemmille protokollakerroksille täysin läpinäkyvä, eli niillä ei ole tietoa kulkiko data matkalla olleiden linkkien läpi salattuna vai ei. Ylemmillä protokollakerroksilla tapahtuvaa salausta taas kutsutaan päästä päähän –salaukseksi. Siinä tieto salataan

lähetyspäässä ja lähetetään tietoliikenneverkon läpi ja lopulta yhteyden toisessa päässä puretaan. [Eng01]

Sittemmin 802.11 sai korjauksia, ja korjattu versio hyväksyttiin 1999. Samana vuonna valmistui 802.11b työryhmän laajennus, jossa määriteltiin 2.4 GHz taajuusalueella toimivan DSSS tekniikan nopeampi versio, joka on taaksepäin yhteensopiva. 802.11b:n tuetut tiedonsiirtonopeudet ovat 1, 2, 5.5 ja 11 Mbit/s [IEEE99]. 802.11b:n mukaiset tuotteet ovat nykyisin erittäin suosittuja. 802.11 alaisia työryhmiä on meneillään muitakin ja niissä kehitellään mm. nopeampia fyysisiä kerroksia ja eri taajuusalueilla toimivia fyysisiä kerroksia (esim. 802.11a on 5 GHz lisenssivapaalla alueella toimiva fyysinen kerros, jonka nopeus on jopa 54 Mbit/s). Tämän työn kannalta mielenkiintoisin työryhmä on 802.11i, joka kehittelee parannuksia tietoturvaan. 802.11:n tietoturvaominaisuudet ja 802.11i-työryhmän parannusehdotukset käsitellään omassa luvussaan tarkemmin.

3.2 HiperLAN

HiperLAN standardi on osa ETSIn BRAN-ohjelmaa (Broadband radio access network). HiperLANin ensimmäinen versio ei ilmeisesti koskaan realisoitunut valmiiksi tuotteiksi. Standardissa ei myöskään määritelty minkäänlaista autentikointia ja salaus toteutettu algoritmilla, joka oli salainen. [Usk97]

HiperLANin seuraava versio on luonnollisesti HiperLAN2 (lyhennetään H2). H2-standardissa määritellään myöskin MAC-kerros ja fyysinen kerros. Fyysinen kerros käyttää OFDM (Orthogonal Frequency Digital Multiplexing) –modulointimenetelmää. Sillä saavutetaan jopa 54 Mbit/s tiedonsiirtonopeus (signalointinopeus). Käytössä on 5 GHz-taajuusalueet seuraavasti:

- Eurooppa 5.15-5.35 GHz ja 5.470-5.725 GHz (Euroopassa tämä taajuusalue on lisensoitu HiperLAN2:lle, ja näin ollen estää tällä hetkellä 802.11a-tuotteiden käytön Euroopassa)
- US 5.15-5.35 GHz ja 5.725-5.825 GHz
- Japani 5.15-5.35 GHz (neuvottelut meneillään)

H2 tukee myöskin kahta verkkotopologiaa, eli ad hoc – ja infrastruktuuriverkkoa. Nämä ovat H2-terminologiassa nimeltään ”direct mode” ja ”network mode”. Muita ominaisuuksia ovat päätelaitteen ja tukiaseman välillä yhteydellinen (connection oriented) yhteys, tuki palvelunlaadulle (Quality of Service, QoS), automaattinen taajuuksien käyttö (ei tarvitse manuaalisesti tehdä taajuussuunnittelua kun lähekkäin useita tukiasemia), turvallisuusominaisuudet, roaming verkon sisällä, valmiudet toimia erilaisten langallisten verkkojen kanssa (tukiasemille convergence layer). Standardin mukaisia tuotteita on jo esitelty. [Hip02]

HiperLAN2:n tuvallisuusominaisuuksiin kuuluu linkkitason DES-pohjainen (Data Encryption Standard) salaus ja kaksisuuntainen (mutual authentication) haaste/vastaus-autentikointi. Salausta käytetään sekä hyötykuorman että signaloinnin salaamiseen. Avainten vaihtoon on kaksi vaihtoehtoa: ennalta jaettu salainen avain tai julkisen avaimen järjestelmä. Yhteysavaimia vaihdetaan säännöllisin väliajoin. Asiakkaan

liikkuessa tukiaseman alueelta toiselle handoverin tapahtuessa käytetään token-pohjaista autentikointia. [Khu00]

3.3 HomeRF

HRFWG on ryhmittymä yrityksiä, jotka ovat kehittäneet HomeRF-standardin. Standardin nykyinen versio on HomeRF 2.0 ja se tukee 10, 5, 1.6 ja 0.8 Mbit/s nopeuksia. HomeRF on nimensä mukaisesti suunnattu kotikäyttöön ja pientoimistoihin. Fyysisen kerroksen radiotekniikkana on taajuushyppelyhajaspektri, joka toimii 2.4 GHz ISM-alueella. Tukee yhtäaikaista vertaisverkkotopologiaa (ad hoc, peer-to-peer) ja infrastruktuuriverkkoa (host/client, eli liikkuva asema/tukiasema). Standardissa on myös määritelty priorisoituja palveluluokkia ja DECT-tekniikkaan (Digital Enhanced Cordless Telecommunications) tuki johdottomille puhelimille. HomeRF-tuotteita on markkinoilla. [Chinitz]

