VAASAN YLIOPISTO

TEKNILLINEN TIEDEKUNTA

TIETOLIIKENNETEKNIIKKA

Ari Takala, P86843

AMBIENT NETWORKS -VISIO JA -LIIKETOIMINTASUHTEET

Diplomityö, joka on jätetty tarkastettavaksi diplomi-insinöörin tutkintoa varten Vaasassa 13.03.2013.

Työn valvoja Timo Mantere
Työn ohjaaja Reino Virrankoski

SISÄLLYSLUETTELO **sivu**

LYHENNELUETTELO

ACS	Ambient Control Space
AES	Advanced Encryption Standard
AK	Anonymity Key
AMF	Authentication and Key Management Field
AN	Ambient Networks
ANAP	Ambient network Attachment Procedures
ANI	Ambient Network Interface
ARI	Ambient Resource Interface
ASI	Ambient Service Interface
AuC	Authentication Centre
AUTN	Authentication Token
BAN	Body Area Network
BSS	Basic Service Set
CA	Composition Agreement
CK	Cipher Key
CRC	Cyclic Redundancy Check
DC-HSDPA	Dual Carrier High-Speed Downlink Packet Access
DNS	Domain Name Server
DSSS	Direct-sequence Spread Spectrum
DUN	Dial-Up Networking
EAP	Extensible Authentication Protocol
GANS	The Generic Ambient Network Signalling
ESS	Extended Service Set
FE	Functional Entity
GLL	Generic Link Layer
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GSLP	Generic Service Layer Protocol
GTLP	Generic Transport Layer Protocol

FHSS	Frequency Hopping Spread Spectrum
HiperLan	High Performance Radio Local Area Networks
HLR	Home Location Register
IK	Integrity Key
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISO	International Organization for Standardization
IST	Information Sciences and Technology
LAN	Local Area Network
LAP	Local Access Provider
LTE	Long Term Evolution
MAC	Media Access Control
MAN	Metropolitan Network
MIC	Message Integrity Check
MRRM	Multi Radio Resource Management
NAT	Network Address Translation
OSI	Open Systems Interconnection Reference Model
PAN	Personal Area Network
PGP	Pretty Good Privacy
PHY	Physical Layer
PMS	Pairwise Master Key
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RNC	Radio Network Controller
SN	Serving Network
SRES	Signed Response
SSID	Service Set Identifier
SQN	Sequence Number
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TTP	Trusted Third Party

UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS Terrestrial Radio Access Network
VLR	Visitor Location Register
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-FI Protected Access

VAASAN YLIOPISTO
Teknillinen tiedekunta
Tekijä: Ari Takala
Tutkielman nimi: Ambient Networks -visio ja -liiketoimintasuhteet
Työn valvoja: Timo Mantere
Työn ohjaaja: Reino Virrankoski
Tutkinto: Diplomi-insinöörin tutkinto
Koulutusohjelma: Tietotekniikan koulutusohjelma
Suunta: Tietoliikenne
Opintojen aloitusvuosi: 2006
Tutkielman valmistumisvuosi: 2013 **Sivumäärä**: 107

TIIVISTELMÄ

Internetiä käyttävien päätelaitteiden määrä on kasvanut räjähdysmäisesti 2000-luvulla. Kun siirryttiin 3G- ja 4G-aikaan, niin erityisesti mobiilit päätelaitteet kuten älypuhelimet ja taulutietokoneet ovat lisänneet verkon tiedonsiirtomäärää huomattavasti. Nykypäivänä päätelaite voi olla yhteydessä Internetiin langattomasti melkein missä päin tahansa maailmaa joko matkapuhelinverkon tai WLAN-verkon välityksellä.

Nykypäivän tekniikoilla ei pystytä tehokkaasti hyödyntämään verkon kapasiteettia täysmääräisesti eikä päätelaitteilla aina ole mahdollista olla yhteydessä Internetiin olemassa olevasta verkosta huolimatta. Tämä johtuu operaattorien yhteistyön puutteesta eikä sitä osata hyödyntää liiketoiminnassakaan. Nykyiset tiedonsiirtoteknologiat eivät toimi saumattomasti keskenään ja käyttäjä joutuu tekemään monet toimenpiteet manuaalisesti. Erääksi ratkaisuksi näihin edellä mainittuihin ongelmiin oli Euroopan Komission rahoittama Ambient Networks -projekti (2004–2007), jonka tarkoituksena on ollut parantaa verkkojen välistä yhteistyötä.

Tässä diplomityössä selvitetään Ambient Networks -konseptia ja mitä kaikkea on saavutettu tähän mennessä ja millä keinoin. Lisäksi työssä käydään läpi asiantuntijoiden arviointia, jossa he käyttivät luomaansa prototyyppiä testatakseen, onko Ambient Networks:ista todella hyötyä operaattoreiden välisessä yhteistyössä ja liiketoiminnassa ja että pystytäänkö verkon kapasiteettia hyödyntämään tehokkaammin.

Työn yhteydessä tehtävä käytännön testaus pitää sisällään arvioinnin siitä, tarvitaanko Ambient Networks:in kaltaista konseptia ja miten verkkojen yhteystyö onnistuu nykytekniikoilla. Testituloksista ilmeni, että vaikka laitteet onnistuvat jakamaan tiedostoja keskenään helposti, niin siitä huolimatta esimerkiksi erilaisiin ad hoc- ja infrastruktuuriverkkoihin liittyminen ja nopeamman Internet-yhteyden jakaminen automaattisesti siirryttäessä 3G:stä WLAN-verkkoon tuotti ongelmia johtuen päätelaitteiden käyttöjärjestelmien puutteista. Testien perusteella voidaan todeta, että Ambient Networksin kaltaista päivitystä nykytekniikkoihin tarvitaan ehdottomasti.

AVAINSANAT: Ambient Networks, Ambient Networks arkkitehtuuri, Ambient Networks liiketoimintasuhteet, Ambient Networks turvallisuus

UNIVERSITY OF VAASA
Faculty of Technology
Author: Ari Takala
Topic of the Thesis: Vision and business relations of Ambient Networks
Supervisor: Timo Mantere
Instructor: Reino Virrankoski
Degree: Master of Science in Technology
Degree Programme: Degree Programme in Information Technology
Major of Subject: Telecommunication
Year of Entering the University: 2006
Year of Completing the Thesis: 2013 **Pages**: 107

ABSTRACT

Amount of Internet using terminals has been increasing rapidly in the 21st century. Especially the use of mobile terminals, like smart phones and tablets, have caused a huge increase in the amount of data transfer moving towards 3G/4G age. Nowadays terminal can be connected to Internet wirelessly via WLAN or cellular network almost all over the world.

Network capacity can not be fully exploited using legacy technologies and terminals do not have possibility to be connected Internet despite of existing network infrastructure. This is due to lack of operators' combatibility between each other and they do not exploit it on their business either. Legacy transfer technologies do not work seamlessly with each other due to absence of general control function. In addition user's intervention is required in networks communication. The Ambient Networks project was seeking solutions to these pre-mentioned problems. The project was founded by European commission and it was native on (2004–2007)

This Master's Thesis makes an overview of Ambient Networks and what has been accomplished by now and how it is done. In addition it will go over the evaluations of the Ambient Networks concept. These evaluations are done by experts with an Ambient Network prototype.

Practical evaluation includes analysis on that do we need Ambient Network in our systems and how co-operation between networks is working using legacy technologies. According to test results data transfers between terminals succeeded quite easily but attachments to networks like ad hoc and infrastructure network and exploiting automatically Internet sharing on faster Internet connection moving from 3G to WLAN caused problems due to restrictions of operating system of terminals. It is obvious that upgrade like Ambient Network will be eventually needed.

KEYWORDS: Ambient Networks, architecture of Ambient Networks, business relations of Ambient Networks, security in Ambient Networks

1. JOHDANTO

1.1. Työn taustaa

Ambient Networks -konseptissa on kyse eri verkkojen välisestä yhteensopivuudesta, jolla pyritään mahdollistamaan verkon saatavuus käyttäjälle riippumatta käyttäjän sijainnista. Käyttäjällä tulee olla mahdollisuus päästä haluamiinsa palveluihin riippumatta siitä, minkä operaattorin asiakas käyttäjä on (Campos, Rui. Kappler, C. Pinho, C. Pöyhönen, P. Ricardo, M & Ruela, J 2005).

Jotta verkkojen yhteensopivuutta pystyttäisiin parantamaan, kehitettiin sitä varten Euroopan komission rahoittama Ambient Networks -projekti. Projekti aloitettiin 2004 ja se sai nimekseen IST Ambient Networks Project (Campos, Rui. Kappler, C. Pinho, C. Pöyhönen, P. Ricardo, M & Ruela, J 2005). Sen ideana on, että käyttäjät voisivat aina olla yhteydessä toisiinsa ja sitä kautta ulkomaailmaan. Se pyrkii ratkaisemaan kaikki tekniset ongelmat liittyen verkkojen vaihtamiseen. Ideana on se, että Ambient Networks -konseptin avulla pystytään poistamaan kaikki rajoitukset verkkojen välillä johtuen niiden käyttämästä erilaisesta radioteknologiasta, ympäristöstä ja erilaisista palveluista. Kaikki verkot toimisivat saumattomasti keskenään, eikä ainakaan radiotekniikka rajoittaisi viiveetöntä siirtoa verkosta toiseen. Tarkoitus on rakentaa olemassa olevan verkon päälle eräänlainen ohjelmistolla toimiva infrastruktuuri, jolla verkkojen välistä yhteistyötä voidaan parantaa. AN:n (Ambient Networks) ideana ei ole kehittää kokonaan uusia tiedonsiirtotapoja, vaan kehittää olemassa olevia tekniikkoja tehokkaimmaksi. Erityinen painopiste tulee olemaan liiketoimintasuhteiden kehittämisessä eri markkinatoimijoiden kesken. Operaattoreiden tulee kilpailla keskenään, mutta jatkossa myös yhteistyön merkitys kasvaa. Tämä on mahdollista erilaisilla lyhyen ja pitkän aikavälin sopimuksilla, joita markkinatoimijat keskenään laativat, kun haluavat liittyä toiseen verkkoon ja käyttää sen palveluja. Tämän kaiken pitäisi tapahtua automaattisesti lennossa ilman että käyttäjä kiinnittää siihen mitään huomiota, eikä käyttäjän tarvitsisi itse manuaalisesti konfiguroida tarvittavia asetuksia.

AN-projekti piti sisällään kaksi vaihetta, joista ensimmäinen kesti kaksi vuotta (2004–2005). Se sisälsi sovellusarkkitehtuurin määrittelyn, jossa luotiin eräänlainen AN-hallintatila (Ambient Control Space), joka mahdollisti eri verkkojen liittymisen toisiinsa ja piti sisällään lukuisia eri toiminnallisuuksia liittyen muun muassa tiedon siirrettävyyteen, tietoturvaan, laadun valvontaan ja pääsyhallintaan. Toisessa vaiheessa (2006–2007) arvioitiin ensimmäisen vaiheen tuloksia. Siinä luotiin hallintatila-prototyyppi, jota käytettiin AN-projektin ensimmäisessä vaiheessa luotujen komponenttien testaamiseen ja selvitettiin AN-konseptin todellinen hyödyllisyys (Campos, Rui. Kappler, C. Pinho, C. Pöyhönen, P. Ricardo, M & Ruela, J 2005).

1.2. Työn tavoitteet ja rajaus

Työn tavoitteena on tutkia, mitä tarkoitetaan Ambient Networks:illä ja miksi se on niin tärkeä päivitys nykytekniikkoihin sekä mitä lisäarvoa se tuo yritykselle ja tavalliselle kuluttajalle. Työn tarkoituksena on tuoda esille asioita, joita ei välttämättä ole koskaan aiemmin osattu ajatella tai edes vaatia nykyverkoilta. Työssä testataan käytännön tasolla, miten verkkojen yhteistoiminta toimii nykytekniikoilla ja mikä on AN:n tuottama lisäarvo verkkojen yhteensopivuudelle. Työssä pääpaino tulee olemaan nimenomaan konseptissa ja AN-projektissa, mitä siinä saatiin aikaan ja miten AN:ää sovelletaan liiketoimintaympäristössä. Työn ulkopuolelle rajataan se problematiikka, että miten esimerkiksi tietoturva pitäisi tarkalleen ottaen toteuttaa eri verkkojen välillä tai miten sovelluksia pitäisi kehittää, jotta ne toimisivat eri laitteissa eri verkoissa lennosta. Lisäksi 4G:tä ei työssä analysoitu sen tarkemmin, koska pääpaino oli nimenomaan 3G:ssä AN-projektissakin.

1.3. Työn toteutustapa

Työ toteutettiin käymällä aluksi läpi eri verkkotekniikkoja ja topologioita, joiden avulla laitteet voivat kommunikoida keskenään. Sen jälkeen siirryttiin käsittelemään muita peruskäsitteitä kuten verkkolaitteita, OSI-mallia ja verkkoympäristöjä, joissa laitteet voivat kommunikoida keskenään sekä eri verkkotyyppejä. Lisäksi työssä käydään läpi sekä 3G- ja WLAN-tietoturva perusteellisesti. 3G-tietoturva on lainattu tekijän kandidaatin tutkielmasta ”Matkapuhelinverkkojen tietoturva” (Takala 2012).

Jotta nämä verkot voisivat toimia tiiviisti yhteistyössä, niin täytyy varmistaa, että tietoturva-asiat ovat kunnossa ainakin näiden verkkojen sisällä ennen kuin voidaan harkita niiden välistä tiivistä yhteistyötä. Pääaihe tulee käsittelemään AN-visiota ja sen soveltamista liiketoimintaympäristössä. AN-projektin vaiheita tullaan käymään melko tarkasti läpi ja erityisesti AN:n ydintä eli hallintatilaa, sen sisältämiä funktioita sekä niiden merkitystä tullaan analysoimaan työssä. Lisäksi kerrotaan, miten tällainen verkkojen yhdistyminen tapahtuu. Lopuksi työssä esitellään asiantuntijoiden arviointia AN-konseptin hyödyllisyydestä käyttäen heidän kehittelemäänsä hallintatilan prototyyppiä eri komponenttien testaukseen eri skenaarioissa, joissa päätelaitteet kommunikoivat keskenään (Akhtar, Nadeem. Bria, A. Jennen, R. Markendahl, J. Miozzo, M. Pöyhönen, P. Rembarz, R & Simon, C 2007).

Lisäksi tässä työssä testataan tekijän toimesta, miten päätelaitteet tällä hetkellä onnistuvat kommunikoimaan keskenään ja kuinka paljon vaaditaan käyttäjältä toimenpiteitä, jos laitteet laitetaan kommunikoimaan keskenään joko Bluetoothin, WLAN:in tai 3G:n välityksellä. Työssä testataan, aiheuttavatko eri radiotekniikat tai käyttöjärjestelmät ongelmia ja miten onnistuu siirtyminen verkosta toiseen Internetin jakoa hyödyntäen. Työssä tullaan käyttämään kolmea erityyppistä päätelaitetta, joissa jokaisessa on eri käyttöjärjestelmä ja laitteiden välistä vuorovaikutusta testataan eri skenaarioissa. Lopuksi tekijä tekee oman henkilökohtaisen arvion AN:n hyödyllisyydestä.

2. TIETOLIIKENTEEN PERUSKÄSITTEET

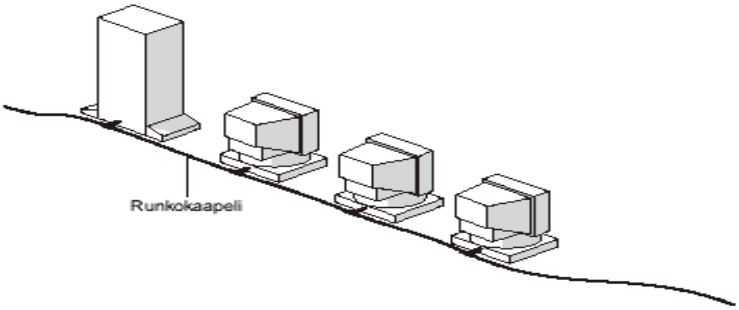
Aluksi käsitellään tietoliikenteen perusteet karkeasti, jotta voidaan myöhemmin ymmärtää paremmin käsiteltyä aihetta, terminologiaa ja sisäistää yleisesti, millä tavoin tieto yleensä verkossa liikkuu. Työssä käydään läpi lyhyesti verkkotopologiat, tiedonsiirtotavat, eri verkkoelementit ja OSI-malli. Langattomien teknologioiden ohella luodaan lyhyt katsaus myös langallisiin.

2.1. Verkkotopologiat

Verkon topologialla tarkoitetaan laitteiden tapaa kytkeytyä verkkoon. Voidaan puhua kahdenlaisista topologioista: rakenteellisista ja loogisista. Rakenteellinen topologia voi poiketa loogisesta rakenteesta jossain määrin. Perustopologioita kiinteässä verkossa ovat rengas, tähti, väylä sekä mesh. Langattomien verkkojen yhteydessä käytettäviä protokollia ovat vuorostaan ad hoc, BSS (Basic Service Set) ja ESS (Extended Service Set). Työssä tullaan keskittymään pääsääntöisesti langattomiin tekniikkoihin ja erityisesti ad hoc:iin.

2.1.1. Väylätopologia

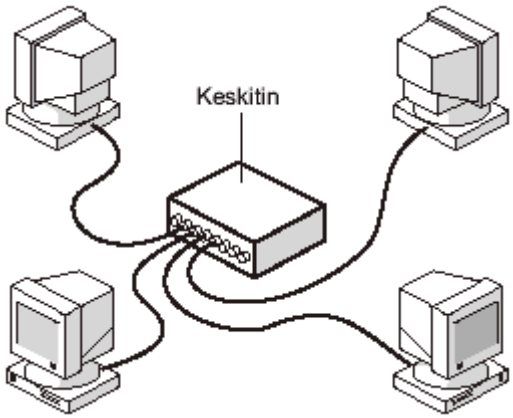
Väylätopologiassa tietokoneet on yhdistetty yhteen kaapeliin. Viesti lähetetään kaikille väylässä oleville koneille, mutta ainoastaan vastaanottava kone hyväksyy sen. Väylän pituus on rajoitettu kaapelin ominaisuuksien vuoksi, joten tarvitaan toistin kaapeleiden välille. Väylässä ainoastaan yksi tietokone kerrallaan voi lähettää tietoa ja kaikki väylään liitetyt tietokoneet voivat kuulla väylälle lähetetyn datan. Päätevastus laitetaan kaapelin päähän absorboimaan signaalia, jotta vältyttäisiin heijastuksilta. Väyläratkaisussa tietokoneet eivät välitä muiden tietokoneiden tiedonsiirrosta. Mikäli yksi kone lakkaa toimimasta, niin sillä ei ole vaikutusta muuhun verkkoon (Oulun kauppaoppilaitos 2004).



Kuva 1. Väylätopologia (Oulun kauppaoppilaitos 2004).

2.1.2. Tähtitopologia

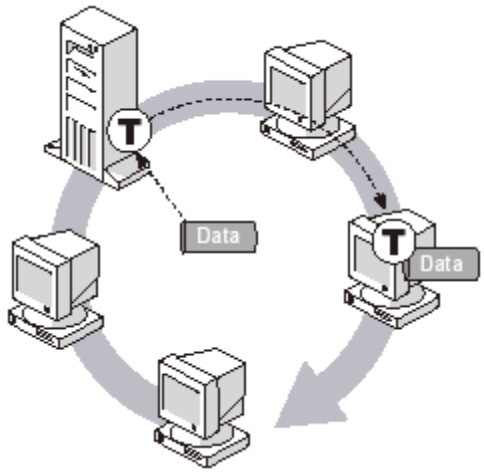
Tähtitopologiassa tietokoneet on kytketty toisiinsa keskittimen välityksellä. Signaali välittyy sen kautta kaikkiin verkon tietokoneisiin. Mikäli keskitin hajoaa, niin se aiheuttaa koko verkon kaatumisen. Toisaalta yhden koneen hajoaminen ei vuorostaan aiheuta ongelmaa verkon muille koneille. Nykypäivänä voidaan käyttää myös keskittimen sijasta kytkintä. (Oulun kauppaoppilaitos 2004). Myöhemmin käydään läpi verkkoelementit osiossa, mitä keskittimellä ja kytkimellä tarkoitetaan ja mitä eroa niillä on.



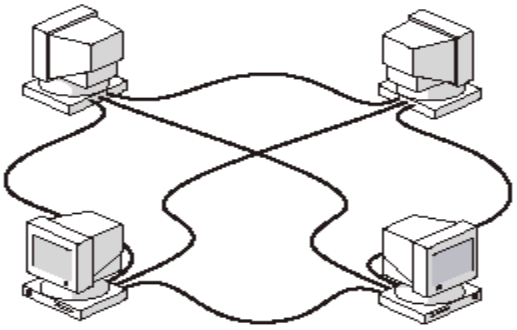
Kuva 2. Tähtitopologia (Oulun kauppaoppilaitos 2004).

2.1.3. Rengas- ja mesh-topologia

Rengastopologiassa tietokoneet on kytketty toisiinsa rengasmaisella tavalla. Rengasverkossa ei ole väyläverkon tapaan päätevastuksia. Tietokoneet toimivat ringissä toistimina vahvistaen signaalia ja välittäen tietoa koneelta toiselle. Yleinen tapa välittää tietoa renkaassa on vuoromerkin käyttäminen. Vuoromerkin avulla tiedetään, millä koneella on oikeus lähettää tietoa. Huonona puolena vuoromerkkiperusteisessa rengastopologiassa on se, että mikäli useampi koneista vioittuu väärästä kohtaa, niin koko verkko voi kaatua. Riippuen rengastopologian tyypistä, voi olla myös mahdollista, että renkaan puoliskot jatkavat toimintaa normaalisti, vaikka yksi kone kaatuisikin. Mesh-topologialla tarkoitetaan lyhyesti sitä, että jokaisesta toimilaitteesta on yhden tai useamman linkin suora polku toiseen laitteeseen (Oulun kauppaoppilaitos 2004).