HomeRF:n tietoturvapalvelut ovat pääsynhallinta ja datan linkkitason salaus. Salaus on toteutettu (ilmeisesti) WEP-tyyppisenä (eli RC4) jonosalauksena, jossa käytetään 128-bittistä avainta ja 32-bittistä alustusvektoria (WEP ja siihen liittyvät käsitteet käsitellään myöhemmin). HomeRF pääsynhallinta perustuu salaiseen verkkotunnisteeseen (network ID, NWID). HomeRF:n ei käytä staattisia hyppelykuvioita vaan pseudosatunnaista ja sen suomaan turvallisuuteen luotetaan myös. Nykyisillä HomeRF-tuotteilla ei suoraan pysty selvittämään hyppelykuviota, jos NWID ei ole tiedossa. Päättäväistä ja riittävät resurssit omaavaa hyökkääjää nämä menetelmät eivät estä. [Hom01]

4 IEEE 802.11 tarkemmin

Kuten aiemmin jo todettiin, standardissa määritellään fyysinen kerros ja MAC-kerros. Fyysinen kerros on se osa, joka on tekemisissä siirtomedian kanssa. Radiotekniikkaan perustuvassa langattomassa lähiverkossa siirtomediana toimii ilma ja fyysistä kerrosta voidaan kutsua myös nimellä radiomodeemi. Radiomodeemin pääominaisuuksia ovat sen käyttämä taajuuskaista, signalointinopeus, modulaatiotekniikka ja lähettimen teho. [Tou00]

MAC-kerroksen tehtävänä on ohjata siirtomedian käyttöä. Tämä tapahtuu kanavapääsymekanismin (channel access mechanism) avulla. Se jakaa pääresurssin, eli tässä tapauksessa radiotien, verkon osapuolten kesken. Kanavapääsymekanismi on MAC-kerroksen ydin ja se kertoo jokaiselle verkon liikennöitsijälle koska voi lähettää dataa ja koska pitää kuunnella verkkoa. [Tou00] MAC-kerros sisältää myös standardin määrittelemät tietoturvapalvelut, jotka ovat luottamuksellisuus, autentikointi ja pääsynvalvonta. Standardin puitteissa nämä tietoturvaominaisuudet ovat rajatut koskemaan vain langattomasti tapahtuvaa kahden aseman välistä liikennettä. [IEEE97]

4.1 802.11 tietoturvaominaisuudet

802.11-standardi tarjoaa MAC-kerroksella tietoturvapalvelut, joilla pyritään saavuttamaan ainakin samantasoinen tietoturvallisuus kuin langallisessa verkossa. Nämä palvelut ovat WEP (Wired Equivalent Privacy), eli datan luottamuksellisuuden takaava salaus, sekä autentikointi ja siihen liittyvä pääsynhallinta. WEP ei ole standardin mukaan pakollinen toteutettava. Suuret valmistajat ovat kuitenkin perustaneet WECA:n (Wireless Ethernet Compatibility Alliance), jonka tehtävänä on varmentaa eri valmistajien 802.11-tuotteiden yhteensopivuus. WECA:n yhteensopivuustestit läpäisseet laitteet ovat Wi-Fi -yhteensopivia (Wireless Fidelity). Wi-Fi pitää sisällään pakollisena tuen 40-bittiselle WEP-salaukselle.

4.1.1 WEP

WEP-salaus suunniteltiin tarjoamaan ainakin samantasoinen luottamuksellisuus langattomasti siirrettävälle datalle kuin on hyvin fyysisesti suojatussa langallisessa verkossa [IEEE97]. WEP on linkkitason salaus ja RC4-jonosalaimen toteutus, jossa käytetään 40- tai 104-bittistä symmetristä (jaettu salainen) avainta (40-bittinen salaus on standardin mukainen ominaisuus, 104-bittinen useiden valmistajien käyttämä oma lisäys). WEP-toteutuksessa käytetään jaetun avaimen ja alustusvektorin yhdistelmää pseudosatunnaislukugeneraattorin (pseudo random number generator, PRNG) siemenenä, joka tuottaa mielivaltaisen pitkän avainbittivirran (keystream). Selkokielinen data ja avainvirta ajetaan biteittäisen XOR-operaation (exclusive OR) läpi, jolloin tuloksena on salattu data. Alustusvektori on 24 bitin mittainen ja lähetetään aina salatun datan mukana selkokielisenä. Näin vastaanottaja saa aikaiseksi saman avainvirran ja selkokielinen data voidaan palauttaa XOR-operaatiolla. Alustusvektorilla pyritään välttämään saman avainvirran käyttöä kahdesti, mikä vaikeuttaa salauksen murtamista. Alustusvektorilla

saavutetaan myös salauksen itsestään synkronoituvuus yksittäisen paketin tasolla, mikä on tärkeää linkkikerroksen salauksessa koska pakettihävikki voi olla mittavaa. Jotta havaittaisiin onko paketti muuttunut siirron aikana, lasketaan datasta tarkistussumma lineaarisella CRC-32 –menetelmällä. [IEEE97]

RC4 on helppo toteuttaa sekä ohjelmallisesti että laitteistolla ja on erittäin nopea. Näiden ominaisuuksien ansiosta RC4 onkin varsin paljon käytetty salausmenetelmä. Salauksen vahvuus perustuu salaisen avaimen selvittämisen vaikeuteen kaikki avaimet läpikäymällä. Tähän taas vaikuttaa avaimen pituus ja yhden avaimen käytön ikä. [IEEE97]

4.1.2 Autentikointi ja pääsynhallinta

Ennen kuin langaton asiakasasema ja tukiasema voivat kommunikoida, asiakkaan täytyy assosioitua tukiaseman kanssa. Tähän tapahtumaan liittyen standardissa on määritelty kolme tilaa, joissa asiakas voi olla:

1. Autentikoimaton (todentamaton) ja ei-assosioitunut
2. Autentikoitu ja ei-assosioitunut
3. Autentikoitu ja assosioitunut

Assosioituminen tapahtuu siis kahdessa vaiheessa käymällä tilat järjestyksessä läpi. (muita mahdollisia tilasiirtymiä varten standardissa on määritelty täydellinen tilakone). Kun asiakas tulee langattoman verkon alueelle se havaitsee tukiasemat niiden lähettämistä merkkipaketeista (beacon). Kun tukiasema on löytynyt, asiakas ja tukiasema autentikoituvat toinen toisilleen lähettämällä useita hallinnointipaketteja (management frame). Autentikoitumisen jälkeen seuraa assosioituminen, minkä jälkeen asiakas kuuluu verkkoon ja voi lähettää dataa. Standardi määrittelee kaksi autentikointimenetelmää: avoin autentikointi (Open System Authentication) ja jaetun avaimen autentikointi (Shared Key Authentication). Avoin autentikointi on 802.11-standardin oletusarvo, ja siten pakollinen toteutettava. Kuten nimikin jo kertoo, avoin autentikointi autentikoi minkä tahansa asiakkaan, joka sitä vaan pyytää. Näin ollen kaikki halukkaat pääsevät liittymään verkkoon, jossa käytetään avointa autentikointia. [IEEE97]

Jaetun avaimen autentikointi perustuu haaste-vastaus –menetelmään ja jaettuun salaiseen avaimeen. Kun asiakas haluaa autentikoitua, tukiasema lähettää asiakkaalle haasteen selkokielisenä, joka salataan WEPilllä ja lähetetään takaisin tukiasemalle. Tukiasema purkaa salauksen ja tarkistaa että saatu data vastaa lähetettyä haastetta ja varmistaa että tarkistussumma pitää paikkansa. Jos tarkistukset menevät läpi, on autentikointi onnistunut. Tämän jälkeen tukiasema ja asiakas vaihtavat rooleja, että saadaan aikaiseksi keskinäinen autentikointi. Jaetun avaimen autentikointi on standardin mukaan siinä mielessä vapaaehtoinen toteutettava, että jos WEP (standardi: vapaaehtoinen, WiFi: pakollinen) ei ole toteutettu, ei jaetun avaimen autentikointiakaan voi toteuttaa. Mutta jos WEP on toteutettu, myös jaetun avaimen autentikointi on toteutettava. Jaetun avaimen autentikoinnilla voidaan siis todentaa, että asiakas kuuluu joko niihin, jotka tuntevat salaisen avaimen tai niihin jotka eivät tunne. Pääsynhallinta seuraa siitä, että autentikoimaton asema ei pääse assosioitumaan tukiasemaan. [IEEE97]

4.1.3 Standardiin kuulumattomia tietoturvaominaisuuksia

Useat valmistajat käyttävät tukiasemissaan pääsynhallintalistoja (Access Control List, ACL), vaikka niitä ei standardissa olekaan määritelty. Pääsynhallinta perustuu MAC-osoitteeseen (tunnetaan myös nimillä laitteisto-osoite, hardware-osoite, hw-osoite), joka on kaikille verkkokorteille yksilöllinen. Pääsynhallintalistat ovat hyvä keino, jos pääsynhallinnan perusteena käytetty ominaisuus on vahva. MAC-osoite on kuitenkin mahdollista väärentää ja sallitut osoitteet voi saada selville salakuuntelemalla, koska MAC-osoitteet on oltava paketeissa salaamattomassa muodossa. Edelleen isossa verkossa listojen ylläpito jokaiselle tukiasemalle erikseen on erittäin työlästä, ellei sitä varten ole kehitetty tehokasta keskitettyä hallintamenetelmää. [Arb01]

802.11b-mukaisten laitteiden valmistajista Lucent käyttää valmistajakohtaisena ei-standardin mukaisena pääsynhallintakeinona verkon nimeä (service set ID, SSID). Menetelmä voidaan asettaa päälle tukiasemista, ja tämän jälkeen verkkoon ei pääse mikäli verkon nimi ei ole tiedossa. SSID toimii siis jaettuna salaisuutena. Tämä ei ole erityisen turvallinen pääsynhallintakeino, koska SSID lähetetään useissa hallinnointipaketeissa selkotekstinä. WEP ei auta asiaan, koska sillä salataan vain pakettien hyötykuorma. SSID:n saa siis helposti selville salakuuntelemalla verkon liikennettä. [Arb01]

4.2 802.11 tietoturvaominaisuuksien ongelmia

4.2.1 WEP-ongelmia

Kuten aiemmin jo nähtiin, WEP käyttää salaukseen RC4 jonosalausalgoritmia, jossa salaamiseen ja purkamiseen käytetään XOR-operaatiota. Tällaista salausmenetelmää vastaan on useita hyökkäysmahdollisuuksia. Jos hyökkääjä muuttaa bitin salatusta tekstistä, vastaava bitti muuttuu salausta purettaessa. Jos salakuuntelija saa haltuunsa kaksi salasanomaa, jotka on salattu käyttäen samaa avainvirtaa, saadaan muodostettua selkotekstien XOR. Tämä tieto mahdollistaa tilastollisen hyökkäyksen, jolla voidaan saada selville alkuperäiset selkotekstit. Kun selkoteksti saadaan selville, selviää myös salaukseen käytetty avainvirta, minkä jälkeen voidaan purkaa kaikki samalla avainvirralla salatut datat. [Bor01]