Kuva 3. Rengastopologia (Oulun kauppaoppilaitos 2004).



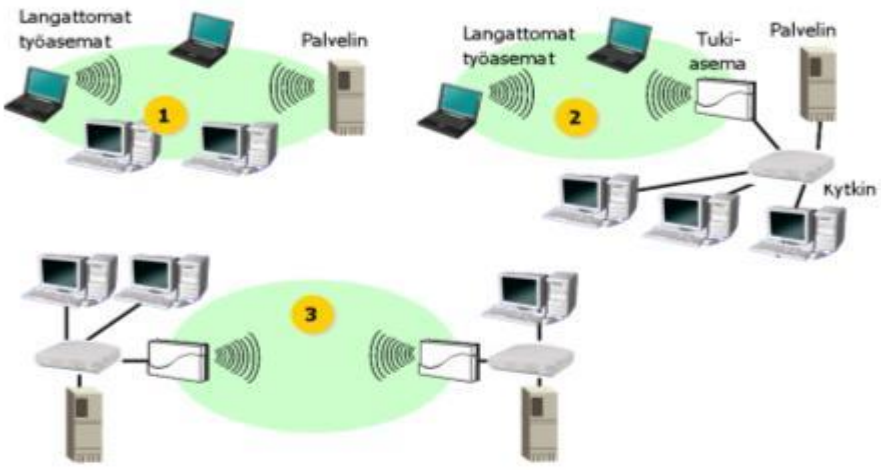
Kuva 4. Mesh-topologia (Oulun kauppaoppilaitos 2004).

2.1.4. Ad hoc -verkko

Ad hoc -verkolla tarkoitetaan laitteiden yhdistämistä toisiinsa ilman tukiasemaa. Kaikki laitteet, jotka ovat kantaman sisäpuolella, voivat kommunikoida keskenään. Ad hoc-verkko on dynaaminen, joten se voidaan pystyttää lähes minne tahansa ja siihen on helppo kytkeytyä ja poistua (Tukiainen 2005).

2.1.5. Basic Service Set

BSS-verkossa tukiasema muodostaa verkon kattavuusalueen. Tällä tapaa toimivat esimerkiksi matkapuhelinverkon tukiasemat. Tukiasemasta on yhteys Internetiin tai muihin palveluihin lähiverkossa. Se voi olla myös yhteydessä toiseen tukiasemaan muodostaen laajemman verkon, josta käytetään lyhennettä ESS (Extended Service Set). ESS-verkko muodostuu kahdesta tai useammasta tukiasemasta. Tukiasemat voidaan yhdistää toisiinsa langallisesti tai langattomasti (Tukiainen 2005).



Kuva 5. WLAN-topologiat (Tukiainen 2005).

2.3. Verkkoelementit

2.3.1. Keskitin

Keskittimet toimivat tiedon välittäjinä eri tietokoneiden välillä. Tietokoneet liitetään keskittimeen Ethernet-kaapelilla ja kaikki tieto kulkee keskittimen kautta. Keskitin ei

tiedä, miltä koneelta tieto tulee ja minne se menee, joten se kopioi ja lähettää saamansa viestin kaikkiin tietokoneisiin. Keskitin ei voi lähettää eikä vastaanottaa tietoja samanaikaisesti. Kytkimiin verrattuna keskittimet ovat edullisempia ja yksinkertaisempia, mutta samalla myös hitaampia (Microsoft 2012).

2.3.2. Kytkin

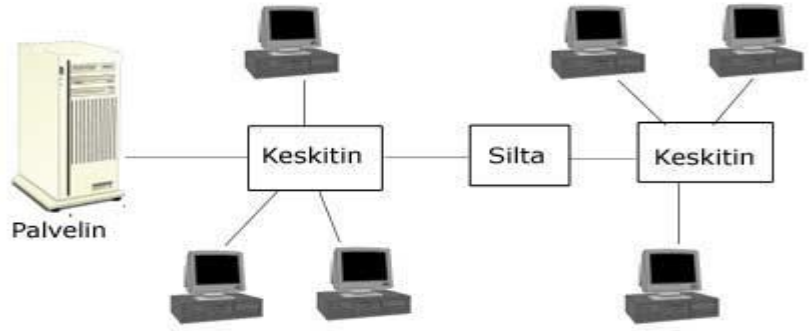
Kytkimet ovat samantyylisiä kuin keskittimet, mutta ne ovat älykkäämpiä. Kytkimet osaavat kohdistaa viestit oikeille vastaanottajille ja pystyvät vastaanottamaan ja lähettämään sanomia samanaikaisesti. Ne ovat nopeampia kuin keskittimet ja sopivat paremmin runsaaseen tiedonsiirtoon. Ne ovat kuitenkin keskittimiä hintavampi vaihtoehto (Microsoft 2012).

2.3.3. Toistin

Toistimet vahvistavat niiden kautta kulkevia signaaleja ja pyrkivät pitämään signaalin voimakkuuden alkuperäisen suuruisena. Toistimia tarvitaan silloin, kun etäisyydet kasvavat kohtuuttoman suuriksi. Aikaisemmin todettiin, että rengastopologiassa tietokoneet toimivat toistimina (Tietoverkot 2012).

2.3.4. Silta

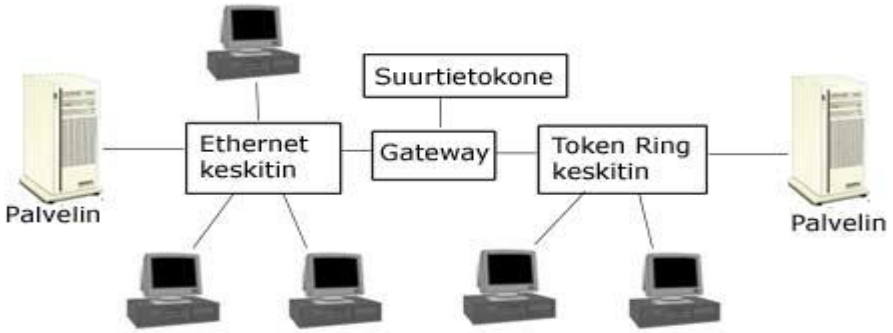
Sillan (bridge) avulla kaksi verkkoa voidaan liittää yhteen. Se voi sisältää suorittimen, mutta sillä ei ole verkko-osoitetta. On olemassa myös sillan ja reitittimen yhdistelmä, jota kutsutaan siltareitittittimeksi (brouter). Sen etuna on nopeus ja monipuolisuus perinteiseen siltaan verrattuna (AK media 2012).



Kuva 6. Verkkojen välinen silta (Tietoverkot 2012).

2.3.5. Yhdyskäytävä

Yhdyskäytävää tarvitaan, kun yhdistetään useampia isoja verkkoja toisiinsa. Se voi toimia reitittimen tavoin, jolloin se tarvitsee suorittimen ja verkko-osoitteen kaikkia siihen liitettyjä verkkoja varten. Yleisimmin keskittimiä näkee käytettävän mobiilisovelluksissa, joissa välitetään liikennettä perinteisen TCP/IP-verkon (Transmission Control Protocol, Internet Protocol) ja mobiiliverkon välillä (AK media 2012).



Kuva 7. Verkkojen välinen yhdyskäytävä (AK media 2012).

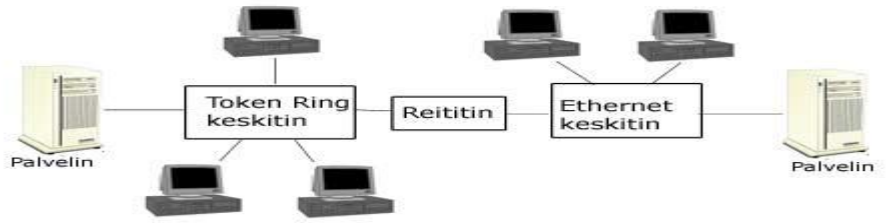
2.3.6. Tukiasema

Tukiasemien avulla voidaan muodostaa yhteys langattomasti langalliseen verkkoon. Ne toimivat kuin matkapuhelinten tukiasemat, johon päätelaitteet voivat ottaa langattomasti yhteyksiä ja mahdollistavat päätelaitteen vapaan liikkuvuuden. Tukiasemaan otetaan yhteys esimerkiksi kahviloissa, lentokentillä tai hotellissa, kun halutaan muodostaa yhteys langattomaan verkkoon. Langattoman lähiverkon (IEEE 802.11) tukiasemissa on yleensä silta ja reititin (Microsoft 2012).

2.3.7. Reititin

Reititin yhdistää toisiinsa kaksi erilaista verkkoa. Mikäli toiseen verkkoon ilmaantuu häiriöitä, voidaan liikenne ohjata toiseen verkkoon reitittimen avulla. Reitittimellä on

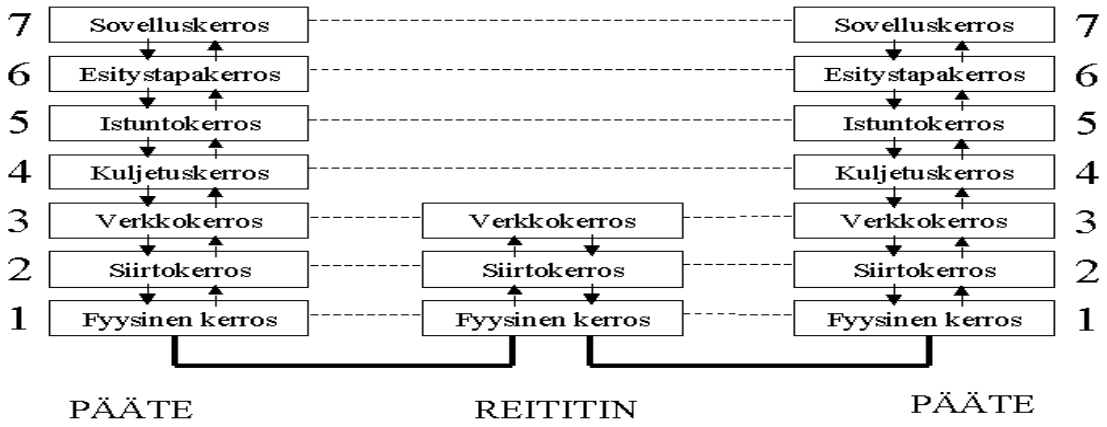
verkko-osoite ja se tarvitsee suorittimen signaalien muuttamiseen eri verkkojen välillä. (AK media 2012).



Kuva 8. Verkkojen välinen reititin (AK media 2012).

2.4. OSI-malli

OSI-malli (Open Systems Interconnection Reference Model) kehitettiin aikanaan 1980-luvulla kansainvälisen standardointiorganisaation ISO:n (International Organization for Standardization) toimesta (LTY 2000). Sen tarkoituksena oli parantaa yhteensopivuutta eri verkkojen välillä ja helpottaa niiden suunnittelua. Se on melko raskas malli ja siitä syystä sitä käytetään lähinnä referenssipinona. Siitä huolimatta OSI-mallin ymmärtäminen helpottaa myös muiden mallien sisäistämistä, sillä siitä on otettu paljon vaikutteita myös muihin malleihin. OSI-malli koostuu seitsemästä eri kerroksesta, joista jokainen on itsenäinen kokonaisuus. Tämä mahdollistaa sen, että jokaista kerrosta voidaan kehittää siten, että se ei vaikuta muihin kerroksiin. OSI-malli toimii siten, että jokainen kerros on yhteydessä vastaavan nimiseen kerrokseen toisessa päässä. Jokainen kerros lisää myös oman otsikkonsa dataan sitä mukaa, kun siirrytään kerrokselta toiselle. Tämä on havainnollistettu kuvassa 9.



Kuva 9. OSI-malli (LTY 2000).

Kummatkin päätteet voivat olla esimerkiksi tietokoneita ja keskimmäinen elementti voi kuvata esimerkiksi reititintä. Kerrokset on nimetty alimmasta alkaen fyysinen-, siirto-, verkko-, kuljetus-, istunto-, esitystapa- ja sovelluskerros. Kerrokset voidaan jakaa myös kolmeen eri pääluokkaan. Kolme alinta kerrosta käsittelevät tiedon reitittämistä ja siirtämistä, kerros neljä tarjoaa siirto-ominaisuudet vastapuolelle verkon yli ja 5-7 kerrokset toimivat palveluntarjoajina sovelluksille (LTY 2000). Kerrosten tehtävät ovat seuraavat:

Fyysinen kerros:

Fyysinen kerros hoitaa varsinaisen bittien välityksen. Fyysisessä kerroksessa määritellään muun muassa modulointitapa kuten esimerkiksi taajuusmodulaatio tai amplitudimodulaatio sekä niiden eri toteutustavat ja rajapinta siirtotiehen, joka voi olla esimerkiksi koaksiaalikaapeli tai radiolähetin. Modulaatiolla tarkoitetaan signaalin yhdistämistä toiseen signaaliin, jota kutsutaan kantoaalloksi. Fyysinen kerros vastaanottaa siirtokerrokselta bittijonon, joka välitetään siirtotielle tietyllä tavalla (LTY 2000).

Siirtokerros:

Tämä kerros muodostaa kehyksen, joka sisältää dataa verkkokerrokselta. Siirtokerros vastaanottaa bittijonon fyysiseltä kerrokselta ja hoitaa virheentarkastuksen. Siirtokehys

toteuttaa virheentarkastuksen jakamalla verkkokerrokselta saadun datan kehyksiin ja antaa niille tietyt tunnukset. Reaktio virheellisiin kehyksiin voi sitten olla erilainen eri tapauksissa. Mikäli havaitaan virheellinen kehys, niin se joko tuhotaan tai pyydetään uudelleenlähetystä. Kun siirretään esimerkiksi liikkuvaa kuvaa, jokaisen kehyksen virheetön siirto ei ole oleellista, vaan oleellisempaa on bittivirran tasaisuus. Virheettömän tiedonsiirron kriittisyys vaihtelee sovelluksittain (Colliander 1999).

Mikäli virheetön bittivirta halutaan toteuttaa, niin vastaanottajan täytyy jollakin tavalla pystyä kuittaamaan saamaansa kehykset, jotta lähettäjä tietäisi kehyksen perillemenosta. Tämä voidaan toteuttaa eri tavoilla riippuen siitä, onko kyseessä yksi- vai kaksisuuntainen yhteys. Mikäli kyseessä on kaksisuuntainen yhteys, niin kuittaukset voi liittää samaan pakettiin lähetettävän kehyksen kanssa. Mikäli kyseessä on yksisuuntainen tiedonsiirto, niin joudutaan käyttämään erillisiä kuittauskehyksiä.
Siirtokerroksen täytyy myös varmistaa bittivirran sopiva nopeus, jottei lähettäjä ylikuormita vastaanottajan puskuria ja näin aiheuta kehysten hukkumista. Tämä hoidetaan usein kuittausten yhteydessä (Colliander 1999).

Verkkokerros:

Verkkokerros pitää huolen pakettien reitityksistä. Se käyttää hyväksi osoitetietoja, joiden perusteella verkkokerros tietää, mille laitteelle tietoa välitetään. Verkkokerros hyödyntää kuljetuskerrokselta saamaansa informaatiota. Aiemmin todettiin, että siirtokerros jakaa datan kehyksiin, mutta verkkokerros toimii toisin ja jakaa tiedon paketteihin. Reitittämisessä hyödynnetään erilaisia reititystauluja. Riippuen tilanteesta reititystaulut voivat olla dynaamisia eli muuttuvat koko ajan verkon kuormituksen mukaan tai harvoin muuttuvia. Verkkokerros pitää huolen myös erilaisten aliverkkojen yhdistämisestä. Ongelmina saattaa olla muun muassa liian isot paketit tai erilaiset osoiterakenteet. Joka tapauksessa nämä ovat kaikki verkkokerroksen vastuulla (Colliander 1999).

Kuljetuskerros:

Kuljetuskerros tarjoaa puitteet tiedon välitykseen kahden järjestelmän välillä. Se pilkkoo istuntokerrokselta saamansa tiedon tarvittaessa pienempiin yksiköihin ja pitää huolen siitä että ne saapuvat oikeassa järjestyksessä vastaanottajalle, jos näin vaaditaan. Myös kuljetuskerroksen tärkeimpiin tehtäviin kuuluu siirtonopeuden säätäminen, jottei hidas vastaanottaja hukkaisi tietoa.

Kuljetuskerros voi järjestää erityyppisiä yhteyksiä eri tarpeisiin eli puhutaan yhdeydellisestä yhteydestä (TCP) ja yhteydettömästä yhteydestä (UDP). Yhteydellinen yhteys on hitaampi kuin yhteydetön, mutta samalla kuitenkin varmempi yhteys, sillä siinä varmistetaan että vastaanottajan saama data on ehyt, kun taas yhteydettömässä yhteydessä ei voi olla varma tiedon perille menosta ja virheettömyydestä. Riippuu tilanteesta, kumpaa yhteyttä käytetään. Kuljetuskerros voi myös järjestää useita verkkokerroksen yhteyksiä, jos tarvitaan suurta nopeutta, mutta se voi myös yhdistää monet ylempää tulevat yhteydet yhdeksi verkkokerroksen yhteydeksi, jos yhteydet ovat esimerkiksi kalliita (Colliander 1999; LTY 2000).

Istuntokerros:

Istuntokerros järjestää istunnon kahden eri järjestelmän välille. Sen vastuulla ovat yhteydenmuodostus sekä sen ylläpito ja lopetus. Istuntokerros pitää myös huolen siitä, että mikäli yhteys katkeaa esimerkiksi häiriön takia, voidaan istuntoa jatkaa siitä mihin jäätiin. Istuntokerros on vastuussa myös kahden järjestelmän välisestä keskustelusta. Tietoa voidaan lähettää joko samanaikaisesti tai vuorotellen. Voidaan myös sopia niinkin, että toinen ainoastaan lähettää ja toinen hoitaa pelkästään vastaanottamisen (LTY 2000).

Esitystapakerros:

Esitystapakerros vastaa nimensä mukaan tiedon esitystavasta. Tiedonsiirtoon liittyvät toiminnot eivät kuulu enää esitystapakerrokselle. Sen vastuulla on, millaisessa muodossa välitettävä data esitetään kuten erilaiset merkistöt ja kuvaformaatit. Esitystapakerros hoitaa myös salausta ja muun muassa PGP-salaus (Pretty Good Privacy) toimii tällä kerroksella (Colliander 1999).

Sovelluskerros:

Sovelluskerros tarjoaa verkkopalveluja sovelluksille. Esimerkki tällaisesta on sähköpostin siirtäminen, tiedoston siirto ja etäkäyttö. Se tarjoaa erilaisia protokollia sovelluksille. Protokollalla tarkoitetaan lyhyesti ohjesääntöä, joka määrittelee tai mahdollistaa laitteiden tai ohjelmien väliset yhteydet. Protokollat mahdollistavat yhteyden päätelaitteisiin. Sovelluskerros toimii rajapintana sovellusten ja OSI-maailman välillä (LTY 2000).

2.5. Verkon toimilaitteet

Verkon toimilaitteilla tarkoitetaan päätelaitteita, jotka käyttävät erilaisia tietoliikenneverkkoja hyväkseen. Tässä työssä kiinnitetään erityinen huomio langattomia verkkoja hyödyntäviin päätelaitteisiin. Näitä toimilaitteita ovat muun muassa kannettavat tietokoneet, taulutietokoneet (tabletit), nettitikut, matkapuhelimet, Blu-ray-soittimet ja televisiot. Aikaisemmin langattomia tietoliikenneverkkoja hyödyntäviä toimilaitteita ei ollut kovin montaa, mutta nykyään etenkin langattomia mobiiliverkkoja (3G) ja WLAN:ia hyödyntäviä laitteita on ilmaantunut markkinoille. Tämä johtuu erityisesti 3G-verkkojen yleistymisestä, ja nykyään on todella paljon erilaisia WLAN-tukiasemiakin ympäri kaupunkia. Nykypäivänä lähestulkoon kaikki uudet älypuhelimet ja myös tavalliset matkapuhelimet osaavat hyödyntää nopeampaa datasiirtoa. Myös 4G, joka on neljännen sukupolven matkapuhelinverkko, tekee kovaa

vauhtia tuloaan. Päätelaiteet voi myös kytkeä langattomasti kotiverkkoonkin, mikäli matkapuhelinverkon kuuluvuus on heikko tai jos haluaa saada tasaisempaa ja nopeampaa tiedonsiirtoa kotiverkossa. Oikeastaan kaikki laitteet, jotka toimivat sähköllä voidaan laittaa verkkoon. Näitä voivat olla tulevaisuudessa esimerkiksi uunit, kahvinkeittimet ja mikroaaltouunit, joita voi hallita etäisesti verkosta käsin.

3. VERKKOPALVELUT

Verkkopalveluilla tarkoitetaan infrastruktuuriverkkoja, joissa nykypäivän yritykset voivat toimia joko yrityksen sisällä tai muiden yritysten kanssa. Nämä verkot ovat Internet, Extranet ja Intranet. Ne pohjautuvat kaikki samaan TCP/IP teknologiaan. TCP/IP on yleinen Internetin tietoliikenneprotokolla, jolla hoidetaan muun muassa kahden päätelaitteen välinen tiedonsiirtoyhteys, pakettien järjestäminen, hukkuneiden pakettien uudelleenlähetys, pakettien osoitteistaminen sekä niiden reitittäminen. Erot Internetin, Intranetin ja Extranetin välillä liittyvät verkkojen kokoon, saatavuuteen sekä hallittavuuteen.

3.1. Internet

Internet on maailmanlaajuinen verkko ja sitä voidaan kutsua myös verkkojen verkoksi. Se pitää sisällään miljoonia paikallisia ja globaaleja verkkoja, jotka on yhdistetty toisiinsa sekä langallisesti että langattomasti. Siihen on pääsy kaikilla IP-osoitteen (Internet Protocol) omaavilla tietokoneilla. IP-osoitteella tarkoitetaan uniikkia osoitetta, joka määrittelee käyttäjän sijainnin. Pääsy Internetiin tapahtuu siten, että kirjoitetaan osoite osoitekenttään esimerkiksi www.uwasa.fi, jonka DNS-palvelin (Domain Name Server) muuntaa IP-osoitteeksi. Sen jälkeen asiakas ottaa yhteyden tietylle palvelimelle, joka kyseisiä sivuja tarjoaa. Kyseinen palvelin ei sijaitse palomuurin alla, mikä erottaa Internetin Extranetistä. Tieto on kaikin tavoin helposti saatavissa. Tietoturvaa saatetaan tietyissä tapauksissa toteuttaa siten, että käyttäjältä kysytään käyttäjätunnusta ja salasanaa (McFarlane 2011).

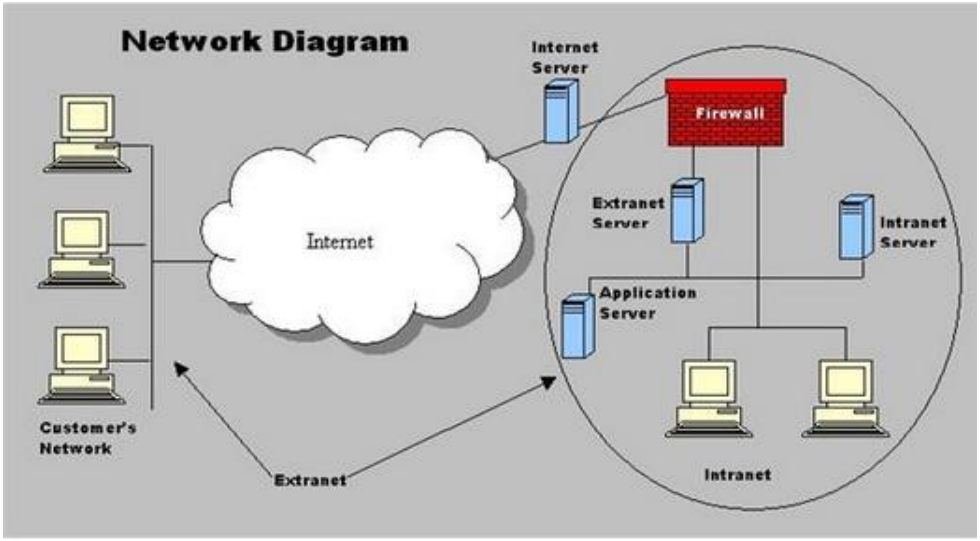
3.2. Intranet

Intranet on verkko, joka ei ole saatavilla ulkopuolisille. Se voi olla esimerkiksi yrityksen oma sisäinen verkko. Mikäli Intranet on yhdistetty Internettiin, tulee verkkojen välillä olla palomuuri käytössä. Jos Intranet sallii liikenteen Internettiin, voidaan sitä kutsua Extranetiksi. Palomuurin avulla pystytään hoitamaan

pääsynhallintaa paremmin ja takaamaan, että esimerkiksi vain yhtiön työntekijöillä on oikeus käyttää verkkoa. Intranet voi yksinkertaisimmillaan koostua vain yhdestä koneesta, jolla ei ole pääsyä Internettiin, mutta pystyy kuitenkin selaamaan sille tarkoitettuja Intranetin sivuja syöttämällä jonkun tietyn komennon osoitekenttään. Intranetin käyttökohteita ovat muun muassa yrityksen ajankohtaisten asioiden tiedotus, tiedostojenjako, työntekijöiden henkilötietojen tietokanta, raporttien jakaminen sekä sähköposti (McFarlane 2011).

3.3. Extranet

Extranet on muuten samankaltainen verkko kuin Intranet, mutta myös ulkopuolisilla on pääsy kyseisen yrityksen verkkoon. Ulkopuolisilla voidaan tarkoittaa esimerkiksi yrityksen alihankkijoita tai sen asiakkaita. Palvelin, joka Internet-sivut tarjoaa, on palomuurin takana. Sen avulla voidaan toteuttaa pääsynhallintaa eri käyttäjien välillä ja tarjota eri sidosryhmille erilaisia oikeuksia. Käyttäjätunnusta ja salasanaa voidaan myös käyttää käyttäjän todentamiseen. Käyttökohteina voidaan pitää samoja asioita kuin Intranetissäkin, mutta lisäksi voidaan olla myös asiakkaaseen päin paremmin yhteydessä ja tarjota ajankohtaista tietoa tuotteista sekä tarjota asiakaspalvelua ja niin edelleen. Tämä säästää muun muassa hallinto- ja matkustelukustannuksia, tarjoaa korkeampaa lisäarvoa asiakkaalle, vähentää paperitöitä ja lisää yleistä tehokkuutta. Haittana on se, että asiakkaaseen ei olla yhteydessä suoraan kasvotusten ja on myös mahdollista, että yritys joutuu huijauksen kohteeksi tai tiedot joutuvat esimerkiksi kilpailijoitten käsiin (McFarlane 2011).



KUVA 10. YRITYKSEN VERKON INFRASTRUKTUURITYYPIT (MCFARLANE 2011).

4. TIETOLIIKENNEVERKOT

Langattomat verkot voidaan jaotella karkeasti kahteen luokkaan: matkapuhelinverkkoihin ja dataverkkoihin. Matkapuhelinverkoissa pääpaino on alun perin ollut puheen ja sms-viestien hyvälaatuisessa siirrossa. Dataverkoissa pääpaino on ollut taas muuntyyppisessä datassa. Nykyisin ero näiden kahden eri verkotyypin välillä on häilyvä ja asteittain katoamassa kokonaan.

4.1. Matkapuhelinverkot

4.1.1. 2G

2G:llä tarkoitetaan toisen sukupolven matkapuhelinverkkoja eli GSM-verkkoja (Global System for Mobile Communications). Erona ensimmäisen sukupolven NMT:hen (Nordisk Mobiltelefon) on se, että signaalit ovat digitaalisia ja tietoturva on parempi. (Tietoturva ei ollut riittävä 2G:ssä ja siitä kerrotaan lisää tietoturvaosiossa) Toinen sukupolvi mahdollisti langattoman tiedonsiirron sekä tekstiviestit ja se palveli laajempaa käyttäjäkuntaa. Datasiirto toteutettiin aluksi piirikytkentäisenä, mutta myöhemmin siirryttiin pakettikytkentäiseen tekniikkaan, jota kutsutaan GPRS:ksi (General Packet Radio Service). Myöhemmin otettiin käyttöön erilaisia laajennuksia (2,5G) kuten EGPRS ja EDGE (Enhanced Data rates for GSM Evolution), jotka nostivat datasiirron suorituskykyä (Korhonen 1999).

4.1.2. 3G

3G:llä tarkoitetaan kolmannen sukupolven verkkoja. Yleisnimityksenä käytetään UMTS:ää (Universal Mobile Telecommunications System). Se mahdollisti entistä suuremmat datasiirtonopeudet, jotka olivat maksimissaan teoriassa jopa 21Mbit/s. Korkeammat siirtonopeudet mahdollistivat perinteisten www-palvelujen sulavamman käytön. Lisäksi pystyttiin käyttämään erilaisia multimediapalveluja sekä soittamaan videopuheluja. 3G tukee myös erilaisia tiedonsiirtonopeuksia sekä asymmetristä tiedonsiirtoa, millä tarkoitetaan sitä, että data siirtyy palveluntarjoajalta käyttäjälle nopeammin kuin käyttäjältä palveluntarjoajalle (Heikkilä 1999).

4.1.3. 4G

3G:n jälkeen kehiteltiin neljännen sukupolven matkapuhelinverkko 4G, joka on vasta hiljattain yleistynyt Suomessa. 4G ei ole samalla tavalla yhteinäinen protokolla tai standardi kuten 2G ja 3G, vaan se on oikeastaan joukko standardeja ja protokollia yhtenäisenä tavoitteena tehokkaampi tiedonsiirto sekä Internet- ja matkapuhelinmaailmojen yhdistäminen. Suomessa käytetään kahta eri termia: LTE (Long Term Evolution) ja DC-HSDPA(Dual Carrier High-Speed Downlink Packet Access). LTE:tä pidetään aitona 4G:nä, jonka maksiminopeus 100Mbit/s ja jälkimmäisempi DC-HSDPA on UMTS:n laajennus, joka käyttää kahta kantoaaltoa. Sen nopeus on maksimissaan 42Mbit/s. Vaikka DC-HSDPA onkin vain 3G laajennus ja käyttää samaa tekniikkaa kuin 3G, on se kuitenkin nykyään määritelty myös 4G-standardiksi (Networkworld 2010).

4.2. Dataverkot

Dataverkot voidaan jakaa kokonsa perusteella eri verkkotyyppeihin. Näillä verkkotyypeillä on keskeinen merkitys, kun puhutaan Ambient Networks:istä. Verkkotyyppejä ovat LAN, MAN, WAN, PAN, BAN ja anturiverkot.

4.2.1. Local Area Network

Local Area Network (LAN), jota kutsutaan lähiverkoksi, yhdistää useita koneita toisiinsa melko lyhyellä kantamalla. Se on yleisin verkkotyyppi. Erilaisten toimistorakennusten, koulujen tai kotitalouksien tietokoneet voivat muodostaa yhden paikallisverkon. Joskus yksittäinen iso rakennus voi sisältää useita paikallisverkkoja ja laajimmillaan ne voivat kattaa useita rakennuksia. Yleensä kaikki tietokoneet kuuluvat samaan IP-avaruuteen. Lähiverkkoa hallitsee yleensä jokin tietty organisaatio tai henkilö (Mitchell 2003).

WLAN:illa (Wireless Local Area Network) tarkoitetaan langatonta lähiverkkoa. WLAN-standardeja ovat 802.11b, 802.11a, 802.11g ja 802.11n. Näiden standardien ominaisuudet on esitelty lyhyesti alapuolella.

- **802.11b:** Nimellinen nopeus on 11 Mbit/s ja toimii vapaalla 2,4 gigahertsin taajuudella.
- **802.11a:** Nimellisnopeus on 54 Mbit/s ja toimii vapaalla 5 gigahertsin taajuudella.
- **802.11g:** Nimellisnopeus on 54 Mbit/s ja toimii vapaalla 2,4 gigahertsin taajuudella.
- **802.11n:** Nimellisnopeus on 600 Mbit/s ja toimii sekä 5 että 2,4 gigahertsin taajuudella (Mitchell 2003).

4.2.2. Metropolitan Area Network

Metropolitan Area Network (MAN) on kaupunkiverkko, jonka kattavuus on lähiverkon ja laajaverkon välillä. Se voi olla suuren yksittäisen organisaation tai kaupungin hallinnoima. Matkapuhelinverkkojen voidaan ajatella olevan myös kaupunkiverkkoja (Mitchell 2003).

4.2.3. Wide Area Network

Tällä laajaverkolla (WAN) tarkoitetaan huomattavasti suurempaa verkkoa kuin mitä LAN on. Internet muodostaa koko maailman kattavan laajaverkon. WAN:in voidaan ajatella koostuvan lukuisista lähiverkoista. Reititin yhdistää lähiverkot laajaverkkoon. Modeemi toimii reitittimenä ja yhdistää käyttäjän palveluntarjoajan välityksellä Internetiin. Reititin ylläpitää listaa sekä laajaverkkojen että lähiverkkojen IP-osoitteista. Laajaverkkoa ei voi hallita pelkästään yksi organisaatio vaan sitä hallitsevat useat eri osapuolet ympäri maailmaa (Mitchell 2003).

4.2.4. Personal Area Network

Personal Area Network (PAN) on lyhyen kantaman likiverkko eli puhutaan vain noin 10 metrin etäisyyksistä. Toisin kuin lähiverkossa, se ei ole suoraan yhteydessä ulkomaailmaan. Yhteys muodostetaan lähinnä toisten toimilaitteiden kesken. Bluetooth on yleisin käytettävissä oleva likiverkko (Mitchell).

4.2.5. Body Area Network

Body Area Network (BAN) tarkoittaa nimensä mukaan kehoalueen verkkoa. Esimerkkinä voidaan mainita esimerkiksi erilaiset sensorit, jotka mittaavat ihmiskehon lämpöä, verenpainetta, sydämen sykettä tai mitä tahansa elintoimintoja. Kaikki nämä tiedot voidaan lähettää reaaliaikaisesti vaikka matkapuhelimeen (Mitchell 2003).

4.2.6. Anturiverkot

Anturiverkot koostuvat useista erilaisista itsenäisistä antureista, jotka mittaavat fyysisiä ja ympäristöön liittyviä ilmiöitä kuten esimerkiksi lämpötilaa, ääntä tai painetta.
Anturiverkot, erityisesti langattomat anturiverkot, ovat lupaava ja nopeasti kasvava tutkimus- ja tuotekehitysalue. Anturiverkkojen yleistymistä ovat edesauttaneet prosessori, anturi- sekä langattomien viestintäteknologioiden nopea kehitys ja hintojen aleneminen. Langattomia sensoriverkkoja voidaan käyttää erityisesti erilaisissa älykkäiden ympäristöjen sovelluksissa, kuten esimerkiksi ympäristön tai taistelukentän valvonta sekä teollisuuden, sairaaloiden ja muiden kiinteistöjen valvonnassa sekä niiden ohjauksessa (Rantala 2006).

5. LANGATTOMIEN VERKKOJEN TIETOTURVA

Langaton tietoliikenne on altiimpi vakoilulle ja datan sieppaamiselle. Käyttäjä voi myös itse vaikuttaa paljon oman tietoturvansa tasoon käyttämällä omaan järkeään. On äärimmäisen tärkeää, että käyttäjä ei hyväksy minkä tahansa sovelluksien asentumista päätelaitteeseensa. Matkapuhelinverkoissa operaattorit ja laitevalmistajat ovat myös pitkälti vastuussa käyttäjän turvallisuudesta. Dataverkoissa käyttäjä voi varmistua parhaiten turvallisuudestaan käyttämällä itse määriteltyä salausta. Seuraavan matkapuhelimen tietoturvaa käsittelevä osio perustuu tekijän kandidaatintutkielmaan ”Matkapuhelinten tietoturva”(Takala 2012).

5.1. Matkapuhelinverkkojen uhat

Mobiilipalvelut ovat yhä tärkeämpi osa tietoverkkoja ja etenkin Internet-palveluja. Analogisissa matkapuhelinjärjestelmissä oli ongelmana radiotien suojaamattomuus. Kuka tahansa pystyi sopivalla laitteistoilla salakuuntelemaan toista henkilöä. GSM-järjestelmässä tietoturva on huomattavasti parempi ja se soveltuu muun muassa sähköpostin käyttöön paremmin. Digitaalisuus tarjoaa tehokkaita mahdollisuuksia suojata puhelut ja estää GSM-puhelimen luvaton käyttö. GSM-verkkoon pätevät samat perussäännöt kuin muihinkin viestintäjärjestelmiin eli suojataso määrää sovelluksen turvatarpeet. GSM-verkon kautta ei tule lähettää liian pitkiä sanomia ja siinä ei saisi käyttää palveluja, joiden turvavaatimukset on erittäin korkeat. GSM soveltuukin paremmin henkilökohtaiseen suojattuun tiedonsiirtoon ja sovelluksiin, missä sanomat ovat lyhytaikaisia ja missä turvavaatimukset ovat kohtuulliset. Digitaalisen GSM-datan siirto on analogisiin verkkoihin verrattuna kohtuullisen ”turvallista”, vaikka dataa ei salattaisi ollenkaan puhekoodauksen, modulation ja kanavavarauksen ansiosta (Kerttula 1998; Heikkilä 1999).

Mobiiliverkot ovat lankaverkkoihin nähden luonnostaan haavoittuvaisempia salakuunteluun perustuville tietoturvahyökkäyksille, koska yhteyksiä voidaan kuunnella ilman erityisjärjestelyjä. Erityisesti analogisissa mobiiliverkoissa (kuten NMT)

tietoturva on aikaisemmin ollut suuri ongelma (Kerttula 1998). Tietoturva-asiantuntija Chris Paget toteaakin Digitodayn artikkelissa ”Kännykän vakoilu onnistuu reilun tonnin laitteilla”, että GSM-puheluiden salakuuntelu onnistuu osista rakennetun salakuuntelulaitteiston avulla. Salakuuntelija voi ohjata puhelun jatkamaan varsinaisen operaattorin tukiasemaan ja oikealle vastaanottajalle, mutta pystyy vakoilemaan kaikkea oman laitteistonsa kautta kulkevaa liikennettä. Pagetin tekniikalla pystyy vakoilemaan kuitenkin vain gsm-verkon kautta kulkevia puheluita ja viestejä, mutta vahvemmin suojatun 3G-yhteyden huijaaminen sillä ei onnistu. Paget toteaakin GSM:n olevan ”rikki” (Digitoday 2010). Ambient Network:issa verkkojen yhteistyö perustuu nimenomaan 3G-tekniikan hyödyntämiseen verkkojen välisessä yhteistyössä, sillä aina pyritään löytämään se paras yhteys. 2G ei nykypäivänä riitä tyydyttämään eri sovellusten tarpeita hitaan tiedonsiirtonsa vuoksi.

Mobiiliverkkojen tietoturva on uhattu radiotiellä, missä voi tapahtua datan sieppaamista ilmarajapinnassa (air interface). Tästä voi aiheutua käyttäjädatan yksilösuojan (luottamuksellisuuden) menetystä, käyttäjän signalointidatan luottamuksellisuuden menetystä tai käyttäjän identiteettisuojan menetystä. Kerttulan mukaan on myös vaarana että käyttäjän palveluita käytetään ilman käyttäjän lupaa vääriin tarkoituksiin (Kerttula 1998).

Tekniikka & Talous lehden artikkelin ”Mobiilitietoturva ei anna aihetta paniikkiin” mukaan käyttäjä pystyy itse vaikuttamaan paremmin mobiililaitteensa tietoturvaan, jos matkapuhelinta vertaa esimerkiksi tietokoneeseen. Toisin kuin tietokoneissa, kännykässä ohjelma ei voi asentua itsestään, vaan käyttäjän pitää hyväksyä toimenpiteet. Palvelunumeroilla rahastaminen on kohtuuhelppo lopettaa alkuunsa, koska operaattori voi sulkea numeron ja estää soitot ulkomaiseen numeroon. Täysin huoleton ei kännykän kanssa kannata olla varsinkaan silloin, jos se sisältää yrityksen kannalta tärkeitä tietoja. Suurin vaara on laitteen kadottaminen (Leino 2005). Nykypäivänä ei mobiiliviruksia vielä hirveästi ole, jos vertaa esimerkiksi Windows-ympäristöön. Yleensä viruksia kehitetään alustoille, jotka ovat laajassa käytössä. Tästä esimerkkeinä mainittakoon PC puolen Windows ja mobiilipuolella Android.

Nykyään matkapuhelinten tietoturvaan kiinnitetään yhtä enemmän huomiota, mutta on selvää, että tekniikka on kallista ja erityisesti edullisimmissa puhelinmalleissa ei pystytä toteuttamaan tietoturvaa riittävän tehokkaasti. Tämä ilmenee muun muassa Taloussanomien Topi Kanniaisen kirjoittamassa artikkelissa ”Sinunkin puhelintasi saatetaan kuunnella”, jossa turvallisuustutkijat Karsten Nohl ja Sylvain Munaut ovat onnistuneet murtamaan toisen myös Suomessa käytetyistä GSM-verkon salausjärjestelmistä. Murrettua tekniikkaa käyttävät halvat ja vanhat puhelinmallit, joissa ei ole riittävää tekniikkaa korkeamman suojauksen pyörittämiseen. Pääsääntöisesti suomalaiset operaattorit tarjoavat puhelimille suojausta, jota ei ole vielä murrettu. Osassa halvoista ja vanhoista puhelimista ei kuitenkaan yksinkertaisesti ole tätä ominaisuutta, jolloin ne käyttävät murrettua suojausmenetelmää, Viestintäviraston tietoturva-asiantuntija Tomi Hasu sanoo. Suomessa käytetään A5/1- ja A5/3-tasoisia suojauksia, joista ykkönen on onnistuttu murtamaan. 3G:ssä tietoturva on kaikin puolin parempi. Vuonna 2007 GSM Association toi saataville 128 bittisen A5/3 –salauksen. Kolmostason suojaus (A5/3) on nyt murrettua suojausta huomattavasti monimutkaisempi, minkä takia sitä on myös hankalampi murtaa ja se on yleistynyt 3G-verkon myötä. Kyseisestä suojauksesta käytetään nimitystä KASUMI (Kanniainen 2011). KASUMI:sta puhutaan myöhemmin lisäää.