WEPissä on suojaukset näitä hyökkäyksiä vastaan. Jotta havaittaisiin onko pakettia muunneltu siirron aikana, lasketaan datasta eheydentarkistusarvo (Integrity Check, IC), joka lisätään pakettiin ja salataan samalla kuin datakin. Jotta samaa avainvirtaa ei käytettäisi pakettien salaamiseen, käytetään alustusvektoria (Initialization Vector, IV), joka liitetään salattuun pakettiin selkokielisenä. Jaettu salainen avain ja alustusvektori yhdistetään liittämällä ne peräkkäin (40-bittinen jaettu salainen avain + 24-bittinen alustusvektori = 64-bittinen PRNG siemen). Valitettavasti molemmat keinot on toteutettu huonosti. [Bor01]

IC-arvo lasketaan tavallisella CRC-32 tarkistussummalla. CRC-32 on lineaarinen toiminpide, mikä tarkoittaa että on mahdollista laskea kahden CRC-arvon ero niiden

kahden datan erosta, josta ne on otettu. Pystytään siis laskemaan mitkä bitit pitää muuttaa, että saadaan oikea tarkistussumma kun ollaan muunneltu pakettia. Paketteja voidaan siis muunnella mielivaltaisesti ja siltikin saadaan se tarkistussuman puolesta näyttämään oikealta.

Alustusvektorille varattu 24-bittinen arvo on liian pieni, ja takaa sen että samaa avainvirtaa tullaan käyttämään uudelleen (tästä käytetään myös nimitystä alustusvektoreiden törmäys). Käytännössä on siis 2^24 erilaista avainvirtaa jokaista salaista avainta kohti. Vilkkaasti liikennöity tukiasema, joka lähettää jatkuvasti 1500 tavun paketteja 11 Mbit/s nopeudella, käyttää koko alustusvektoriavaruuden 1500*8/(11*10^6)*2^24 = ~18000 sekunnissa, eli viidessä tunnissa. Käytännön toteutuksissa sama salainen avain on jaettu kaikkien langattoman verkon laitteiden kesken, jolloin alustusvektoreiden törmäyksiä sattuu aika suurella todennäköisyydellä. Standardin mukaan ei edes ole pakollista vaihtaa alustusvektorin arvoa jokaisen paketin kohdalla. Mainituista ongelmista johtuen WEPillä salattua liikennettä vastaan on useita hyökkäyksiä. [Bor01]

4.2.2 Hyökkäyksiä WEP-salausta vastaan

Standardin mukaista 40-bittisellä avaimella tehtyä salausta vastaan on mahdollista tehdä raa'an voiman hyökkäys (brute force attack), eli käydä kaikki mahdolliset 40-bittiset avaimet läpi. Vaadittavat resurssit eivät ole kovinkaan mahdottomat hankkia.[Dol95]

24-bittinen alustusvektori tekee mahdolliseksi löytää salakuuntelemalla alustusvektoreiden törmäyksiä ja johtaa niistä tilastollisella hyökkäyksellä selkotekstit ja käytetyt avainvirrat. Riittävästi liikennettä tallentamalla on mahdollista laajentaa hyökkäystä ja kasata kaikkiin alustusvektoreihin liittyvät avainvirrat minkä jälkeen kaikki liikenne voidaan purkaa vaikka itse jaettu salainen avain ei olekaan tiedossa. Hyökkäyksestä käytetään nimitystä sanakirjahyökkäys. [Bor01] Tällaiset hyökkäykset ovat täysin passiivisia ja varsin mahdollisia toteutettavia. Tähän tarkoitukseen tehty ohjelmapaketti on vapaasti saatavilla Internetistä [New01].

RC4:ään liittyen löytyi myöskin heikkous, joka mahdollistaa WEP-salauksen täydellisen murron (eli saadaan selville salausavain). Pelkästään salattua liikennettä keräämällä on mahdollista laskea käytetty salainen avain. Hyökkäys perustuu siihen, että tietyt alustusvektorin arvot tuottavat heikkoja avaimia. Näistä avaimista tuotetulla avainvirralla salattu data antaa tietoa itse salaisesta avaimesta. [Flu01] Hyökkäys on erittäin tehokas. Laskentatehoa ei tarvita juuri ollenkaan ja hyökkäykseen tarvittava aika skaalautuu lineaarisesti. Vilkkaasti liikennöidyssä verkossa murto tapahtuu muutamassa tunnissa (joskus jopa nopeammin). Tämäkin hyökkäys on täysin passiivinen ja käytännössä erittäin toteutettavissa. Hyökkäyksen toteutti ensimmäisenä Adam Stubblefield, mutta hän ei julkaissut käyttämiään ohjelmia [Stu01]. Pian tämän jälkeen Internetiin ilmestyi vapaasti saataville kaksi hyökkäyksen toteuttavaa ohjelmaa: Airsnort (http://airsnort.shmoo.com/) ja Wepcrack (http://wepcrack.sourceforge.net/).