Vaikka artikkelissa kovasti säikytelläänkin tavallisia puhelinkäyttäjiä, niin samalla siinä kuitenkin painotetaan, että salakuuntelu on äärimmäisen vaikeaa, vaikka siitä löytyykin hyvät ohjeet Internetistä. Viestintäviraston tietoturva-asiantuntija Tomi Hasu sanookin, että salakuuntelu vaatii, että salakuuntelijan on oltava saman tukiaseman kattavuusalueella, missä puhelinkäyttäjä sijaitsee. Lisäksi tekniikan tohtori Arto Karila painottaa vielä, että kovin moni ei ole kiinnostunut tavallisen ihmisen puheluista (Kanniainen 2011).

5.2 Matkapuhelinverkon autentikointi ja salaus

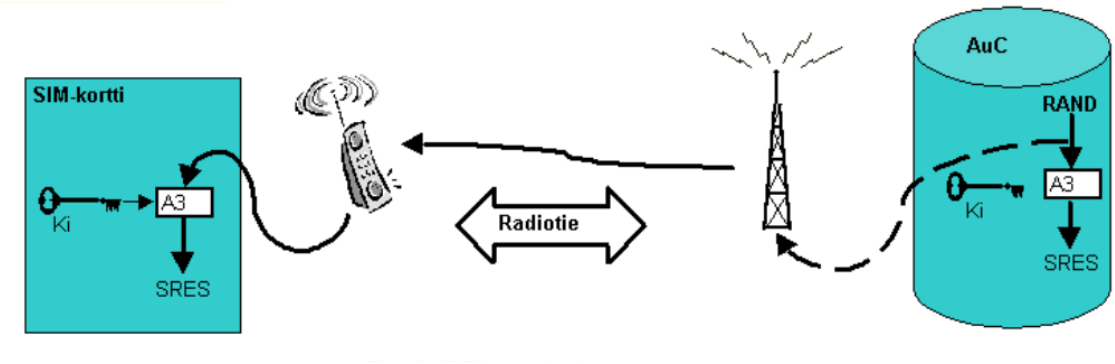
5.2.1 GSM-verkon autentikointi

GSM-verkon yhtenä verkkoelementtinä on tunnistuskeskus AuC (Authentication Centre), jonka tietokannoissa säilytetään tietoturvaan liittyviä tilaajatietoja. Tunnistuskeskuksen tarkoituksena on tutkia onko tilaajan SIM-kortilla oikeus käyttää verkkoa puhelun alkaessa. Oikeuksien tarkistamisessa käytetään parametreja RAND, Ki ja SRES (Heikkilä 1999). GSM-tilaajaan verkkotasoinen autentikointi perustuu haaste/vaste-menetelmään (kts. kuva 11). Menetelmä käyttää hyväkseen 128 bitin RAND-satunnaislukuja (2^128-1) sekä julkistamatonta A3-algoritmia. Periaatteessa A3-algoritmi on julkinen, mutta jokainen operaattori käyttää omaa A3-algoritmiaan. Se ei silti estä verkkojen välistä yhteistoimintaa (Kerttula 1998).

Tunnistuskeskus laskee satunnaisluvun RAND (Random Number), joka lähetetään puhelun alustusmerkinannossa tilaajan SIM-kortille. SIM-kortti laskee RAND:n ja kortilla sijaitsevien salausavaimen Ki ja salausalgoritmin A3 avulla arvon SRES (Signed Response). Tunnistuskeskuksessa, joka tietää tilaajan salausavaimen Ki, lasketaan sama SRES. Näitä kahta laskettua SRES-tulosta verrataan toisiinsa. Jos tulokset eivät täsmää, on joko käyttäjän salausavain Ki tai SIM-kortin A3-algoritmi väärä. Tällöin verkko päättelee kyseessä olevan luvattoman verkon käytön, jonka seurauksena puhelu katkaistaan (Kerttula 1998; Heikkilä 1999). Satunnaisluku RAND vaihtuu jokaisella autentikointikerralla, eikä sen arvoa voi etukäteen määritellä tai ennustaa. Verkon ei tarvitse laskea RAND:ia ja SRES:iä jokaisella yhteydenotolla, vaan AuC voi laskea ne valmiiksi ja tallentaa kotirekisteri HLR:ään (Home Location Register). Sieltä ne voidaan lähettää pyytävälle vierailijarekisterille VLR (Visitor Location Register), jolloin tilaajan autentikointi pystytään suorittamaan. Toiminnon avulla saavutetaan parempi turvallisuus käyttäjän tietojen salaamisessa ja autentikointiavain Ki pystytään pitämään turvassa AuC:ssa (Haavisto 2009).

Autentikoinnin tietoturva on siis avaimen Ki ja algoritmin A3 varassa. Tilaaja ei itse pääse näkemään avainta Ki, mitä säilytetään sekä SIM-kortilla että

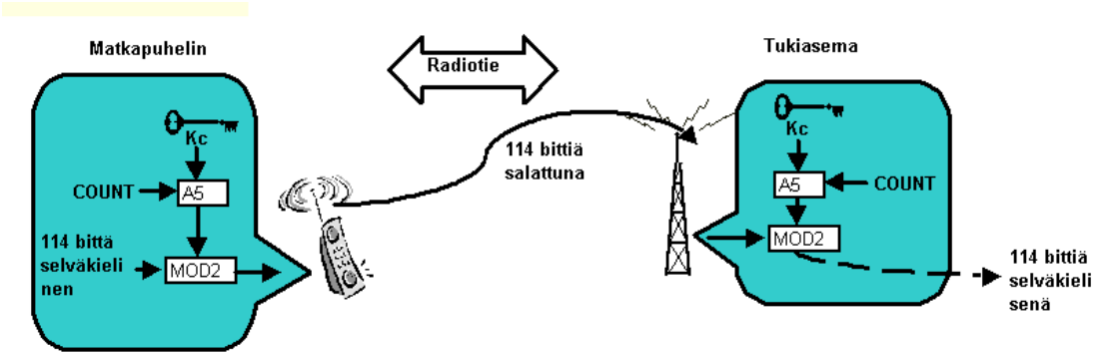
Autentikointirekisterissä AuC. Avainta Ki ei tarvitse koskaan siirtää verkossa (Kerttula 1998).



Kuva 11. GSM-autentikointi (Heikkilä 1999).

5.2.2. GSM-verkon salaus

GSM-verkon salauksen (kts. kuva 12) voidaan ajatella koostuvan kahdesta eri vaiheesta. Salausavaimen Kc generoinnista ja itse salauksesta. Salaus suoritetaan A5-algoritmeilla ja 64-bittisen salausavaimen Kc generointi RAND-luvusta tapahtuu A8-algoritmilla. A8 sijaitsee sekä SIM-kortilla että autentikointirekisterissä. AuC ja Kc on tallennettu sekä SIM-kortille että kotirekisteriin (HLR). Salausavain Kc ja GSM-verkon hyperkehyksessä (hyper frame) oleva kehysten järjestysnumero toimivat siis parametreina salauksessa. Lopputulokseksi saadaan salausjono, jolle suoritetaan modulo-2 laskutoimitus yhdessä salattavan purskeen 114 databitin pituisen lohkon kanssa. Kehysnumero muuttuu jokaisen salattavan lohkon yhteydessä, jolloin kunkin purskeen 114 databitin salauslukujonotkin ovat erilaisia. GSM:ssä voidaan määrittää seitsemän erilaista A5 algoritmia. Niistä kuitenkin kaksi on vain standardoitu A5/1 ja A5/2. A5/0 tarkoittaa siirtoa ilman salausta. Näistä A5/1 on erittäin tehokkaan salauksen omaava ja A5/2 on helpommin purettavissa. Suomessa on käytössä A5/1 mutta maailmalla on operaattoreita, jotka käyttävät A5/2-algoritmia. A5 algoritmi sijaitsee A3- ja A8-algoritmeistä poiketen puhelinlaitteessa eikä SIM-kortilla sekä tukiasemassa, jossa radiotien salaus ja purku tapahtuvat. Tukiasemasta eteenpäin tieto on siis suojaamatonta. Toinen ero verrattaessa algoritmeja keskenään on se, että A5 ei ole julkinen (Kerttula 1998; Haavisto 2009).



Kuva 12. GSM-verkon salaus (Heikkilä 1999).

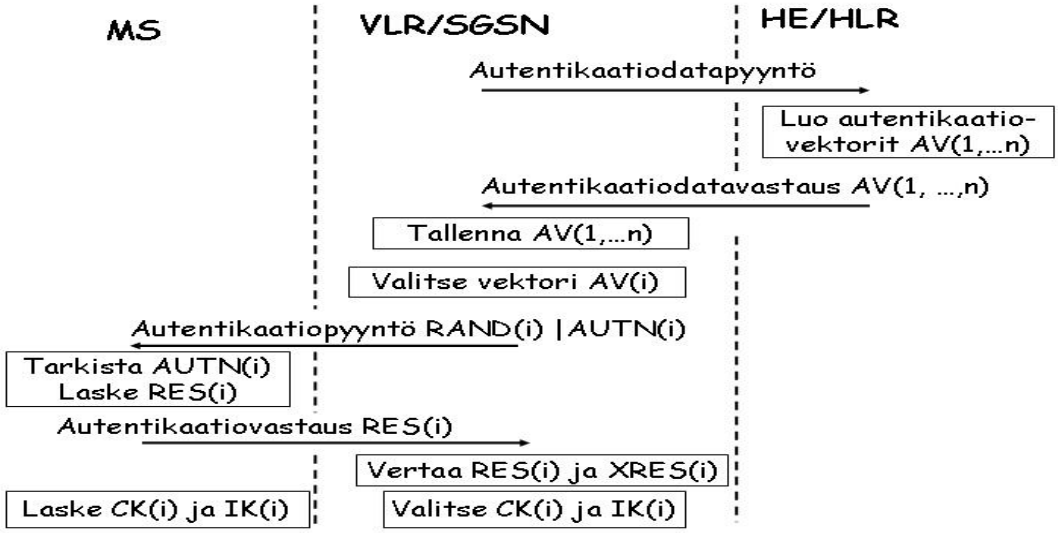
5.2.3. UMTS-autentikointi

UMTS-verkon autentikointi perustuu kättelyviesteihin, kuten GSM-verkossakin, mutta toiminnassa on merkittäviä eroja. GSM-verkossa autentikaation yhteydessä laskettiin todennusvektoreina triplettejä, jotka koostuivat haasteesta RAND, odotetusta käyttäjän vasteesta SRES ja salausavaimesta Kc. UMTS-verkossa käytetään kvintettejä (Vesanen 2003). RAND on 128-bittinen satunnainen haaste, XRES 32-128 bittiä odotettu käyttäjän vaste, CK on 128-bittinen salausavain (Cipher Key), IK on 128-bittinen integrointiavain (Integrity Key) ja AUTN on 128 -bittinen verkon tunniste (Authentication Token) (Vesanen 2003).

3G autentikointiprosessissa on mukana kolme osapuolta, jotka ovat kotiverkko (HLR), palveleva verkko SN (VLR, SGSN) ja päätelaitteen USIM. Autentikointi tapahtuu molemmissa suunnissa, SN (Serving Network) tarkastaa käyttäjän identiteetin, kun taas käyttäjä tarkastaa HLR:ltä, että SN (Service Network) on valtuutettu tekemään autentikointiopyyntöjä (Haavisto 2009).

Autentikointi perustuu salaiseen 128 bittiseen avaimeen K kuten GSM-verkossakin ja sen tulisi sijaita ainoastaan käyttäjän kotiverkon todennuskeskuksessa ja USIM-kortilla. Lisäksi USIM ja kotiverkko ylläpitävät laskureita SQN(HE) ja SQN(MS). Ensin mainittu on jokaiseen käyttäjään verkossa liitettävä laskuri ja viimeksi mainittu USIM:in saama suurin arvo. Näiden avulla voidaan hoitaa autentikointien synkronointi. Autentikoinnin ja avainten luonnin (Authentication and Key Agreement, AKA) yhteydessä sekä käyttäjä että verkko todentavat toisensa ja sopivat käytettävistä avaimista. Käyttäjän kotiverkko luo useita

todennusvektoreita ja lähettää ne käyttäjän sijaintiverkon VLR/SGSN:lle, joka hoitaa autentikoinnin asiakkaaseen seuraavan kaavion (kuva 13) mukaisesti (Vesanen 2003).



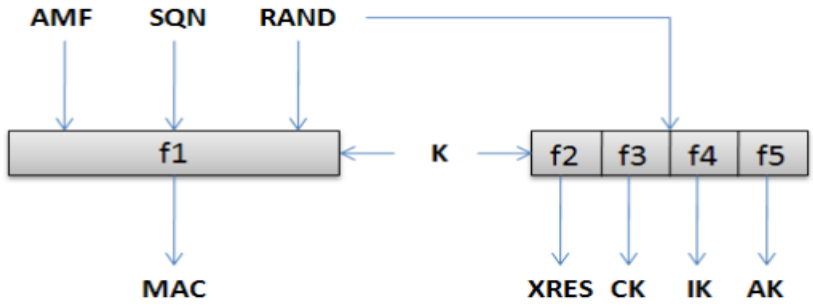
Kuva 13. UMTS-autentikointiprosessi (Vesanen 2003).

Autentikointivektorin laskemisessa käyteään seuraavia parametreja: SQN (Sequence Number) on 48-bittinen kasvava sarjanumero, AMF 16-bittinen autentikointi- ja avaimenhallintakenttä (Authentication and Key Management Field), K ilmaisee 128-bittinen salaista käyttäjäavainta ja RAND on 128-bittinen satunnainen haaste (Vesanen 2003).

Autentikointi alkaa siitä, kun IMSI tai TMSI (Temporary Mobile Subscriber Identity) siirretään SN:LLE, joka puolestaan tekee autentikointipyynnön kotiverkon (HLR:n) autentikointikeskukseen (AuC). Luodakseen autentikointivektorit AuC:in tulee sisältää tieto IMSI:stä (IMSI International Mobile Subscriber Identity) sekä käyttäjien K-avaimet. Autentikointivektorit lähetetään takaisin autentikointidatavastauksena SN:lle (Vesanen 2003).

Saatuaan autentikointivektorit SN tekee autentikointipyynnön päätelaitteelle sisältäen parametrit RAND ja AUTN. Kertauksena RAND oli siis on 128-bittinen satunnainen haaste ja AUTN 128-bittinen verkon tunniste. Näiden parametrien avulla päätelaitteen USIM pystyy suorittamaan autentikointilaskelmat yhdessä salaisen käyttäjäavaimen K:n kanssa. Näiden laskelmien avulla USIM tietää, että verkon tunniste (AUTN) on luotu autentikointikeskuksessa. Mikäli näin on, niin lähetetään parametri RES autentikaatiovastauksena SN:lle. SN vertailee saamaansa RES- ja autentikointivektorin XRES-arvoa keskenään. Mikäli ne ovat samat, niin on autentikointi onnistunut, mutta mikäli ei, niin lähetetään virheilmoitus (Vesanen 2003).

Autentikointivektorien luonti tapahtui kotiverkon autentikointikeskuksessa sekvenssinumeron SQN:n valinnalla. Numero on kasvava luku. Joka kierroksella kasvavalla sekvenssiluvulla varmistetaan, että sitä ei ole käytetty aikaisemmilla kerroilla. Samalla myös luodaan 128-bittinen satunnaisluku RAND. Autentikointivektori lasketaan yksisuuntaisten funktioiden avulla, joita on yhteensä viisi. Funkiot ovat f1, f2, f3, f4 ja f5. f1 eroaa muista funktioista siten, että sen laskemiseen tarvitaan neljä parametria, kun taas muiden funktioiden kaksi. f1:n funktiot ovat AMF (Autentication management field), RAND, SQN ja pääavain K. f2:n, f3:n, f4:n ja f5:n parametrit ovat vain K ja RAND (Vesanen 2003).

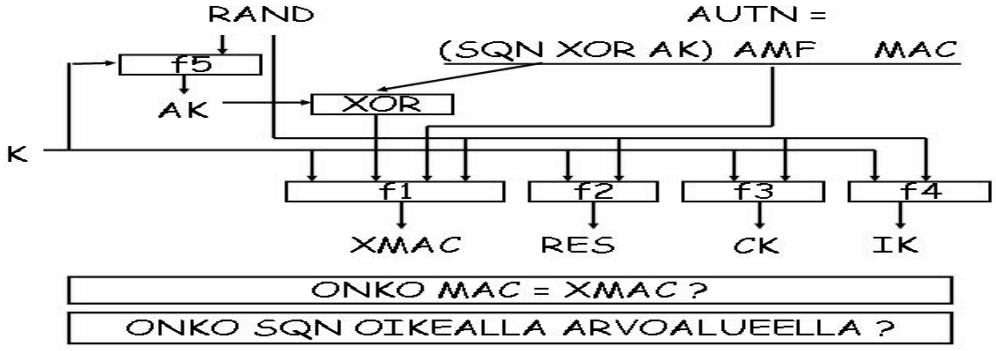


Kuva 14. Autentikointivektoreitten määrittely funktioiden avulla (Haavisto 2009).

Kuva 14 havainnollistaa selkeästi autentikointivektoreiden muodostumisen.
Kuten kuvasta 14 näkyy, niin muodostuu viisi eri lukua: MAC, XRES, CK, IK ja AK.

1. MAC = f1(K, AMF, SQN, RAND) , joka on 64-bittinen luku.
2. XRES = f2(K, RAND), 32-128 bittinen, käyttäjän odotettu vaste.
3. CK = f3(K, RAND), 128-bittinen salausavain.
4. IK = f4(K, RAND), 128-bittinen eheysavain.
5. AK = f5(K, RAND), 48-bittinen anonyymisyysavain.
6. AUTN = (SQN XOR AK) | AMF | MAC, verkon todennusluku.
7. AV = RAND | XRES | CK | IK | AUTN, autentikaatiovektori (Vesanen 2003; Haavisto 2009).

Vektorien luomisen jälkeen suoritetaan autentikointimäärittelyt myös USIM:in puolella. Periaate on sama, mutta vaiheet ovat vähän eri järjestyksessä. f5 on laskettava ensin f1:stä, koska sitä käytetään SQN:n piilottamisessa. Näin toimitessa mahdollinen hyökkääjä ei voi päästä käyttäjän identiteettiin käsiksi. Asia on havainnollistettu kuvassa 15.



Kuva 15. Autentikointivektoreitten luonti USIM-puolella (Vesanen 2003).

1. SN siis muodostaa käyttäjälle todennushaasteen lähettämällä vektorin RAND | AUTN.

2. Vastaanottaja laskee anonyymisyysavaimen AK (Anonymity Key) siitä funktion viisi avulla eli AK = f5(K, RAND).

3. Laskelman avulla vastaanottaja saa selville AUTN:n alkuosasta SQN:n ja varmistuu, että luku ei ole liian vanha. AUTN:n avulla taas voidaan selvittää AMF ja MAC.

4. Seuraavaksi käyttäjä laskee XMAC = f1(K, AMF, SQN, RAND). Jos XMAC=MAC, niin verkko on todentanut itsensä käyttäjälle eli osoittanut tietävänsä avaimen K ja varmistanut, ettei käyttäjä ole valeverkossa.

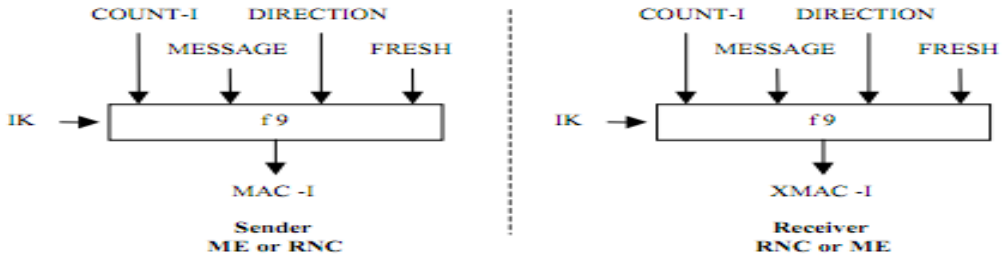
5. Tämän jälkeen käyttäjä laskee vasteen RES = f2(K, RAND) ja lähettää tiedon vasteesta VLR:lle tai SGSN:lle.

6. Vastaanottaja vertaa lukua lukuun XRES ja todentaa käyttäjän. Osapuolet ovat näin todentaneet toisensa ja sopineet avaimista CK ja IK, jotka siis liittyvät funktioihin f3 ja f4 (Vesanen 2003).

5.2.4 UMTS-verkon eheyden suojaus ja salaus

Kun molemminpuolinen autentikointi on suoritettu, toteutetaan seuraavaksi itse salaus. Viestien eheyteen tulee kiinnittää huomiota, joten useimmat kontrolliviestit tulee salata päätelaitteen ja verkon välillä. Eheyden suojaamiseen hyödynnetään algoritmia f9 ja avainta IK kun taas ilmatien salaukseen käytetään algoritmia f8 sekä avainta CK. f8:ssa on lukuisia erilaisia algoritmeja käytettävissä, mutta vain yksi algoritmi nimeltään KASUMI on spesifikoitu (Vesanen 2003).

Eheysalgoritmilla f9 (kts. kuva 16) pyritään varmistamaan, että viesti säilyy alkuperäisenä. Toisin sanoen viestiä ei muokata eikä sitä poisteta mitään. Syitä, miksi eheyden suojaamiseen ja tiedon salaamiseen käytetään eri algoritmeja on useita. Yksi tärkeä syy on se, että ei voida vaatia päätelaitteelta, että kaikki yhteydet toteutettaisiin salatussa tilassa. Jos hyökkääjällä on tarkoitus aiheuttaa vahinkoa ja luoda salaamaton yhteys käyttäjään, niin hyökkäys pystytään estämään eheysalgoritmin avulla. GSM-verkossa ei ole käytössä mitään eheysalgoritmia käytettäessä salaamatonta yhteyttä, joten silloin tiedon eheys saattaa kärsiä. Vaikka pelkkä salausalgoritmikin tarjoaa jonkinlaista suojaa eheyteen, niin yhdessä eheysalgoritmin kanssa voidaan 3G-verkossa suojautua lukuisilta erilaisilta hyökkäystavoilta, joita vastaan oli vaikeampi suojautua GSM-aikana. Yksi hyökkäystavoista on ”bidding-down”, jossa hyökkääjä pakottaa käyttämään vanhaa algoritmia. GSM-verkossa tämä oli erityisesti suuri ongelma, koska algoritmeja oli käytössä useita. (Boman, G. Horn, P. Howard & V. Niemi 2002).



Kuva 16. 3G-verkon eheysalgoritmi f9 (Boman, G. Horn, P. Howard & V. Niemi 2002).

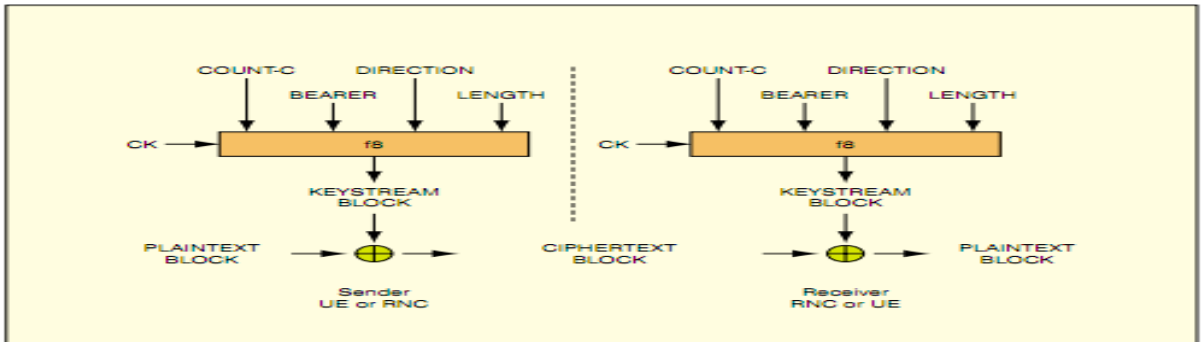
Algoritmin parametrit ovat seuraavat:

- Eheysavain IK, joka on 128 bittiä pitkä.
- Eheyssekvenssiluku (COUNT-I) ja RNC:n luoma satunnaisluku (FRESH) ovat molemmat 32-bittisiä. Yhdessä ne muodostavat toistuvan suojauksen.
- Suunnan ilmaisija (DIRECTION) estää niin sanotut heijastushyökkäykset.
- MESSAGE ilmaisee Radio Resource Control:n (RRC:n) signalointiviestin sisältöä.

Perustuen algoritmin sisääntuloparametreihin lähettäjä laskee 32-bittisen viestin autentikointikoodin dataeheydelle (MAC-I) eheysalgoritmia f9 käyttäen. MAC-I liitetään sitten RRC-viestiin, kun se lähetetään radioteitse. Vastaanottaja laskee odotetun MAC-I:n (XMAC-I) vastaanotetusta viestistä samalla tavalla kuin lähettäjä laski MAC-I:n lähetetystä viestistä ja varmistaa datan eheyden vertamaalla XMAC-I:tä MAC-I:hin. Niiden tulee siis olla yhtä suuret. Eheysominaisuuden lisäksi pystytään myös määrittämään samalla datan alkuperäisyys ja varmentamaan lähettäjän oikeellisuus. Tämä helpottaa myös operaattoreiden työtä, kun ei joka kerta tarvitse yhteyttä muodostaessa suorittaa täyttä autentikointia ja avainten vaihtoa (Boman, G. Horn, P. Howard & V. Niemi 2002;Niemi, Valtteri & Kaisa Nyberg 2003).

Salaus ja salauksen purku tapahtuvat päätelaittessa ja RNC:ssä (Radio Network Controller) verkon puolella. Tieto CK:sta on siis jaettu päätelaitteen ja ydinverkon (CN)

välillä. Jotta salaus voitaisiin suorittaa, niin CK tulee lähettää ydinverkosta UTRAN:ille (UMTS Terrestrial Radio Access Network). Kun RNC on saanut CK:n, niin se voi kytkeä salauksen päälle lähettämällä käskyn päätelaitteelle. Salausprosessi perustuu jonosalaukseen, jossa algoritmi (f8) toimii jonosalaajana, jolle syötetään CK:n lisäksi neljä muuta parametria, jolloin salaaja tuottaa pseudosatunnaisbittivirran (maskin). Tämän virran kanssa selväkielisestä viestistä(plain text) lasketaan XOR. XOR on looginen operaatio, josta käytetään logiikassa joskus symbolia ⊕ tai ⩛. Sen merkitys on se, että *toinen ja vain toinen on tosi*. Vastaanottaja laskee saman pseudosatunnaisbittivirran ja laskemalla salatusta viestistä XOR:in saa selväkielisen viestin. Tässä tapauksessa KASUMI-algoritmia voidaan käyttää jonosalaajana (Niemi, Valtteri & Kaisa Nyberg 2003). Kuva 17 havainnollistaa tilannetta.



Kuva 17. Salauksen luonti ja purku f8 avulla (Boman, G. Horn, P. Howard & V. Niemi 2002).

Tämän tyylisessä salauksessa on se etu, että maski pystytään luomaan jo aikaisemmin ennen kuin edes tiedämme selkokielistä tekstiä. Varsinainen salaus on nopea bittioperaatio kuten kuvasta 17 näkyy. Kuvassa on esitetty myös muut salaukseen käytettävät parametrit: COUNT-C, BEARER, DIRECTION ja LENGHT. COUNT-C on 32-bittinen salaussarjanumero, BEARER on 5-bittinen tunniste, joka estää identtisten parametrien käytön toiselle salausjonolle, DIRECTION kuvaa nimensä mukaisesti suuntaa eli (1 bitti) saa arvon 0 jos liikennöidään UE:stä RNC:hen ja arvon 1 jos RNC:stä UE:hen. LENGHT kuvaa salatun lohkon pituutta. Se on 16-bittinen (Niemi, Valtteri & Kaisa Nyberg 2003; Vesanen 2003).

5.3. Dataverkkojen uhat

Dataverkkojen tietoturvassa painotetaan tässä tarkastelussa erityisesti lähiverkkojen WLAN-tietoturvaa. WLAN on tällä hetkellä dataverkkotekniikoista yleisin ja siihen pätevät samat pelisäännöt kuin muihinkin langattomiin dataverkkoihin.

WLAN-verkkoon liittyvät tietoturva-uhat voidaan luokitella kahteen kategoriaan. Voidaan puhua passiivisista ja aktiivisista uhista. Passiivisiin uhkiin kuuluvat salakuuntelu ja liikenteen analysointi, kun taas aktiivisiin uhkiin kuuluu siirtomedian häirintä tai katkaisu, tiedon muokkaus sekä tietojärjestelmiin tunkeutuminen. Seuraavaksi kerrotaan lyhyesti näistä eri uhkatyypeistä.

Salakuuntelu:

Salakuuntelussa joku ulkopuolinen henkilö kuuntelee verkon liikennettä ilman lupaa. WLAN:issa kuuluvuusalue on sen verran laaja, että salakuuntelu voidaan toteuttaa myös rakennuksen ulkopuolelta käsin ja tämä lisää valtavasti tarvetta suojata yhteys. Salakuuntelun tarkoituksena on saada selville arkaluontoista tietoa, jonka avulla varsinainen hyökkäys voidaan toteuttaa. Sitä on erittäin vaikea estää ja havaita, joten siihen tulee varautua kunnolla.

Salakuuntelu perustuu siihen, että tukiasema lähettää ns. beacon -kontrolliviestejä, joita verkon asiakkaat kuuntelevat. Beacon-sanomat ovat viestejä, joita tukiasema lähettää määrätyn väliajoin. Sanoman tehtävänä on tarjota verkkoon liittyjille tarvittavat tiedot sekä solun asiakkaille tietoa tukiaseman kellosta. Näiden tietojen perusteella asiakkaat voivat liittyä verkkoon. Beacon-viestejä ei salata WLAN:issa mitenkään. WLAN:in lisäksi on myös toinen yleisesti käytössä oleva ainoastaan kotikäyttöön tarkoitettu lyhyen kantaman omaava HomeRF-järjestelmä, joka käyttää FHSS-taajuushyppelymenetelmää (Frequency Hopping Spread Spectrum). Taajuushyppelyssä lähettäjä vaihtaa lähetystaajuutta tietyn algoritmin mukaan. Taajuushyppelyalgoritmi voi olla täysin satunnainen kuitenkin siten, että lähettäjä ja vastaanottaja molemmat ovat tietoisia siitä tai että se on etukäteen sovittu. HomeRF vaihtaa taajuutta ainoastaan 50

kertaa sekunnissa. Vertailun vuoksi Bluetooth vaihtaa 1600 kertaa sekunnissa eikä tätäkään pidetä paljona (Vesanen 2003).

Vesanen kommentoi vielä lisäksi, että ”Koska käytettävällä taajuusalueella on vain 75 kanavaa, voidaan näitä kaikkia seurata esimerkiksi kuuntelemalla yhtä taajuutta, kunnes havaitaan beacon-viesti, siirtyä seuraavalle taajuudelle ja niin edelleen. Näin saadaan taajuusvaihtomalli helposti selville, kun tiedetään, että yhtä taajuutta käytetään vain 20ms kerrallaan. Myöskään DSSS-liikenteen (Direct-sequence Spread Spectrum) seuraaminen ei tuota asiansa osaavalle salakuuntelijalle vaikeuksia, vaikka DSSS-tekniikka kehitettiinkin Toisen Maailmansodan aikaan juuri hämäämään vihollista luulemaan radioliikennettä kohinaksi”

FHSS ja DSSS estävät salakuuntelun, mikäli kuuntelija ei saa selville taajuusmuutosten mallia. Tämä ei kuitenkaan tuota ammattilaisille ongelmia, joten sen varaan ei kannata suojaustaan jättää (Vesanen 2003).

Liikenteen analysointi:

Liikenteen analysoinnissa seuratataan vain tiedon kulkua, mutta ei yritetä selvittää, mitä datapaketit pitävät sisällään. Silloin tällöin saattaa kuitenkin paljastua luottamuksellistakin tietoa (Vesanen 2003).

Siirtomedian häirintä tai katkaisu:

Mikäli verkon kuormitus kasvaa, saattaa järjestelmän käytettävyys huonontua ja yhteydet katketa. Koska WLAN toimii vapaalla radiotaajuusalueella, on periaatteessa mahdollista kuormittaa koko taajuusalue niin, että koko verkko on tukossa. Tällaista häirintää vastaan ei voi suojautua muuta kuin eristämällä oma verkko ulkopuolisilta häiriöiltä. Verkko voidaan ylikuormittaa myös jatkuvilla tarpeettomilla palvelupyynnöillä (palvelunestohyökkäys). Väärennetyn tukiaseman perustaminen on myös mahdollista (Vesanen 2003).

Tiedon muokkaaminen:

Ulkopuolinen voi periaatteessa muokata verkossa liikkuvaa dataa tunkeutumatta lainkaan verkkoon. Tämä voi tapahtua myös tahattomasti ja siihen on varauduttu tarkistussummien avulla. Tarkistussumma on tietotekniikassa käytetty yksinkertainen tarkistuskoodaustapa, jolla voidaan varmistaa siirrretyn tiedon eheys. Tarkistussumma toimii tyypillisesti siten, että datapaketin tavujen summa tallennetaan vaikkapa 16-bittiseksi katkaistuna paketin loppuun pariin tavuun. Varsinaisen datan perään lisätään siis niin sanottu tarkistussumma. Tarkoituksellisen datan muokkauksen pitää myös muokata tarkistussummaa, joten datan muokkaus pitäisi olla helposti havaittavissa. Tarkistussummaa tehokkaampia koodeja tarkistukseen on esimerkiksi CRC (Cyclic Redundancy Check). Sillä voidaan muun muassa välttää edellä kuvattu parin pienen virheen sisältävän datan tulkitseminen ehjäksi kokonaisuudeksi (Vesanen 2003).

Tietojärjestelmään tunkeutuminen:

Tietojärjestelmiin tunkeutuminen tarkoittaa sitä, että ulkopuolinen onnistuu murtautumaan järjestelmään. Mikäli WLAN on yhteydessä langalliseen lähiverkkoon, WLAN:iin murtautuja saattaa päästä murtautumaan organisaation koko verkkoon tätä kautta. Tästä syystä tulisi miettiä, kannattaako WLAN-verkkoa yhdistää kiinteään verkkoon (Vesanen 2003).

5.4 Suojautuminen dataverkoissa

On olemassa monta eri tapaa, millä tavalla yritys tai yksityishenkilö voi suojata oman langattoman verkonsa. Seuraavaksi käydään läpi yleisesti, mitä eri suojaustapoja WLAN:ille löytyy, sillä AN:ssa käytetään hyödyksi todella paljon WLAN-hotspotteja, joita päätelaitteet osaavat muodostaa joko itse tai ovat sellaiseen yhteydessä. On äärimmäisen tärkeää, että käyttäjä voi varmistua turvallisuudestaan käyttämällä saatavilla olevia suojausmenetelmiä.

5.4.1 Autentikointi ja pääsynvalvonta

Autentikoinnilla tarkoitetaan sitä, että käyttäjä tunnistautuu tukiasemalle ja näin varmistutaan, että oikea käyttäjä on liittymässä verkkoon. Autentikaatiota voidaan toteuttaa kolmella tapaa: avoin/suljettu (salaamaton) autentikaatio, MAC-osoitteisiin pohjautuva todennus tai jaetun avaimen (salattu) autentikaatio. Seuraaksi tarkempaa tietoa näistä tekniikoista.

Salaamattomassa autentikoinnissa asiakas lähettää asiakastunnuksen sisältävän autentikontihallintapaketin. Tukiasema vastaa paketilla, jossa ilmoitetaan onnistuminen/ epäonnistuminen. Se perustuu avoimeen/suljettuun SSID-tunnukseen (Service Set Identifier). SSID on tunnus, joka yksilöi verkon ja antaa sille nimen. Se on korkeintaan 32 merkkiä pitkä ja sen avulla henkilö kytkeytyy haluamaansa langattoman verkon tukiasemaan. Yleensä saman valmistajan tukiasemilla on sama SSID-tunnus, joten sen vaihtaminen on suotavaa myös turvallisuuden vuoksi. Asetuksista voidaan itse päättää, halutaanko SSID lähettää ilmateitse, jotta kaikki näkevät sen. Tämä helpottaa huomattavasti verkkoon yhdistämistä esimerkiksi oppilaitoksissa, kun tunnus on kaikkien nähtävissä. Tällaista autentikointia kutsutaan avoimeksi. Mikäli kuitenkin SSID halutaan piilottaa, niin voidaan tämä tehdä tukiaseman asetuksista. Tätä puolestaan kutsutaan suljetuksi autentikoinniksi. SSID:n piilottaminen mahdollistaa paremman tietoturvan, sillä ulkopuolisen täytyy tietää kyseinen tunnus, jotta tukiasemaan saataisiin yhteys. Tämä tunnus voi olla vain tiettyjen henkilöiden tiedossa. On kuitenkin otettava huomioon se seikka, että SSID kulkee verkossa salaamattomana, joten verkkoa kuuntelemalla voidaan tunnus selvittää todella helposti (Vesanen 2003).

Pääsynvalvonnalla tarkoitetaan sitä, että pyritään rajaamaan, millä koneilla on lupa liittyä verkkoon. Pääsynhallintaa toteutetaan autentikoinnin avulla. Tämä voidaan toteuttaa määrittelemällä listat MAC-osoitteista (Media Access Control), joilla on oikeus liittyä verkkoon. MAC-osoitteella tarkoitetaan verkkosovittimen yksilöivää tunnusta, jolla yksittäinen kone on tunnistettavissa. Listan avulla voidaan määritellä,

että mitkä laitteet saavat olla yhteydessä verkkoon. Tämä pitää tehdä manuaalisesti tukiaseman asetuksissa, joten se on melko työlästä, mikäli lisättäviä laitteita on paljon. Vaikka MAC-suodatuksella pystytään estämään tiettyjen koneiden liittymistä verkkoon, ei se yksinään ole riittävä suojaustapa. Vaikka lähetetty data olisikin salakirjoitettu, liikkuvat MAC-osoitteet kuitenkin selkokielisinä ja ne on helppo selvittää. Kun MAC-osoite on selvitetty, on tunkeilijan helppo väärentää oma MAC-osoite vastaamaan kaapattua MAC-osoitetta. Mikäli verkkoon kaiken lisäksi liittyy jatkuvasti uusia koneita tai vanhoja poistuu, niin on todella vaikeaa pitää listaa sallituista osoitteista (Vesanen 2003).

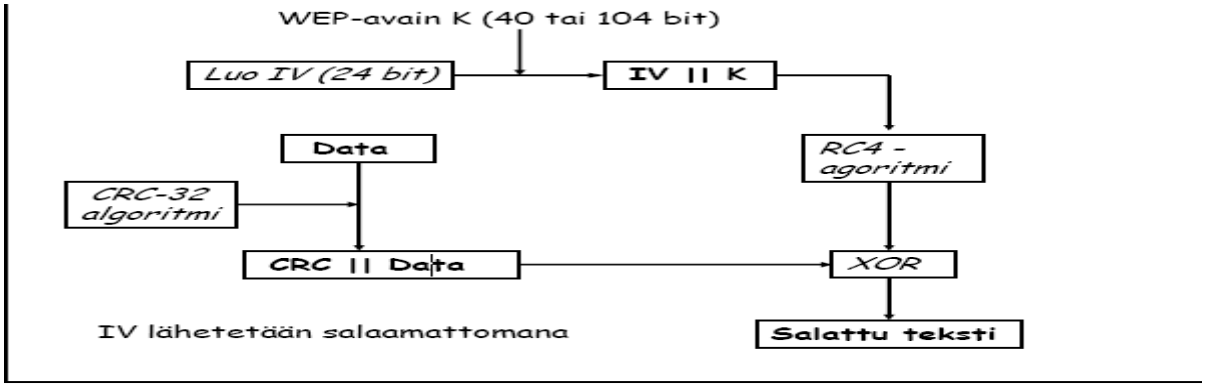
Jaetun avaimen (salatussa) autentikaatiossa käyttäjät todentavat itsensä käyttäen WEP-salausta (Wired Equivalent Privacy). WEP voidaan toteuttaa myös avoimella autentikoinnilla eli se mahdollistaa verkkoon liittymisen ja pakettien lähettämisen tukiasemalle. Verkkoa ei kuitenkaan pysty käyttämään ilman salausavainta. WEP perustuu kättelypaketteihin. Menetelmässä päälaite lähettää ensin autentikointipyynnön kuten avoimen autentikoinninkin yhteydessä, mutta tukiasema vastaakin tähän salaamattomalla viestillä, joka sisältää satunnaisen haastetekstin. Päätelaitteen tehtävänä on lähettää samainen teksti vastausviestissään, mutta päätelaite salaa haastetekstin omalla WEP-avaimellaan. Tukiasema purkaa vasteen omalla avaimellaan ja vertaa tulosta lähettämäänsä haastetekstiin. Jos tulos on sama, tunnistus hyväksytään kuittauksella. On huomattava, että WEP-tunnistus tarjoaa rajoitetun tavan verkossa tunnistautumiseen. Se ei todenna käyttäjää, vaan yksinkertaisesti vahvistaa, että käyttäjällä on avain. Tällöin ei kuitenkaan tiedetä, kuka käyttäjä on, mutta tiedetään, että hän tuntee avaimen. Mikäli käyttäjä kuitenkin halutaan tunnistaa, niin se voidaan toteuttaa RADIUS-protokollaa (Remote Authentication Dial In User Service) käyttäen (Havukainen 2010). Tästä kerrotaan lisää salausprotokollien yhteydessä.

5.4.2. Salausprotokollat WEP, WPA (TKIP) ja WPA2 (AES)

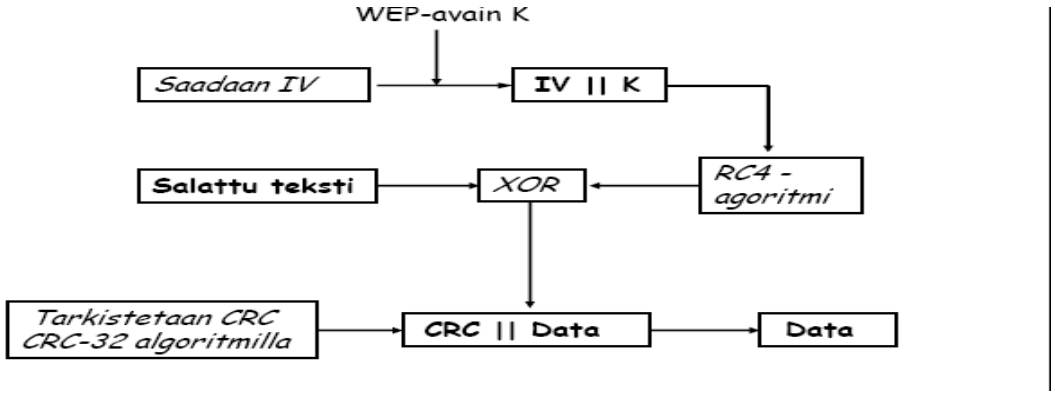
Salausprotokollien käyttäminen on hyvä tapa toteuttaa autentikointia käyttäjän ja tukiaseman välillä. Niiden käyttäminen on tärkeää pääsynhallinnan kannalta, joiden avulla estetään, ettei salausavain joudu ulkopuolisten käsiin. Jotkut salausprotokollat ovat tehokkaampia kuin toiset ja riippuu pitkältä käyttäjän intresseistä, mitä

salausmenetelmää halutaan käyttää. Seuraavaksi käydään läpi seuraavat kolme salausprotokollaa: WEP, WPA (Wi-Fi Protected Access) ja WPA2.