Liikenteen muuntaminen on myös mahdollista koska standardissa käytetty tarkistussumma ei estä tahallista pakettien muuntamista. Myös kokonaisten pakettien väärentäminen on mahdollista jos on tiedossa salatun paketin selkoteksti. Koska alustusvektoria ei tarvitse muuttaa, voidaan samaa pakettia käyttää väärentämisen pohjana koko ajan. Tällaiset hyökkäykset ovat tyypiltään aktiivisia ja hankalampia toteuttaa kuin pelkästään passiivista monitorointia vaativat hyökkäykset. Myös kerättyjen pakettien toistaminen on mahdollista ja sitä voidaan käyttää hyökkäyksissä.

4.2.3 Heikkous jaetun avaimen autentikoinnissa

802.11:ssä käytettävä jaetun avaimen autentikointimenetelmä esiteltiin aiemmin. Salakuuntelemalla onnistunut autentikointi on mahdollista saada selville haasteen mittainen käypä avainvirta ja siihen liittyvä alustusvektori. Näillä tiedoilla ja laskemalla tarkistussumma on mahdollista luvattomien tahojen autentikoitua verkkoon, vaikka salainen avain ei olekaan tiedossa. Verkon käyttö tästä eteenpäin kuitenkin tarvitsee muiden hyökkäysmenetelmien käyttöä, koska jaettu WEP-avain ei ole tiedossa. [Arb01]

4.2.4 Avainten jakelu ja käyttö

Avainten hallinta on jätetty kokonaan määrittelemättä standardissa. Näin ollen suurin osa tuotteiden valmistajista on jättänyt toteuttamatta avainten jakelun missään muodossa. Siten loppukäyttäjälle jää ratkaistavaksi tunnettu kryptografian ongelma: kuinka toimittaa salaiset avaimet luotettavasti verkon tukiasemille ja verkkoa käyttäville tietokoneille. Manuaalisesti tehtynä työmäärä verkon koon suurentuessa käy nopeasti käytännössä liian suureksi. Ja mitä useammalle jaettu salaisuus on kerrottu, sitä heikommaksi salaisuus tulee. Käytännössä usein sama salainen avain on jaettu koko verkon laitteiden kesken. Jos käytetään samaa avainta kaikkien osapuolten kesken, olisi avaimet vaihdettava kohtuullisen usein WEP:n heikkouksista johtuen.

802.11 määrittelee kaksi tapaa kuinka WEP-avaimia voidaan käyttää. Ensimmäisessä tavassa verkon liikkuville asemille ja tukiasemille voidaan asettaa jokaiselle korkeintaan neljä eri avainta (yleensä kaikilla siis neljä samaa eri avainta). Salauksen purkamisen voi suorittaa millä tahansa näistä neljästä avaimesta, mutta salaamiseen käytetään vain yhtä valittua avainta kerrallaan (kun lähetetään WEP:llä salattuja paketteja, paketissa kerrotaan millä avaimella salaus on tehty). Tällä pyritään helpottamaan avainten kiertoa ja salausavaimia vaihdettaessa tapahtuvaa siirtymäajanjaksoa, kun kaikilla ei vielä välttämättä ole sama avain käytössä. Toinen tapa on avaintaulukko (WEP key mapping), jossa voidaan määritellä jokaista MAC-osoitetta kohden oma WEP-avain. Käyttäjäkohtaiset avaimet heikentävät salausta vastaan tehtyjen hyökkäysten onnistumismahdollisuuksia tehokkaasti, varsinkin jos avaimet vaihdetaan riittävän usein. Kaikkien avaimien vaihto manuaalisesti on työlästä ja suuremmissa verkoissa käytännössä mahdotonta. [IEEE97]

4.3 Liikenteen kuuntelu käytännössä

802.11b-standardin mukaisen liikenteen tarkkailu on käytännössä helppoa. Tarvittava laitteisto on esimerkiksi tavallinen PC-kone (kannettava saattaa olla kätevin vaihtoehto) ja siihen 802.11b-mukainen langaton verkkokortti. Langattomissa verkkokorteissa käytettävien piirien valmistajia on muutamia ja itse korttien valmistajia enemmänkin. Kaikki alla esiteltävät ohjelmat eivät toimi kaikkien korttien kanssa. Suosituimpia ovat Intersil Prism2-piiriin perustuvat kortit, kun on puhe ohjelmien tuesta.

Langattomien verkkojen löytämiseen sopii mainiosti vaikkapa Netstumbler-niminen ohjelma. Netstumbler lähettää probe request –paketteja, joihin tukiasemat (ja ad hoc-moodissa olevat verkkokortit) vastaavat. Näistä paljastuu kaikenlaista hyödyllistä tietoa. Toimii Windows-ympäristössä ja on ilmainen. Samaan tarkoitukseen on myös Aerosol (Windows), ApSniff (Windows 2000) ja Wellenreiter (Linux, BSD)

Saatavuus:

- http://www.netstumbler.com/
- http://www.sec33.com/sniph/aerosol.php
- http://www.bretmounet.com/ApSniff/
- http://www.remote-exploit.org/ (Wellenreiter)

Langattoman liikenteen kaappaamiseen sopivia ohjelmia (eli sniffereitä) on myös tarjolla vapaasti. Joitain mahdollisia:

- Kismet 2.0 (Linux), http://www.kismetwireless.net/
- prismdump, työkalu joka toimii Ethereal-analysaattorin kanssa (linux), http://developer.axis.com/download/tools/ ja http://www.ethereal.com
- Mognet, http://chocobospore.org/mognet/
- BSD Airtools, BSD-johdannaisille Airsnort, prismdump ja muita työkaluja, http://www.dachb0den.com/projects/bsd-airtools.html

4.4 802.11 tietoturvan tulevaisuus

Pahimpaan uhkaan, eli hyökkäykseen jossa saadaan salainen avain selville (Airsnort jne.) on jo olemassa korjauksia. Korttien valmistajista ainakin Agere Systemsillä on ORiNOCO-tuotesarjaansa firmwaren päivitys, joka estää heikkojen alustusvektoreiden käytön. Tällä tavalla päivitetyt laitteet toimivat myöskin päivittämättömien kanssa, koska lähettävä ja samalla salaava osapuoli valitsee alustusvektorin. Jotta kyseisen hyökkäyksen uhka poistuisi kokonaan, on kaikkien verkon laitteiden oltava päivitetty.