WEP on ensimmäinen standardoitu salausmenetelmä WLAN-tekniikassa. Se voi käyttää 40,104 tai 232 bittistä salausta. WEP:illä on kolme pääasiallista tarkoitusta, joista ensimmäinen on pääsynvalvonta, jonka avulla estetään verkkoon pääsy käyttämällä salasanaa (WEP-avainta) tunnistautumiseen. Toinen tehtävä on suojata käyttäjän lähettämä ja vastaanottama tieto salaamalla data WEP-avaimen avulla ja kolmas tehtävä on taata datan eheys eli varmistaa, että tieto ei muutu matkan aikana. Eheys varmistettiin tarkistussummien avulla. WEP:in käyttämä salausprotokolla on nimeltään RC4, joka on symmetrinen jonosalaaja ja se salaa tiedon yksi tavu kerrallaan. Se on melko nopea toiminnaltaan ja siinä käytetään vaihtelevan mittaisia salausavaimia. RC4:sta voidaankin kutsua satunnaislukugeneraattoriksi, joka luo isoja satunnaislukuja annettujen avaimien perusteella. Salattu teksti saadaan ottamalla XOR-operaatio satunnaisluvusta sekä salattavasta tekstistä. WEP:issä käytetään samaa avainta viestin salaukseen ja purkuun eli se on symmetrinen salaus. WEP ei kuitenkaan sovellu tehokkaaseen salaukseen johtuen RC4:n heikkouksista. Ongelmana on se, että pakettien kehyksissä osa biteistä (alustusvektoreista) lähetetään salaamattomana ja niiden perusteella voidaan helposti laskea käytetty salausavain. WEP ei myöskään salaa liikennettä koko siirtoväliltä, ainoastaan asiakkaalta tukiasemalle, mikä helpottaa huomattavasti ulkopuolisten tunkeutumista verkkoon (Tuominen 2005). Alla on havainnollistettu WEP-salausta ja -purkua.



Kuva 18. Viestin salaus WEP:issä (Vesanen 2003).



Kuva 19. Viestin purku WEP:issä (Vesanen 2003).

Jotta tietoturvaa voitaisiin tehostaa, voidaan WEP-salausta laajentaa erilaisilla protokollilla. Tällaiset protokollat ovat EAP (Extensible Authentication Protocol) ja RADIUS (Remote Authentication Dial In User Service)-protokollat. Nämä protokollat mahdollistavat sen, että jokaiselle käyttäjälle tulee omat henkilökohtaiset salasanat, joiden vaihtaminenkin onnistuu usein. EAP hoitaa käyttäjän tunnistamisen esimerkkinä VPN-asiakkaaat (Virtual Private Network) ja RADIUS taas hoitaa tunnus/salasanaparien hallinnan, joiden avulla voidaan luoda käyttäjille vaihtuvat ja satunnaisesti generoituvat salasanat (Havukainen 2010).

WPA ja WPA2:sessa autentikointi tapahtuu molemminpuolisesti. Tukiasema tiedostaa asiakkaan läsnäolon, mutta ei päästä tätä verkkoon ennen kuin autentikointi on suoritettu. Asiakas välittää tunnistetietoja ja tukiasema välittää ne autentikointipalvelimelle. Tunnistautuminen verkkoon tapahtuu käyttäen IEEE

802.1X/EAP-rajapintaa. Sekä asiakas että autentikointipalvelin tunnistautuvat molemmat toisilleen tukiaseman kautta. Molemminpuolisessa tunnistautumisessa on huomattava etu, sillä myös palvelin tunnistautuu asiakkaalle. Asiakas tietää ainakin olevansa yhteydessä oikeaan autentikointipalvelimeen. Kun asiakas on tunnistettu asiakas ja palvelin luovat samanaikaisesti PMK (Pairwise Master Key)-avainparin. Kirjautuminen täytyy kuitenkin saattaa vielä loppuun tukiaseman ja asiakkaan välillä, joten salausavaimet luodaan tämän jälkeen asiakkaalle. WPA-standardissa käytetään tähän protokollaa TKIP (Temporal Key Integrity Protocol) ja WPA2-standardissa puolestaan AES:ää (Advanced Encryption Standard) (Tuominen 2005; Havukainen 2010).

Temporal Key Integrity Protocol (TKIP) kehitettiin aikanaan WEP:in tilalle sen lukuisten haavoittuvuuksien vuoksi. TKIP käyttää myös WEP:in tapaan RC4-algoritmia, mutta erona on se, että salausavaimet ovat 128-bittisiä manuaalisesti syötettävien 40-bittisten avainparin sijaan. Lisäksi TKIP luo jokaiselle paketille omat salausavaimensa, joten avaimien ennustaminen on huomattavasti vaikeampaa. WPA:ssa kiinnitetään huomiota myös paketin eheyteen hyödyntämällä MIC:iä (Message Integrity Check) ja näin varmistustaan, että ulkopuolinen ei pääse muokkaamaan pakettien tietoja. Tämä tapahtuu siten, että lähettäjä ja vastaanottaja vertaavat toistensa kanssa jokaisen paketin tarkistussummia eli niiden pitää olla samat. WPA:n yksi pahimmista heikkouksista on sen tapa selvitä palvelunestohyökkäyksistä. Palvelunestohyökkäyksen havaitessaan WPA sulkee koko verkon minuutiksi havaittuaan hyökkäyksen, jolloin myös verkon lailliset käyttäjät jäävät katkon aikana ilman palvelua (Tuominen 2005; Havukainen 2010).

WPA2:n AES (Advanced Encryption Standard) on salausalgoritmina hyvin erilainen kuin WPA:n käyttämä RC4 ja vaatii vähän enemmän suoritintehoa. RC4 on korvattu CCMP-protokollalla (Counter Mode Protocol). WPA2 eli IEEE 802.11i kehitettiin, jotta saataisiin ratkaistua loputkin ongelmat WLAN-standardissa. AES pystyy käyttämään kolmea eri avainpituutta, jotka voivat olla joko 128-,192- tai 256-bittisiä. Se on huomattavasti tehokkaampi salaustapa kuin TKIP, mutta se vaatii laitteistomuutosta

eikä sen käyttöönottokaan riitä pelkkä ohjelmistopäivitys. Se on toistaiseksi murtamaton lohkosalausmenetelmä (Havukainen 2010).

Yhteenvetona voidaan todeta, että sekä 3G-verkossa että WLAN-verkossa tietoturvan taso on hyvä. 3G:ssä ainoana haittana on IMEI-koodin (International Mobile Equipment Identity) salaamattomuus, joten periaatteessa sen kaappaaminen on siirtotiellä mahdollista. WLAN:issa sen sijaan käyttäjän turvallisuus on varmasti taattu, mikäli käytetään käyttäjän itsensä asettamaa WPA2-salausta. Vaikka mobiilipuolella laitteistovalmistajat ja operaattorit ovat vastuussa käyttäjän tietoturvasta, niin myös myös käyttäjä voi omilla toimillaan vaikuttaan turvallisuutensa. Tämä pätee myös PC-puolella. Käyttäjän ei tule hyväksyä minkä tahansa ohjelmien asentumista laitteelleen, vaan niiden tulee olla peräisin luotettavasta lähteestä. Lisäksi palomuuriohjelmien ja virustorjuntojen käyttäminen on tärkeää kaikentyyppisissä päätelaitteissa aina tietokoneista matkapuhelimiin. Kun tiedetään, että tietoturvan taso on näissä kyseisissä langattomissa tekniikoissa näinkin hyvä, niin se luo hyvät edellytykset näiden kyseisten verkkojen turvalliselle yhteistyölle AN-visiota ajatellen.

6. AMBIENT NETWORKS

Tässä työssä on käyty tähän mennessä läpi perustekniikat liittyen Ambient Networks:iin, WLAN:in ja matkapuhelinverkkojen uhkia sekä niihin liittyvää tietoturvaa. Seuraavaksi perehdytään työn keskeiseen aiheeseen, eli Ambient Networks -konseptiin. Ambient Networks:illä tarkoitetaan kaikkialla läsnä olevaa verkkoa. AN:n visiona on, että jokaisella käyttäjällä tulisi olla mahdollisuus olla yhteydessä aina verkkoon missä päin maailmaa tahansa riippuen käyttäjän tarpeista. Tämä on mahdollista operaattorien välisillä liiketoimintasuhteilla ja se taas puolestaan vaatii päivitystä arkkitehtuuriin, jossa nykyiset tiedonsiirtotekniikat toimivat.

6.1. Ambient Networks -konsepti

Samanniminen Euroopan komission rahoittama ”Ambient Networks” -projekti käynnistettiin edistämään AN-vision toteutumista ja se sai alkunsa IST:n (Information Sciences and Technology) toimesta. Se koostui kahdesta eri vaiheesta. Ensimmäinen vaihe aloitettiin 2004, jossa Ambient Networks -konsepti kehitettiin ja toisessa vaiheessa kehiteltiin eräänlainen prototyyppi, jonka avulla pystyttiin testaamaan Ambient Networks:in hyötyjä eri ympäristöissä. Tästä projektista kerrotaan lisää myöhemmin.

Nykypäivänä meillä on käytössä valtava määrä erilaisia tiedonsiirtotekniinoita. On lähiverkkoja (LAN, WLAN), likiverkkoja (PAN), matkapuheliverkkoja (2G, 3G, 4G) ja niin edelleen. Ei ole mitään olemassa mitään universaalia radioteknologiaa, joka riittäisi kaikille päätelaitteille ja olisi kaikkien näiden laitteiden kanssa yhteensopiva. Siksi tulisikin panostaa eri verkkojen yhteistyöhön ja tyytyä nykyisiin standardeihin. On teoreettisesti todistettu, että kapasiteetti on kääntäen verrannollinen etäisyyteen (Emfwise 2002). Lisäksi langattomissa tekniikoissa joudutaan käyttämään tehokkaampaa signaalinkäsittelyä, mikäli halutaan lisätä tiedonsiirtokapasiteettia (throughtput) johtuen erilaisista esteistä ja se puolestaan lisää runsaasti tehonkulutusta. Korkea tehonkulutus on matkapuhelimissa ongelmallista niiden rajallisen akkukapasiteetin vuoksi. Kun otetaan esimerkkinä normaali puhelu, jonka

tiedonsiirtonopeus on 100kbps, niin yhteys kattaa jopa 10 km etäisyyden, mutta tiedonsiirtonopeus on silti suhteellisen pieni, vaikka riittääkin puheluun. Jos halutaan siirtää laadukasta videota, niin se vaatii jo 10Mbps, mutta kommunikaatioetäisyys jää vain 100 metriin. Tekniikkana käytetään HiperLania (High Performance Radio Local Area Networks).

Kuvitellaan käytännön tilanne, että jokainen kotona oleva sähköllä toimiva laite olisi yhdistetty myös tietoliikenneverkkoon. Nykyään tällaisia laitteita ovat esimerkiksi matkapuhelimet, tietokoneet, taulutietokoneet (tabletit), kämmentietokoneet (PDA), televisiot, vahvistimet, Bluray-soittimet ja niin edelleen. Tulevaísuudessa esimerkiksi uuni, kahvinkeitin, leivänpaahdin ja mikroaaltouuni voisivat myös olla tällaisia laitteita. Periaatteessa kaikki laitteet, jotka käyttävät sähköä, voidaan liittää verkkoon. Otetaan esimerkkinä käytännönläheinen tilanne, jossa olen kannettavalla tietokoneellani yhteydessä langattomasti WLAN:iin koulun kampusalueella. Lataan esimerkiksi jotain luentomateriaalia koulun palvelimelta. Samalla myös puhelimeni on yhteydessä kannettavaan Bluetoothin välityksellä ja hyödyntää sitä kautta koneen WLAN-yhteyttä, sillä Bluetooth kuluttaa vähemmän virtaa kuin puhelimen oma WLAN. Lisäksi voi olla mahdollista, että puhelimessa ei ole lainkaan WLAN:ia. Yhtäkkiä päätän poistua kampusalueelta, mutta en haluaisi katkaista kannettavalla tietokoneellani käynnissä olevaa latausta. Ongelma voidaan ratkaista siten, että kun poistun koulun alueelta, niin kannettava tietokoneeni alkaakin hyödyntää automaattisesti matkapuhelimen 3G-verkkoa esimerkiksi Bluetoothin välityksellä, joten tiedoston lataaminen ei keskeydy missään vaiheessa. Tämä ei edellytä minulta mitään toimenpiteitä, vaan kaikki tapahtuu automaattisesti. Kun pääsen kotiin, niin tiedoston lataaminen jatkuu, mutta yhteys vaihtuukin kotiverkkoni WLAN-yhteydeksi. Mikäli tiedosto on kuitenkin ehtinyt latautua, niin tiedosto voisi automaattisesti siirtyä esimerkiksi pöytätietokoneelleni Bluetoothin (PAN) välityksellä.

Ambient Networks -konsepti tähtää tällaiseen automaattisesti ja saumattomasti tapahtuvaan erilaisten tarjolla olevien tietoliikenneverkkojen yhdistettyyn käyttöön, jossa heterogeenisessa ympäristössä liikenne voidaan välittää sovellustarpeiden mukaan eri nodien välillä, jotka pitävät sisällään erilaisia laskentatehoja ja resursseja. Tällaisen

toteuttamiseen liittyy kuitenkin monia haasteita. Eri päätelaitteiden tulee olla mukautuvia, skaalautuvia resurssin tarjoajia ja lisäksi pitää pystyä energiatehokkaisiin mutta nopeisiin laskutoimituksiin. Ohjelmistopuolella eri protokollien tulisi toimia joustavasti ja automaattisesti. Neuvottelut pitäisi hoitua automaattisesti ja kaikki päätelaitteet voisi nimetä selkeästi jollain nimellä esimerkiksi ”lähin tulostin” sen sijaan, että käytettäisiin jotain osoitetta. Ideana on se, että jokainen päätelaite ei varsinaisesti olisi vain node, vaan päätelaite olisi samalla älykäs toiminnallinen yksikkö, joka pystyisi hyödyntämään erilaisia tarjolla olevia tietoliikenneyhteyksiä. Aiemmin käsiteltiin ad hoc -verkon toimintaa, jossa päätelaitteet ovat keskenään langattomasti yhteydessä. Ad hoc -verkon avulla pystytään takaamaan pidemmillekin matkoille korkeat tiedonsiirtonopeudet tai sitten voidaan lisätä joustavuutta reitittimillä (Jacquet 2002)

6.2. Ambient Networks:in suunnittelun lähtökohdat

6.2.1. Ambient Networks -konseptia edistävä projekti

Kuten aiemmin mainittiin, niin samanniminen Ambient Networks -projekti käynnistettiin 2004, jotta pystyttäisiin lisäämään verkkojen välistä yhteistyötä sekä yhteensopivuutta ja täten edistämään AN-konseptin mahdollistavan tekniikan kehittämistä. Tämän erään EU:n rahoittaman projektin tarkoituksena oli löytää ratkaisut sille, että eri verkkojen toimilaitteet voisivat toimia yhteensopivasti siten, että ne täytyisi vain kytkeä johonkin verkkoon, jonka jälkeen ne voisivat kommunikoida toistensa kanssa tarjolla olevia erilaisia tietoliikenneyhteyksiä käyttäen. Tällä hetkellä esimerkiksi likiverkkoa (PAN) käyttävät laitteet eivät voi kommunikoida keskenään lennosta, vaan se vaatii aina käyttäjältä manuaalisia konfiguraatioita. Yhteydelliset neuvottelut eivät ole mahdollisia likiverkkoa käyttävien käyttäjien välillä siten, että käyttäjien tarpeet otettaisiin huomioon, eikä esimerkiksi käyttäjän sijaintitietoa tai laitteiden tyyppiä hyödynnetä mitenkään. Nykypäivänä tiedonsiirto eri verkkotyyppien välillä onnistuu melko hyvin, mutta datan hallintavoissa on runsaasti eroavaisuuksia eri verkkotyyppien välillä. Erilaiset hallintaympäristöt johtuvat siitä, että niiden avulla halutaan helpottaa

erilaisten palvelujen toimintaa kuten esimerkiksi VPN:ää (Virtual Private Network), liikkuvuutta, turvallisuutta, QoS:ää (Quality of Service) sekä NAT:ia (Network Address Translation). Ongelmana on, että ei ole olemassa mitään yleistä kaikille yhteensopivaa hallintakerrosta (Control Layer), joka hallitsisi kaikentyyppisiä laitteita ja verkkoja. Pitäisi kyetä hyödyntämään kaikkia laitteita, verkkoja ja rajapintoja tehokkaasti. Tämän hetken tekniikoilla se ei ole mahdollista. Ambient Networks:issä tarkoituksena on saada laitteet toimimaan saumattomasti keskenään, ilman että käyttäjän tarvitsee puuttua tilanteeseen mitenkään ja että kaikki tapahtuu käyttäjältä automaattisesti. Kaiken pitäisi tapahtua AN-konseptissa nopeasti lennossa.. Internet-yhteys pitäisi olla aina saatavilla juuri oikeaan aikaan ja tilanteeseen sopivimmalla tavalla automaattisesti. Projektin yhteydessä korostettiin verkkojen kompositiota, joka tarkoittaa sitä, että mahdollistetaan eri verkkojen saumaton ja automaattinen yhteiskäyttö kunkin käyttäjän yksilöllisiä tarpeita varten. Kullakin käyttäjällä voi olla kotonaan oma likiverkkonsa laitteidensa kesken (Campos, Rui. Kappler, C. Pinho, C. Pöyhönen, P. Ricardo, M & Ruela, J 2005).

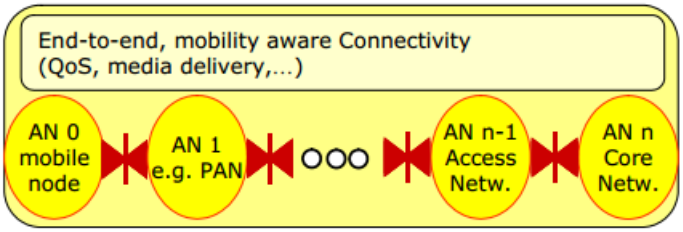
6.2.2. Ambien Networks:in kriteerit

Niin kuin aikaisemmin tuli todettua, niin yhteisten kaikkien saatavilla olevien hallintafunktioiden puute sekä riippuvuus Internet-teknologioista ja omistajuudesta ovat olleet esteenä nopealle verkkojen kehittymiselle. Tuottaa suuria haasteita määritellä joukko universaalisesti saatavilla olevia hallintafunktioita. Viitekehyksen tulee toteuttaa tietyt periaatteet, jotta tarvittavat hallintafunktiot saadaan käyttöön sekä tarvittava kapasiteetti. Ambient Networks:in tulee perustua avoimiin yhteyksiin ja funktioihin. Yksi tapa olisi poistaa arkkitehtuureihin perustuvat rajoitukset koskien sitä, kuka tai mikä saa ottaa yhteyttä mihinkin verkkoon. Ambien Network-konseptissa oli käyttäjä sitten operaattori tai loppukäyttäjä, niin pitäisi olla hyvät liiketoimintamahdollisuudet kaikkiin kumppaneihin riippumatta kumppanin sijainnista (Campos, Rui. Kappler, C. Pinho, C. Pöyhönen, P. Ricardo, M & Ruela, J 2005).

Kun eri verkkoja yhteensovitetaan nykytekniikoilla toisiinsa, niin pakettien reititys on suhteellisen helppoa, mutta kun otetaan mukaan liikkuvuus, turvallisuus ja palvelun laatu, niin kohdataan paljon haasteita. AN-konseptissa tarvitaan automaattiset

määrittelyt sille, millaisten verkkotyyppien välillä yhteiskäyttö on mahdollista ja millaisten ei. Mikäli kaksi eri verkkotyyppiä päättää yhdistyä, niin tulee sen tapahtua automaattisesti ja itsehallinnointi pitää toimia myös automatiikalla (Campos, Rui. Kappler, C. Pinho, C. Pöyhönen, P. Ricardo, M & Ruela, J 2005).

Nykypäivän eri verkkotekniikoissa on hyvin paljon samoja piirteitä, kun puhutaan pakettien reititykseen liittyvistä funktioista. Niiden kontrollointiin liittyvät funktiot on kuitenkin hajautettu monelle eri verkkoprotokollan kerrokselle ja ne on määritelty sekä toteutettu eri tavoin eri operaattorille, mikä lisää verkon monimutkaisuutta. AN:ssa sekä yhteys- että hallintataso ovat loogisesti erotettu toisistaan. Hallintatasolla viitataan AN:n sisällä olevaan keskeiseen elementtiin ACS:ään (Ambient Control Space). Se on eräänlainen laajennus nykyisiin tekniikkoihin, joka pitää sisällään tiettyjä funktioita, jotka ovat yhteensopivia kaikkialla verkossa. Kyseiset funktiot voidaan lisätä olemassa oleviin verkkoihin. Alla olevassa kuvassa 20 on havainnollistettu tilanne tällaisesta eri verkkojen yhdistämisestä eli kompositiosta (Abramowicz, Henrik. Karl, H. Niebert, N. Prehofer, C & Schieder A 2007).



Kuva 20. Eri verkkojen yhdistäminen Ambient Networks -konseptin mukaan (Abramowicz, Henrik. Karl, H. Niebert, N. Prehofer, C & Schieder A 2007).

Tämän tyylisellä lähestymistavalla saavutetaan tietynlaisia hyötyjä. Verkon operaattorit voivat päättää, minkä tason tukea he antavat käyttäjille ja liikekumppaneille perustuen joustaviin hallinta- ja kompositiofunktioihin. Edullisia ja sisältörikkaita verkkoja pystytään rakentamaan maailmanlaajuisesti ja nykyisiä verkkoja pystytään integroimaan toisiinsa sekä käyttämään uusia teknologioita. Loppukäyttäjät määrittelevät oman käyttäjäprofiilinsa, jonka perusteella toimilaite ja verkko tekevät päätökset. Jokaisella voi olla oma yksilöllinen käyttäjäprofiillinsa. Käyttäjät voivat vapaasti kehittää

palvelujaan helposti laajennettavien yhteysrajapintojen avulla. Palveluntarjoajat voivat tarjota palvelujaan laajalle käyttäjäryhmälle ilman että palveluntarjoajien tarvitsee huolehtia käyttäjien verkkokapasiteetista tai verkkoon pääsemisestä (Abramowicz, Henrik. Karl, H. Niebert, N. Prehofer, C & Schieder A 2007).

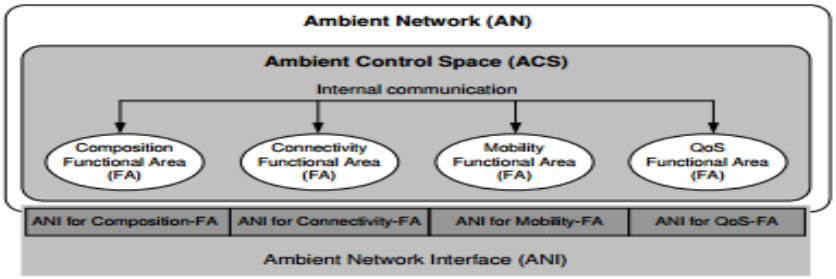
6.2.3. Ambient Control Space

ACS on eräänlainen hallintatila AN:n sisällä. Sillä on tiettyjä funktioita, joihin muilla käyttäjillä on pääsy ja sillä on täysi hallintaoikeus verkon resursseihin. Aiemmin puhuttiin eri AN:ien kompositiosta. Verkon kompositio koostuu neuvottelusta ja sopimuksen toteutumisesta. Eri verkkojen yhteiskäytön tulee tapahtua automaattisesti. Etukäteen määritellyt toimintavat määrittelevät sen, miten verkkojen yhteiskäyttö toteutetaan. ACS ja liitettävyysverkko (Connectivity Network) muodostavat yhdessä Ambient Networks:in. ACS:n sisältämät funktiot sisältävät tuen esimerkiksi liikkuvuudelle (mobility) tai erilaisten radioteknologioiden tukemisen (multiaccess). Erilaisten radioteknologioiden tukemisesta ja yhteistyöstä puhutaan tarkemmin myöhemmin. ACS:llä on käytössään myös tietyt rajapinnat, joita se käyttää hyödykseen liittyessään muihin AN:siin. Näihin rajapintoihin palataan myös myöhemmin. ACS:llä on modulaarinen rakenne eli se koostuu pienistä itsenäisistä funktionaalisista alueista (Functional Areas), joilla jokaisella on joku tietty toiminnallisuus. Näitä alueita ovat muun muassa liitettävyysfunktioalue (Connectivity Functional Area), kompositiofunktioalue (Composition Functional Area) sekä liikkuvuuteen ja palvelun laatuun liittyvät funktioalueet ja niin edelleen (Abramowicz, Henrik. Karl, H. Niebert, N. Prehofer, C & Schieder A 2007).

6.2.4. Rajapinnat ja verkon kompositio

ACS:llä on käytössään kolme eri rajapintaa, joiden kanssa se kommunikoi muiden AN:ien kanssa. Nämä ovat ANI (Ambient Network Interface), ASI (Ambient Service Interface) ja ARI (Ambient Resource Interface). Verkkojen tulisi toimia kaikenlaisissa verkkoympäristöissä maailmanlaajuisesti. Nämä rajapinnat mahdollistavat samantyylisten funktioiden käytön riippumatta AN:n tyypistä, edesauttavat verkon nopeaa toimintaa AN:n kytkeytyessä verkkoon ja lisäksi mahdollistavat verkon uudelleen konfiguroinnin, tukevat liikkuvuutta ja lieventävät verkon monimutkaisuutta.

Jos jokin verkko haluaa liittyä toiseen verkkoon, niin se tapahtuu ANI:n välityksellä. ANI tarjoaa standardoidut keinot eri ACS:ien funktioiden yhdistämiseen eri domainien välillä. Se myös mainostaa ACS:n funktioita lähellä oleville muille domaineille. Jos funktioihin (palveluihin) pitää päästä käsiksi ACS:n sisällä, niin se tapahtuu ASI:n välityksellä. Jos taas halutaan päästä johonkin resurssiin käsiksi verkon sisällä esimerkiksi liikenteen määrään, niin käytetään ARI-rajapintaa. Rajapinnoilla pyritään peittämään verkon sisäisiä rakenteita (Abramowicz, Henrik. Karl, H. Niebert, N. Prehofer, C & Schieder A 2007).



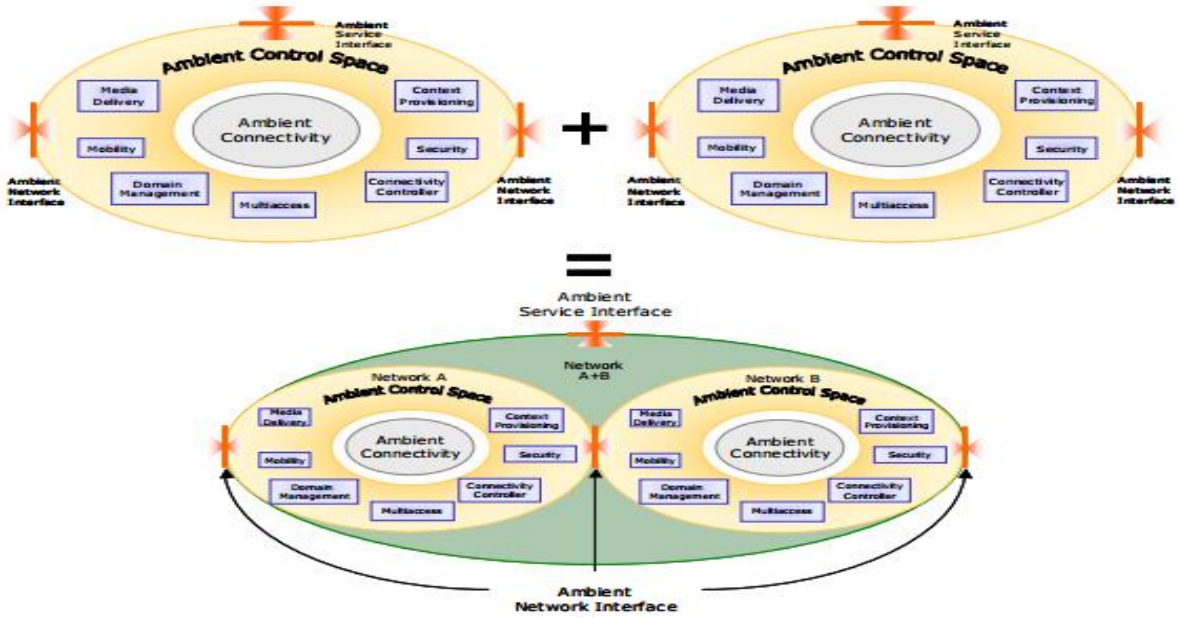
Kuva 21. Ambient networks:in hallintatilan arkkitehtuuri (Campos, Rui. Kappler, C. Pinho, C. Pöyhönen, P. Ricardo, M & Ruela, J 2005).

Kun kaksi verkkoa päättää yhdistyä, niin ne kommunikoivat ANIN:n välityksellä neuvotellakseen yhteistyösopimuksesta, jota kutsutaan nimellä kompositiosopimus (Composition Agreement). GANS (The Generic Ambient Network Signalling) on puolestaan protokollajoukko, joka mahdollistaa signaloinnin funktionaalisten alueiden ja ANI:n välillä. GANS hoitaa tiedonvälitystä yleisesti hyväksyttyjen protokollien välityksellä liittyen neuvotteluun, kapasiteetin määrään ja kompositiosopimukseen.
Kompositiosopimus sisältää tiedot liittymisresursseista, ACS:n hallintaan liittyvistä säännöistä ja muille tarjottavista palveluista. Kompositiosopimus on määritelty niiden funktionaalisten alueiden (FA) toimesta, jotka kompositioon haluavat ottaa osaa. Tuloksena kummankin AN:n ACS:stä muodostuu uusi ACS, joka kontrolloi kaikkia loogisia ja fyysisiä resursseja, mitä vanhoilla ACS:llä oli. Uusi ACS on myös yhteydessä ulkomaailmaan omalla uudella rajapinnalla ANI. Tämä kompositiosta syntynyt uusi ACS on ainut, joka näkyy ulkopuolisille yhdistymisen jälkeen. Kompositio ei kuitenkaan välttämättä aina johda uuden AN:n syntymiseen. Tällöin

kukin AN säilyttää oman ACS:nsä ja siihen liittyvät resurssit entisellään ja tämä kyseinen AN toimii vain määritellyn kompositiosopimuksen mukaan yhteistyössä toisen AN:n kanssa. Se, että päättääkö kaksi AN:ää liittyä toisiinsa, voi riippua monestakin eri tekijästä. Se voi riippua esimerkiksi siitä, onko verkkojen välillä luottamussuhde tai ennalta määritellyistä säännöistä. (Abramowicz, Henrik. Karl, H. Niebert, N. Prehofer, C & Schieder A 2007).

Kun käydään vielä tarkemmin läpi kahden eri AN:n yhdistyminen, niin se lähtee siitä, että aluksi etsitään sopivia verkkoja, joita voitaisiin käyttää yhteisesti. Tällainen esimerkki voi olla esimerkiksi junassa, kun matkapuhelin siirtyy lennosta omasta matkapuhelinverkostaan käyttämään esimerkiksi junan tai mahdollisesti kanssamatkustajan verkkoa. Ideana on, että ei tarvittaisi mitään erillisiä roaming-sopimuksia, vaan siirtyminen tapahtuisi automaattisesti vierasverkkoon, eikä olisi sidoksissa mihinkään tiettyyn kotiverkkoon. Seuraava vaihe liittyy sopivan AN:n löytämiseen. Ennen kompositiota molemmat AN:t voivat mainostaa toisilleen, millaisia palveluja ja resursseja heiltä löytyy. Sen perusteella osataan sanoa, onko toinen sopiva kandidaatti. Liitettävyysfunktio (Connectivity-FA) pitää sisällään tiedot siitä, millaisissa yhteyksissä kompositio voi tapahtua. Kun sopiva kandidaatti on löytynyt, niin sen jälkeen pitää hoitaa tietoturvaan liittyvät toimenpiteet. Joku ennalta määrätty kolmas luotettava osapuoli voisi hoitaa autentikointiin tai auktorisointiin liittyvät toimenpiteet (security) ja varmistaa, että kyseisten osapuolten identiteetit pitävät paikkansa ja ne ovat luotettavia. Kolmatta osapuolta ei kuitenkaan välttämättä aina tarvita. Sen jälkeen protokolla sopii kompositiosta, joka pitää sisällään toisilleen tarjottavat palvelut ja resurssit. Lisäksi sopimus pitää sisällään tiedot siitä, kuinka näihin palveluihin ja resursseihin pääsee käsiksi, kompositioon liittyviä sääntöjä, yhdistyneen AN:n tunnisteen sekä laskutukseen ja veloitukseen liittyviä tietoja eri osapuolten välillä. QoS:llä puolestaan tarkoitetaan tietoliikenteen luokittelua ja priorisointia. Priorisoinnin perusteella osaa liikenteestä voidaan hidastaa tai jopa pudottaa kokonaan pois, mikäli linjojen välityskyky ei riitä. Liikennettä voidaan priorisoida sovellusten, käyttäjien tai käytettyjen tietokoneiden perusteella (Campos, Rui. Kappler, C. Pinho, C. Pöyhönen, P. Ricardo, M & Ruela, J 2005).

Kompositiosopimus on äärimmäisen laaja kokonaisuus ja keskeisin osa yhdistymisessä. Kompositiosopimuksessa on hirveä määrä erilaisia parametreja, arvoja ja vaihtoehtoja, joista joudutaan sopimaan osapuolten välillä. Tämän kaiken pitäisi tapahtua automaattisesti ja mahdollisimman nopeasti ja on selvää, että joudutaan keksimään keinoja, millä yhdistymistä voitaisiin nopeuttaa. Yksi näistä keinoista on käyttää etukäteen laadittuja yleisiä asetustaulukoita (templates). Ne sisältävät valmiiksi laadittuja parametreja, arvoja ja vaihtoehtoja, joista ei enää tarvitse erikseen sopia yhdistämisen yhteydessä, vaan jos taulukko on tilanteeseen sopiva, niin se hyväksytään automaattisesti. Ne pätevät kaikkiin tilanteisiin. Näitä voi olla esimerkiksi identiteetti, palvelujen kuvaus, laadunvalvontaan liittyvät vaatimukset, valvontaan ja suorituskykyyn liittyvä raportointi sekä ongelmia ja verkon kaatumista koskeva raportointi. Kun näihin liittyvät asetukset on jo etukäteen tallennettu tällaiseen asetustaulukkoon, niin voidaan merkittävästi vähentää yhdistymiseen kuluvaa aikaa. Kun kompositiosopimuksesta on päästy yhteisymmärrykseen, niin varsinainen yhdistyminen tapahtuu muodostamalla kokonaan uusi yhteinen ACS ja ANI. Uudelle AN:lle annetaan myös uusi identiteetti ja tarvittavat konfiguraatiot ja säännöt päivitetään hallintafunktioille kompositiosopimukseen perustuen (Campos, Rui. Kappler, C. Pinho, C. Pöyhönen, P. Ricardo, M & Ruela, J 2005).

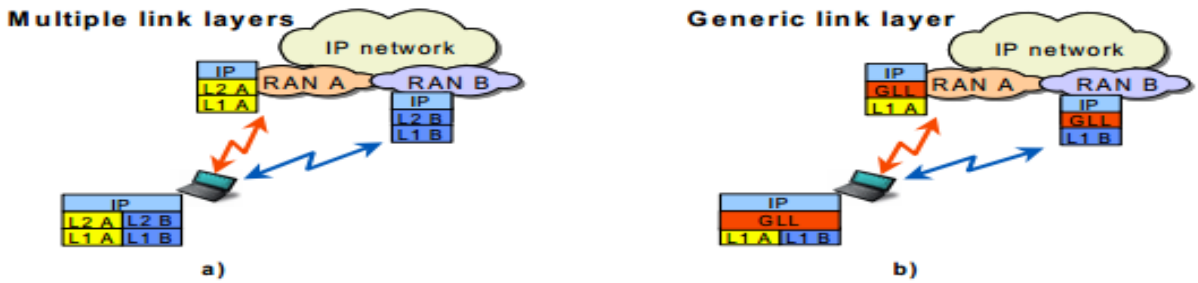


Kuva 22. Kahden Ambient Networksin hallintatilan yhdistyminen yhdeksi domainiksi (Abramowicz, Henrik. Karl, H. Niebert, N. Prehofer, C & Schieder A 2007).

Kuvasta 22 nähdään yksityiskohtaisemmin, että millaisia erilaisia funktioita hallintatila voisi pitää sisällään. Muun muassa median välitys (media delivery) ja multiaccess ovat keskeisessä osassa AN:n konseptia. Multimediapalveluilla on erilaisia vaatimuksia riippuen käyttötavasta kuten esimerkiksi suoratoisto, tiedostojen lataus, pikaviestintä ja videopuhelut. Sen takia vaaditaan, että kaikille näille eri tekniikoille pitäisi löytyä sellainen yhteinen medianvälityskerros, joka tukee kaikkia näitä multimediatekniikoita. Sen tulee tukea kaikkia nykytekniikoita, mutta sen pitää olla myös konfiguroitavissa tulevaisuuden tekniikoita varten. Suurin haaste on saada eri tekniikat toimimaan yhteensopivasti eri ympäristöissä ja vielä eri laitteissa ilman että siitä aiheutuu haittaa käyttäjälle. Medianvälityskerros on toteutettu OSI-mallissa kuljetuskerroksen päälle. Medianvälitysverkko koostuu niin sanotuista mediaporteista, jotka sijaitsevat joko verkon toimilaitteiden sisällä tai niitä yhdistävässä kerroksessa ja mediavälitysverkon tarjoamat funktiot välittyvät palvelukerrokselle ennaltamäärätyn rajapinnan kautta. Tällaisia funktioita ovat esimerkiksi tietoliikenteen reititys, tiedon tallennus (caching) sekä tietoliikenteen mukauttaminen eri olosuhteisiin. Tiedon varastoinnilla tarkoitetaan sitä, että varastoidaan tietty osa datasta, ettei kuljetusreittien tarvitsisi olla liian pitkät

osapuolten välillä. Yleensä tällaista tiedon varastointia tapahtuu silloin erityisesti, kun siirtotielle on asetettu korkeat kapasiteettivaatimukset. Tiedonsiirron mukautuksella tarkoitetaan yksinkertaisesti datan muuntamista (transkoodausta) eri päätelaitteisiin sopivaksi (Campos, Rui. Kappler, C. Pinho, C. Pöyhönen & Ruela, J 2005).

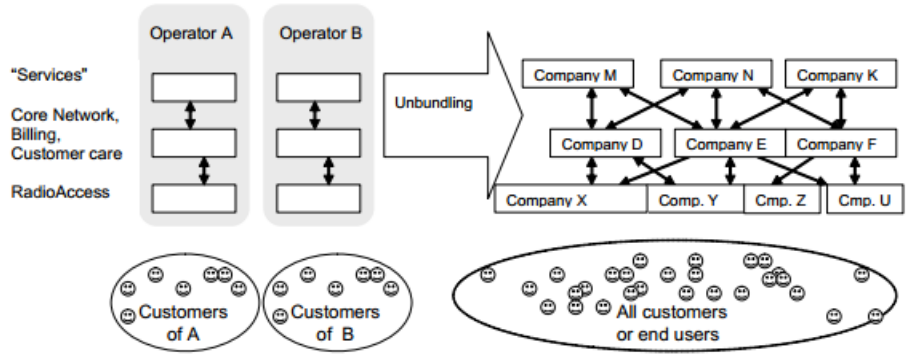
Aiemmin puhuttiin multiaccess-funktiosta, joka mahdollistaa eri radioteknologioiden ja verkkojen yhteistyön. Koska langattomat mobiiliverkot käyttävät eri radiotekniikoita (vrt. 2G ja 3G), niin tarvitaan jokin yleinen linkkikerros (Generic Link Layer), joka pystyy käsittelemään näitä erilaisia tekniikoita. Se toimii erilaisten radiotekniikoiden resurssien varaajana eli yleinen linkkikerros pyrkii hyödyntämään tahokkaammin verkon tiedonsiirtokapasiteetin tasapainottamalla kuormaa eri tekniikoiden välillä. Yleinen linkkikerros pyrkii toimimaan dynaamisesti ja konfiguroimaan radioprotokollaa radiotekniikoiden muutosten mukaisesti. Se etsii erilaisia yhteneväisyyksiä tekniikoiden välillä nopeuttaakseen konfigurointia. Yleinen linkkikerros tarjoaa niin sanotusti konfiguroitavan linkkikerroksen funktioiden työkalupakin luodakseen maailmanlaajuisen linkkikerroksen eri radiotekniikoille. Se tarkoittaa käytännössä sitä, että tarjolla on oikeat funktiot kullekin radiotekniikalle sekä määritellään protokollaparametrit ja näin ollen saadaan yleinen linkkikerros konfiguroitua. Tämän tulee tapahtua automaattisesti, kun siirrytään verkosta toiseen ja ilman, että dataa katoaa. Lopputuloksena saadaan toteutettua yleinen linkkikerros, joka tarjoaa yhteensopivia radiolinkkikerroksia erilaisille radiotekniikoille (Radio Access Network). (Campos, Rui. Kappler, C. Pinho, C. Pöyhönen, P. Ricardo, M & Ruela, J 2005). Tämä on havainnollistettu kuvassa 23.



Kuva 23. Siirtyminen monikerrosmallista yleiseen linkkikerrosmalliin (Campos, Rui. Kappler, C. Pinho, C. Pöyhönen, P. Ricardo, M & Ruela, J 2005).