Varsinaisia tulevaisuuden langattomien lähiverkkojen tietoturvaratkaisuja kehittää meneillään oleva työryhmä 802.11i. Sen standardiehdotuksessa esitellään käsite RSN (Robust Security Network). RSN turvallisuusalgoritmit toteuttava laitteisto on RSN-pystyvä (RSN-capable) ja nykyiset vuoden 1999 802.11 standardin mukaiset laitteet ovat pre-RSN laitteita. RSN turvallisuus koostuu kahdesta perusalijärjestelmästä:

- Datan luottamuksellisuusmekanismi. RSN turvallisuus määrittelee näitä kaksi:

    - TKIP (Temporal Key Integrity Protocol), kokoelma algoritmeja joilla parannetaan WEP-protokollaa. Mahdollistaa nykyisten laitteiden turvallisuuden parantamisen ohjelmistopäivityksellä.
    - AES-pohjainen (Advanced Encryption Protocol) protokolla uuden sukupolven laitteille, joka tarjoaa vahvan salauksen.
- Turvallisuusassosiaatioiden hallinta (Security association management). RSN määrittelee useita komponentteja tähän tarkoitukseen:
    - RSN-neuvottelu, jolla muodostetaan turvayhteys.
    - IEEE 802.1X autentikointi, joka korvaa IEEE 802.11 autentikoinnin.
    - IEEE 802.1X avaintenhallinta, jolla hoidetaan avainten jakelu.

[IEEE02]

802.1X määrittelee MAC-siltaustason toimintaan vaadittavat muutokset, jotta voidaan tarjota porttipohjainen verkon pääsynhallintamenetelmä (Port based network access control capability). Sen mukaan verkkoonpääsyportti (network access port) on paikka josta järjestelmä liitetään verkkoon. Portti voi siis olla fyysinen portti (esim. keskitin/kytkin) tai looginen kuten esimerkiksi 802.11 tapauksessa liikkuvan aseman ja tukiaseman välinen assosiaatio. Liitettävä järjestelmä voi olla työasema, palvelin, silta, jne. Standardin mukaan laite jossa on portteja toimii autentikaattorina. Porttiin kiinnittyvän laitteen on kerrottava tarvittavat tiedot autentikaattorille ennen kuin se voi kommunikoida muun verkon kanssa. Autentikaattori keskustelee autentikointipalvelimen, joka suorittaa itse autentikoinnin, kanssa mistä selviää pääseekö liittyvä laite verkkoon vai ei. [IEEE01]

4.5 Johtopäätöksiä

Nykyisellään 802.11(b) mukaisten verkkojen tietoturva on helposti murrettavissa. Tämä on syytä tiedostaa ja käyttää salausta ylemmillä protokollakerroksilla, mikäli langattomassa verkossa liikkuvan tiedon arvo niin vaatii. Niin ikään verkkoon pääsyä on syytä hallita muilla kuin 802.11 tarjoamilla keinoilla.

802.11 tietoturva on hyvä esimerkki siitä, että tietoturvaprotokollien suunnitteleminen on vaikeaa. Tässä tapauksessa ei onnistuttu saavuttamaan edes luvattua langallisen verkon turvallisuuden tasoa.

5 WLAN käytännössä

IEEE 802.11b-standardin mukaiset laitteet ovat tällä hetkellä saavuttaneet suuren suosion tietoturvan puutteistaan huolimatta. Muiden standardien mukaisia tuotteita on myynnissä vain vähän. Tästä syystä käsitellään 802.11(b)-standardiin perustuvia langattomia verkkoja. Tästä eteenpäin käsitteet langaton lähiverkko ja WLAN viittaavat tässä työssä kyseisen standardin mukaisiin verkkoihin ja laitteisiin ellei toisin mainita. WLAN-verkkoja on asennettu varsinkin toimistoihin ja muutenkin enimmäkseen yrityssektorille. WLAN-tuotteet alkavat kuitenkin jo löytää kuluttajasektorillekin ja koteihin.

5.1 WLAN kotikäytössä

WLAN-verkon yleisin käyttö kotona lienee laajakaistaiseen Internet-yhteyteen liitetty tukiasema, jonka kautta omaan langattomaan lähiverkkoon liitetyt laitteet jakavat yhteyden Internetiin. Laajakaistayhteyksien tekniikoita ovat esimerkiksi kaapelimodeemi ja DSL (Digital Subscriber Line). Laajakaistayhteydet ovat jatkuvasti päällä olevia yhteyksiä ja kotikäyttäjän on syytä olla selvillä Internet-yhteyden tuomista tietoturvauhkista sekä lisäksi mahdollisen käytössä olevan WLAN-tekniikan tuomista lisähuolista.

Internet-yhteyteen liittyviin tietoturvauhkiin ei tässä syvällisemmin puututa. WLAN-tekniikkaan liittyvissä tietoturvaongelmissa paras lähtökohta on, että tiedostaa kyseiset ongelmat. Näin ongelmiin osaa varautua ja osaa ottaa tekniikassa olevat puutteet huomioon tehdessään ratkaisuja. Kotikäytössä oleva langaton lähiverkko lisää lähialueen uhkia. Internet-yhteys avaa paljon suuremmalle yleisölle mahdollisuudet tunkeutua omaan lähiverkkoon. Internetistä hyökkäyksiä tekevät eivät useinkaan etsi kotikoneilta mitään tietoja (siitä syystä, että siellä ei useinkaan ole mitään kovin mielenkiintoista), vaan haluavat koneen hallintaansa jotta voisivat käyttää sitä hyväkseen muissa hyökkäyksissä naamioiden näin hyökkäyksen todellisen alkuperän.

Vastaavasti kuluttajan langatonta lähiverkkoa uhkaavat lähellä asuvat ihmiset, jotka mahdollisesti haluavat vaikka käyttää ilmaiseksi toisen Internet-yhteyttä joko ihan vain surffaillakseen tai tehdäkseen pahojaan toisen Internet-yhteyden taakse naamioituneena. On kyllä mahdollista, että joku murtautuu varta vasten juuri sinun verkkoosi ja tämän takia kannattaakin miettiä miten arvokasta koneilla oleva tieto on ja kuinka paljon kuluttaa resursseja uhkilta suojautumiseen. Kannattaa käyttää ainakin tuotteissa olevia tietoturvaominaisuuksia, eli tässä tapauksessa asettaa WLAN-laitteissa salaus päälle ja asettaa kunnon salasana sekä tehdä ohjelmistopäivitykset. Mahdolliset pääsylistat kannattaa myöskin asettaa. Salasanat kannattaa vaihtaa riittävän usein ja käyttää ylempien protokollakerrosten salausmenetelmiä aina kun se on mahdollista. Pääteyhteyksissä kannattaa käyttää SSH:ta, webissä asioidessa SSL:ää ja arkaluontoiset sähköpostit salata vaikka PGP:llä. Nämä keinot takaavat riittävän tietoturvan useimmissa tapauksissa.

5.2 WLAN yrityskäytössä

WLANit ovat varsin suosittuja yrityskäytössä. Yrityksen verkossa liikkuva tieto saattaa olla tietyille tahoille erittäinkin arvokasta, joten tietoturvaan on suhtauduttava vakavasti. Suurissa yrityksissä WLAN-uhkiin osataan varautua ylläpidon puolesta, mutta on täysin mahdollista, että työntekijät asentavat oman luvattoman tukiaseman ilman mitään tietoturva-asetuksia ja avaavat näin suoran tien hyökkääjälle. Näin ollen saattaa olla hyödyllistä tarkistaa omat alueet Netstumblerin kaltaisella verkkokartoittimella luvattomien tukiasemien ja mahdollisten asennusvirheiden varalta.

Suurissa WLAN-kokonaisuuksissa verkon hallitseminen manuaalisesti (avaintenjakelu ja pääsylistat) on liian työlästä. Muutenkin jos verkossa liikkuvan tiedon arvo on suuri, ei kannata luottaa 802.11 standardin tietoturvaominaisuuksiin. Yleisin tapa on eriyttää WLAN infrastruktuuri luotetusta langallisesta verkosta palomuurilla. Eli suhtaudutaan langattomaan verkkoon tietoturvan osalta kuin Internet-yhteyteen. Langattomilla yhteyksillä varustetut työasemat varustetaan VPN-ohjelmistoilla. Palomuuri asetetaan ottamaan vastaan vain VPN-yhteyksiä langattomasta verkosta. VPN-palvelin voi olla vaikka palomuurin yhteydessä. Luotetaan siis ylemmän protokollatason salaukseen. Muitakin mahdollisia ratkaisuja on.

Langattomat yhteydet hankitaan yleensä kannettaviin päätelaitteisiin. Kannettavien suojaaminen kannattaa ottaa huomioon, ettei varkauden sattuessa luvattomat pääse käsiksi koneella oleviin tietoihin, tai koneen avulla yrityksen verkkoon.

6 Lähdeluettelo

[Arb01] Arbaugh, William & Shankar, Narendar & Wan, Justin. 2001. Your 802.11 Wireless Network Has No Clothes. [Julkaisusarja]. Proceedings of the International Conference on Wireless LANs and Home Networks, 2001, sivut 131-141. ISBN 981-02-4826-1. Saatavissa: http://www.cs.umd.edu/~waa/wireless.pdf, viitattu 28.4.2002.

[Aso95] Asokan, N. 1995. Security Issues in Mobile Computing. University of Waterloo. [Verkkodokumentti]. Saatavissa: http://www.semper.org/sirene/people/asokan/research/proposal.ps.gz, viitattu 26.3.2002.

[Bor01] Borisov, Nikita & Goldberg, Ian & Wagner, David. 2001. Intercepting Mobile Communications: The Insecurity of 802.11. [Verkkodokumentti]. Saatavissa: http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf, viitattu 18.4.2002.

[Chinitz] Chinitz, Leigh. HomeRF Technical Overview. [Verkkodokumentti]. Saaatavissa: http://www.homerf.org/data/events/past/pubseminar_0501/tech_overview.pdf, viitattu 28.4.2002.

[Cis01] Cisco Systems, Inc. 2001. Overview, Wireless LAN Security. [Verkkodokumentti]. Saatavissa: http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm, viitattu 26.3.2002.

[Dea97] Dearden, James. 1997. Wireless Networks. [Verkkodokumentti]. Saatavissa: http://www.jisc.ac.uk/jtap/htm/jtap-014-1.html, viitattu 20.3.2002.

[Dol95] Doligez, Damien. 1995. I broke Hal’s SSL challenge. [Verkkodokumentti]. Saatavissa: http://pauillac.inria.fr/~doligez/ssl/index.html, viitattu 18.4.2002.

[Eng01] Engdahl, Tomi. 2001. Prosessori 5/2001: Salaus Internetissä ja muissa verkoissa. ISSN 0357-4121.

[Flu01] Fluhrer, Scott & Mantin, Itsik & Shamir, Adi. 2001. Weaknesses in the Key Scheduling Algorithm of RC4. [Verkkodokumentti]. Saatavissa: http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps, viitattu 28.4.2002.

[Gei99] Geier, Jim. 1999. Wireless LANs: Implementing Interoperable Networks. ISBN 1-57870-081-7.

[Hip02] HiperLAN2 Global Forum. 2002. FAQ’s. [Verkkodokumentti]. Saatavissa: http://www.hiperlan2.com/faq.asp, viitattu 28.4.2002.

[Hom01] HomeRF Working Group. 2001. A Comparison of Security in HomeRF versus IEEE802.11b. [Verkkodokumentti]. Saatavissa: http://www.homerf.org/data/tech/security_comparison.pdf, viitattu 28.4.2002.

[IEEE97] The Institute of Electrical and Electronics Engineers, Inc. 1997. IEEE Std 802.11-1997. ISBN 1-55937-935-9.

[IEEE99] The Institute of Electrical and Electronics Engineers, Inc. 1999. IEEE Std 802.11b-1999. ISBN 0-7381-1812-5.

[IEEE01] The Institute of Electrical and Electronics Engineers, Inc. 2001. IEEE Std 802.1X-2001. ISBN 0-7381-2927-5. Saatavissa: http://standards.ieee.org/getieee802/download/802.1X-2001.pdf, viitattu 28.4.2002.

[IEEE02] The Institute of Electrical and Electronics Engineers, Inc. 2002. Proposed Tgi D1.8 Clause 8 Editing Changes. [Verkkodokumentti]. Saatavissa: http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/2-178.zip, viitattu 28.4.2002.

[Khu00] Khun-Jush. 2000. HiperLAN Type 2: A Candidate for Fixed Wireless Access Systems Below 11 GHz & Wireless HUMAN. A presentation to IEEE 802.16 BWA.3 Task Group & BWA HUMAN Group, San Diego. [Verkkodokumentti]. Saatavissa: http://grouper.ieee.org/groups/802/16/tg3/contrib/802163p-00_09.pdf, viitattu 28.4.2002.

[New01] Newsham, Timothy. 2001. 802.11 Wireless LANs. [Verkkodokumentti]. Saatavissa: http://www.lava.net/~newsham/wlan/, viitattu 18.4.2002.

[Oha99] O'Hara, Bob & Petrick, Al. 1999. The IEEE 802.11 Handbook: A Designer's Companion. ISBN 0-7381-1855-9.

[Rus01] Russell, S. F. 2001. Wireless network security for users. [Julkaisusarja]. Proceedings of the International Conference on Information Technology: Coding and Computing, 2001, sivut 172-177. ISBN 0-7695-1062-0. Saatavissa: http://ieeexplore.ieee.org/iel5/7336/19864/00918786.pdf, viitattu 26.3.2002.

[Sch90] Schilling, Donald & Pickholtz, Raymond & Milstein, Laurence. 1990. Spread spectrum goes commercial. ISSN 0018-9235. Saatavissa: http://fp.ieeexplore.ieee.org/iel3/6/2121/00058433.pdf, viitattu 19.3.2002.

[Sep00] Seppänen, Lasse. 2000. Langattomat lähiverkot, kurssimateriaali. Hämeen ammattikorkeakoulu. [Verkkodokumentti]. Saatavissa: http://trade.hamk.fi/~lseppane/courses/wlan/doc/WLANmat.doc, viitattu 8.3.2002.

[Sta97a] Stallings, William. 1997. Data and Computer Communications, Fifth Edition. ISBN 0-02-415425-3.

[Sta97b] Stallings, William. 1997. Local & Metropolitan Area Networks, Fifth Edition. ISBN 0-13-190737-9.

[Stu01] Stubblefield, Adam & Ioannidis, John & Rubin, Aviel D. Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. AT&T Labs Technical Report TD-4ZCPZZ, Revision 2. [Verkkodokumentti]. Saatavissa: http://www.cs.rice.edu/%7Eastubble/wep/wep_attack.pdf, viitattu 28.4.2002.

[Tou00] Tourrilhes, Jean. 2000. A bit more about the technologies involved… Hewlett Packard Laboratories, Palo Alto. [Verkkodokumentti]. Saatavissa: http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.Overview.pdf, viitattu 26.3.2002.

[Usk97] Uskela Sami. 1997. Security in Wireless Local Area Networks. Department of Electrical and Communications Engineering. Helsinki University of Technology. [Verkkodokumentti]. Saatavissa: http://www.tml.hut.fi/Opinnot/Tik-110.501/1997/wireless_lan.html, viitattu 28.4.2002.

[WLANA] The Wireless LAN Association. 1999. Introduction to Wireless LANs. [Verkkodokumentti]. Saatavissa: http://www.wlana.org/learn/intro.pdf, viitattu 8.3.2002.