7. AMBIENT NETWORKS LIIKETOIMINTAYMPÄRISTÖSSÄ

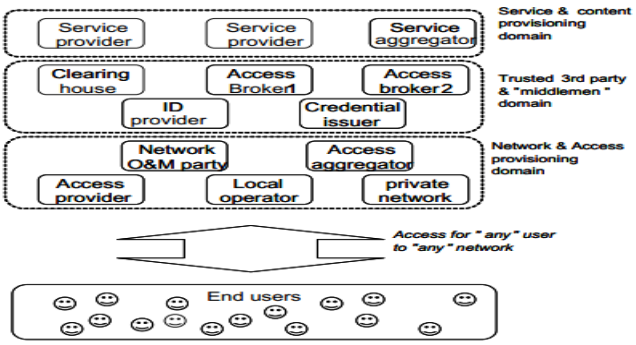
Liiketoimintamielessä AN:n avulla pyritään kehittämään uusia tapoja tehdä yhteistyötä eri toimijoiden kesken siten, että kilpailu ei kärsisi siitä, ja kaikki tahot hyötyisivät ja että kaikki osapuolet hyötyisivät siitä. Jotta kommunikointi olisi helpompaa ja joustavampaa lukuisten eri toimijoiden välillä, niin tarvitaan AN:n kaltaista konseptia mahdollistamaan tällainen skenaario. Nykypäivänä meillä on lukuisia eri operaattoreita, joilla jokaisella on tietty asiakasmäärä eli karkeasti voidaan yleistää, että yksi asiakas per operaattori. Soveltamalla AN:n käsitettä tällaiseen tilanteeseen voidaan mahdollistaa, että kaikilla operaattoreilla on pääsy kaikkiin asiakkaisiin ja päinvastoin (Huitema, George. Markendahl, J & Rietkerk O 2006). Alla oleva kuva 24 havainnollistaa, millainen tilanne on nykypäivänä ja mihin halutaan pyrkiä AN:n konseptin avulla.



Kuva 24. Tämänhetkisen markkinarakenteen jakautuminen pienemmiksi osiksi (Huitema, George. Markendahl, J & Rietkerk O 2006).

Kuvassa 24 ovat operaattorit A ja B, joilla kummallakin on omat asiakkaansa. Operaattorit eivät ole keskenään millään tavallaan yhteistyössä, vaan toimivat kokonaan omineen. Arkkitehtuuri koostuu kolmesta eri kerroksesta: palvelut, ydinverkko (asiakaspalvelu,laskutus) ja pääsykerros. Visiona olisi, että kyseiset operaattorit tekisivät yhteystyötä keskenään myös vaakatasolla eli operaattoreilla olisi mahdollisuus päästä käsiksi kaikkiin asiakkaisiin ja kaikilla asiakkailla vuorostaan olisi mahdollisuus käyttää usean eri operaattorin palveluja. Tällainen operaattoreiden ja käyttäjien

ylläpitämien lähiverkkojen välinen yhteistyö edellyttää uusia liiketoimintamalleja ja uusia toimijoita verkkoon. Käyttäjät voivat olla joko itsenäisiä tai operaattorin alaisuudessa. Tällaisella liiketoimintamallilla on lukuisia hyötyjä sekä operaattorin että loppukäyttäjän kannalta. Käyttäjällä on parempi verkon saatavuus, laatu ja luotettavuus. Operaattorilla taas on laajempi asiakaskanta sekä pienemmät kustannukset, sillä resursseja voidaan käyttää aikaisempaa tehokkaammin, eikä aina tarvitse pystyttää erilaisia tukiasemia tiheämmin. Tämä vähentää myös verkon ylikapasiteettia, kun voidaan käyttää olemassa olevia resursseja tehokkaammin hyödyksi. Operaattoreilla on mahdollisuus päästää oman verkkonsa alueelle vieraan operaattorin asiakkaita. Ideana on, että tietyllä tasolla operaattorit toimivat yhteistyössä ja tietyllä tasolla kilpailevat keskenään. Kilpailukyvyn lisääntyminen on puolestaan aina kuluttajan edun mukaista. Kaikki osapuolet hyötyvät AN:sta. Erilaisia toimijoita voisivat olla paikallinen pääsyntarjoaja (local access provider), pääsynryhmittäjä (access aggregator), pääsynvälittäjä (access broker), luotettava kolmas osapuoli (trusted third party), selvitysryhmä (clearing house), laskutuspalvelu (compensation service provider) ja palvelunryhmittäjä (service aggregator). Kuten kuvassa 25 nähdään, kerrosajattelu toimii samalla tavalla AN:n konseptissa eli palvelut ovat ylimpänä, keskimmäisenä on laskutus (clearing house) ja alimpana pääsy verkkoon. Operaattorit toimivat kuvassa tiiviissä yhteistyössä (Huitema, George. Markendahl, J & Rietkerk O 2006).



Kuva 25. Ambient Networks:in liiketoimintaroolit (Huitema, George. Markendahl, J & Rietkerk O 2006).

7.1. Liiketoimintaroolit

7.1.1. Paikallinen pääsyntarjoaja

Paikallinen pääsyntarjoaja tarjoaa nimensä mukaan paikalliselle verkolle pääsyn paikallisiin resursseihin. Yhdistämällä paikalliset resurssit maailmanlaajuisten verkkojen kanssa voidaan säästää huomattavasti kustannuksissa hyödyntämällä tehokkaammin eri verkkojen resursseja. Jos esimerkiksi puhutaan jostain suuresta kauppaketjusta, niin jokaisessa kaupassa voi olla oma langaton tukiasemansa, joka tarjoaa pääsyn paikallisiin asiakkaisiin. Paikalliset pääsyntarjoajat yhdistetään mitä todennäköisimmin paikallisten palveluntarjoajien kanssa, kun halutaan kohdentaa myös palveluja tietyn alueen asiakkaille. Kynnys päästä näihin palveluihin on huomattavasti matalampi, koska AN tukee montaa eri verkko-operaattoria samaan aikaan. Paikallisilla pääsyntarjoajilla tarkoitetaan muun muassa eri koti- ja toimistoverkkoja (Huitema, George. Markendahl, J & Rietkerk O 2006).

7.1.2. Pääsynryhmittäjä

Koska paikallisia pääsyntarjoajia voi olla jopa tuhansia pienellä alueella esimerkiksi kaupungissa, niin niitä tulee ryhmitellä jollain tavalla. Paikallisilta pääsyntarjoajilta ostetaan pääsyoikeuksia tiettyihin palveluihin ja sitten ne ryhmitellään ja myydään palvelunryhmittäjille tai pääsynvälittäjille tiettyinä paketteina. Pääsynryhmittäjä voi olla itsenäinen kokonaisuus tai osa operaattorin toimintoja (Huitema, George. Markendahl, J & Rietkerk O 2006).

7.1.3. Pääsynvälittäjä

Pääsynvälittäjä toimii nimensä mukaan pääsynvälittäjänä hallinnoimalla yhteyksiä palvelunryhmittäjien ja palveluntarjoajien sekä pääsynryhmittäjien ja pääsytarjoajien välillä. Pääsynvälittäjällä voi olla myös laskutussuhde asiakkaiden kanssa. Mikäli näin on, niin voidaan puhua kahdenlaisista pääsynvälittäjistä: vähittäiskauppaan liittyvä pääsynvälitys, jossa tarjotaan kapasiteettia loppukäyttäjälle tai tukkukauppaan liittyvä pääsynvälitys, jossa tarjotaan kapasiteettia esimerkiksi matkapuhelinoperaattoreille tai palvelunryhmittäjille (Huitema, George. Markendahl, J & Rietkerk O 2006).

7.1.4. Palvelunryhmittäjä

Palvelunryhmittäjä kokoaa eri palveluita yhteen. Se on asiakkaan ja kaupan välinen rooli, jossa asiakas ostaa jotain tiettyjä palveluja ja ne kootaan sitten yhteen. Sen tarkoitus on vähentää verkon monimutkaisuutta. Nykypäivänä asiakas on sidottu yhteen operaattoriin. Tulevaisuudessa asiakas voi olla yhteydessä useisiin kymmeniin paikallisverkkoihin tai paikallisiin pääsyntarjoajiin. Palvelunryhmittäjät ja vähittäiskaupan pääsynvälittäjät voivat toimia käyttäjän puolesta. Se tarjoaa käyttäjälle automaattisesti juuri häntä kiinnostavia palveluja ja tekee sen maailmanlaajuisesti. Asiakkaalla on aina mahdollisuus päästä verkkoon paikasta ja operaattorista riippumatta (Huitema, George. Markendahl, J & Rietkerk O 2006).

7.1.5. Luotettava kolmas osapuoli

Luotettava kolmas osapuoli helpottaa eri toimijoiden välistä vuorovaikutusta, koska kaikki luottavat tähän kyseiseen tahoon. Se on vastuussa tietoturvasta, joka liittyy esimerkiksi osapuolten identiteetin varmistukseen, hallinnointiin ja maksunvälitykseen. Se hoitaa sopimukset osapuolten välillä, sähköisen allekirjoituksen ja niin edelleen. Sen tulee olla luotettava ja puolueeton toimija. Esimerkiksi pankki tai luottoyhtiö voisi ottaa tämän roolin (Huitema, George. Markendahl, J & Rietkerk O 2006).

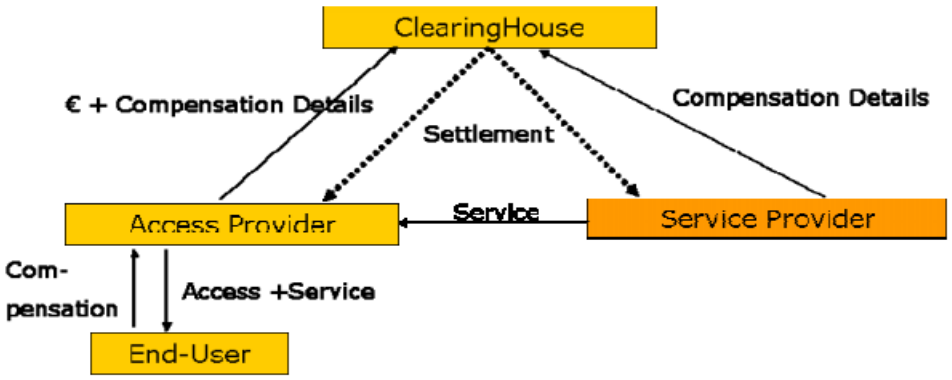
7.1.6. Laskutuspalvelu

Laskutuspalvelu tarjoaa laskutukseen liittyvää palvelua eri osapuolille, joiden täytyy veloittaa asiakasta tarjotuista palveluista. Se auttaa hoitamaan osapuolten välistä maksuliikennettä, mikäli osapuolilta ei itseltään löydy tällaista toiminnallisuutta. Se voisi toimia yhteistyössä selvitysryhmän (clearing house) kanssa. Laskutuspalvelu voisi hoitaa vähittäiskaupan laskutusta operaattorin ja asiakkaan välillä. Voidaan ajatella, että matkapuhelinoperaattori esimerkiksi voisi yksin hoitaa tätä laskutuspuolta
(Huitema, George. Markendahl, J & Rietkerk O 2006).

7.1.7. Selvitysryhmä

Selvitysryhmä hoitaa puolestaan tukkukauppaan liittyvää laskutusta eri operaattorien välillä pitäen sisällään tulojen jaon operaattoreiden kesken. Selvitysryhmänä voisi toimia myös pääsy- tai palveluryhmittäjä. Selvitysryhmä on enemmän yritykseltä

yritykselle hoituva laskutuspalvelu. Selvitysryhmä keskittyy esimerkiksi sen tyyliseen laskutukseen, jossa asiakas on vieraillut vieraan operaattorin alueella ja käyttänyt sen palveluja ja asiakasta on veloitettu siitä. Kuva 26 kuvaa selvitysryhmän sekä palveluntarjoajan että pääsyntarjoajan välistä vuorovaikutusta, jossa asiakas tekee maksusuorituksen, joka välittyy selvitysryhmälle eli laskuttajalle ja vastineeksi asiakas pääsee käyttää kyseisen palveluntarjoajan palveluja (Huitema, George. Markendahl, J & Rietkerk O 2006).



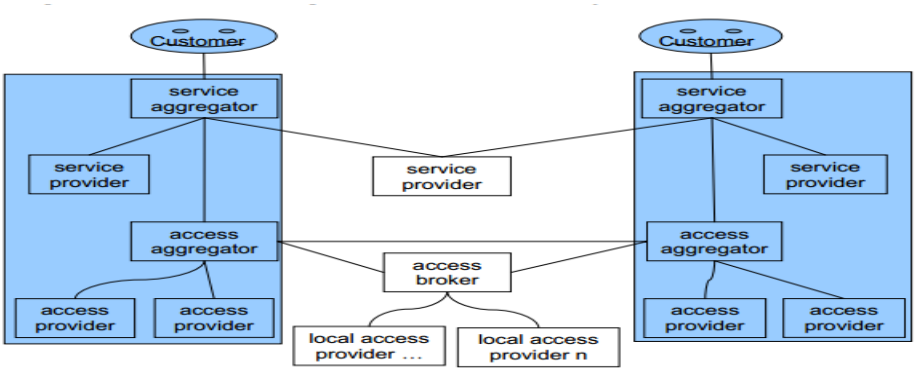
Kuva 26. Laskutusprosessi selvitysryhmän näkökulmasta (Huitema, George. Markendahl, J & Rietkerk O 2006).

7.2. Roolien väliset suhteet

AN-konseptin myötä kyseisten roolien väliset suhteet muuttuvat ja jopa uusia rooleja tarvitaan. Eri roolit voivat toimia itsenäisinä kokonaisuuksina tai osana operaattoria. Kuten aikaisemmin mainittiin, niin AN mahdollistaa yhteistyön vaakatasolla kuten kuvassa 24 eli se tarkoittaa sitä, että eri operaattoreilla on mahdollisuus päästä käsiksi kaikkiin asiakkaisiin ja kaikilla asiakkailla vuorostaan on mahdollisuus käyttää usean eri operaattorin palveluja . Kun mietitään esimerkiksi paikallisia verkkoja, jotka kaikki toimivat tiiviisti yhdessä, niin on selvää, että loppukäyttäjä hyötyy siitä. Kun käyttäjä liikkuu paikasta toiseen, niin paikallisverkon vaihtumisen toiseen tulee tapahtua automaattisesti ja joustavasti. On tärkeää, että kummatkin osapuolet hyötyvät tällaisesta

aina läsnä olevasta verkosta. On olemassa tiettyjä tilanteita, missä isot toimijat hyötyvät pienemmistä paikallisverkoista. Paikallisverkoilla saattaa olla jo ennestään toimiva infrastruktuuri ja hyvä asiakaskunta ja näin ollen ei ole järkevää perustaa omaa verkkoa pienemmille alueille. Kumpikin osapuoli hyötyy yhteistyöstä, sillä isompi toimija säästää muun muassa kustannuksissa, kun saa käyttää paikallisverkon palveluja, kun taas pienempi toimija pääsee mahdollisesti laajempaan asiakaskuntaan käsiksi isomman toimijan ansiosta (Huitema, George. Markendahl, J & Rietkerk O 2006).

On myös syytä pohtia, mitkä roolit toimivat itsenäisinä kokonaisuuksina ja mitkä taas toimivat osana operaattoria? Onko mahdollista, että tietyt roolit hoitavat useampaa eri tehtävää käyttäjän tai pääsyntarjoajan puolesta vai onko kenties järkevämpää, että käyttäjä saa itse enemmän vastuuta? Aiemmin puhuttiin ryhmittelijöistä (aggregators), kun koottiin yhteen eri palveluja tai paikallisia pääsyntarjoajia. Pääsynryhmittäjät (access aggregators) kokoavat eri paikallisverkkoja yhteen. Pääsynryhmittäjät mahdollistavat sen, että operaattorin paikallisverkot toimivat saumattomasti yhdessä. Palvelunryhmittäjät (service aggregators) puolestaan kokoavat eri palveluja ja verkkoja yhteen nippuun käyttäjän puolesta ja mahdollistavat eri asiakkaiden välisen vuorovaikutuksen. Kuvassa 27 näkyy kaksi tummaa laatikkoa, jotka kuvaavat operaattoreita. Operaattorit pitävät sisällään lukuisia paikallisverkkoja. Operaattorin sisällä on tietynlainen arvoketju. Arvoketjussa siirrytään alhaalta ylös siten, että alimpana ovat paikallisverkot, jotka kootaan yhteen ryhmittäjillä. Sen jälkeen niihin lisätään tietyt palvelut ja välitetään asiakkaalle. Tämä tapahtuu kummankin operaattorin sisällä. Operaattoreiden välillä näkyvät itsenäiset pääsy- ja palveluntarjoajat, jotka eivät ole osana operaattoria. Näiden itsenäisten toimijoiden ansiosta päästään hyödyntämään AN:n visiota operaattoreiden välisestä yhteistyöstä (Huitema, George. Markendahl, J & Rietkerk O 2006).

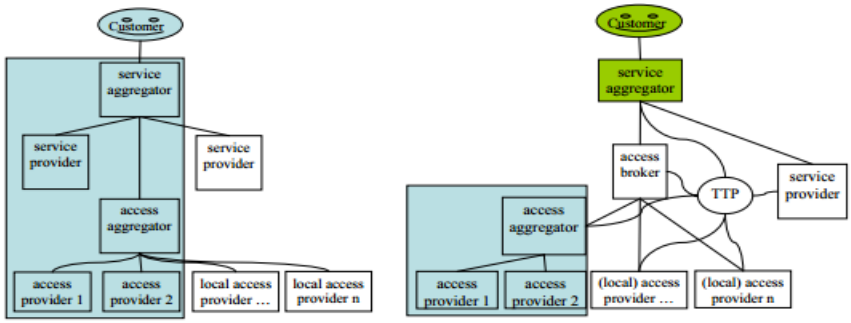


Kuva 27. Kahden operaattorin välinen yhteistyö itsenäisen pääsy- ja palveluntarjoajan välityksellä (Huitema, George. Markendahl, J & Rietkerk O 2006).

Pääsynryhmittäjät jakavat resurssejaan keskenään. Ne voivat esimerkiksi ostaa toiselta kapasiteettia tai myydä ylimääräistä ja niin edelleen. AN-teknologia mahdollistaa tällaisen resurssien jakamisen automaattisesti. Kuten kuvasta 27 näkyy, niin pääsynvälittäjä (access broker) hoitaa tätä roolia. Pääsynvälittäjä voi toimia kokonaan pääsyntarjoajien puolesta, ja lisäksi se voi tehdä niin sanottua tukkukauppaa eri operaattoreiden välityksellä. Pääsynvälittäjällä voi olla kymmeniä ellei jopa satoja paikallisverkkoja alaisuudessaan ja jokainen uusi paikallisverkko voi tehdä itselleen lisätuloja siirtymällä tietyn pääsynvälittäjän alaisuuteen. Paikallisverkko voi myös tarjota jotain asiasisältöäkin muille paikallisverkoille, kuten esimerkiksi sijaintinsa. Tilanne on lopulta se, että operaattoreiden yhteistyössä palvelut saadaan itsenäisiltä palveluntarjoajilta ja pääsy hoituu pääsynvälittäjän kautta (Huitema, George. Markendahl, J & Rietkerk O 2006).

On myös mahdollista, että palveluryhmittäjä (service aggregator) on kokonaan itsenäinen taho, joka ei siis ole osana operaattoria. Tämä on havainnollistettu kuvassa 28. Mitä enemmän löytyy tällaisia itsenäisiä toimijoita, sitä paremmin toimii kilpailu. Se taas on loppukäyttäjän kannalta paras skenaario. Periaatteessa erillistä palveluryhmittäjää ei tarvita, sillä jokainen asiakas voi itsekin hoitaa tällaista roolia ja kerätä itse haluamansa palvelut. Toisaalta monet asiakkaat arvostavat sitä, että jokin yksittäinen taho hoitaa asiakkaiden puolesta järjestelyt, neuvottelut ja erilaisten palvelujen kokoamisen. Tähän liittyy kuitenkin tietoturvariski, sillä jos yksittäisen tahon tietoturva kärsii, niin kaikkien asiakkaiden tiedot ovat vaarassa. Jos taas jokainen

asiakas hoitaisi itse palveluryhmityksen roolia, niin vahinko rajoittuisi vain yhteen asiakkaaseen. Kuvassa 28 esiintyy myös toinen yhteinen taho, jota kutsutaan luotettavaksi kolmanneksi osapuoleksi (TTP). Se hoitaa kaikki tietoturvaan ja laskutukseen liittyvät toimenpiteet (Huitema, George. Markendahl, J & Rietkerk O 2006).



Kuva 28. Laajennus kuvaan 27 muutamalla lisäelementillä (Huitema, George. Markendahl, J & Rietkerk O 2006).

Kuvassa 28 näkyy vasemmalla, että sinisellä pohjalla oleva operaattori toimii sekä pääsy- että palveluryhmittelijänä. Vihreällä pohjalla näkyy itsenäinen palveluryhmittelijä, joka ei ole osana operaattoria ja toimii käyttäjän puolesta. Se tekee yhteistyötä palveluvälittäjän ja TTP:n (Trusted Third Party) kanssa. Oikealla sinisellä pohjalla oleva operaattori toimii ainoastaan pääsyryhmittelijänä (Huitema, George. Markendahl, J & Rietkerk O 2006).

Yleisesti voidaan todeta, että kaikenlaisia vaihtoehtoja tulee varmasti näkymään tulevaisuudessa. On operaattoreita, jotka tarjoavat koko pakettia eli palveluita ja pääsyä näihin palveluihin. Sitten on myös itsenäisiä toimijoita, jotka eivät ole osana operaattoria ja toimivat joko pääsy- tai palveluntarjoajana. Jotkut toimivat keskenään yhteistyössä ja jotkut taas yksin riippuen ihan liiketoimintastrategiasta. Joka tapauksessa AN-arkkitehtuuria suunniteltaessa on tärkeää, että oikeanlaiset resurssit ovat käytössä oikeaan aikaan. On pystyttävä nopeasti päättämään, onko verkolla mahdollisuus yhdistyä toiseen verkkoon, mitä palveluja pystytään milläkin hetkellä tarjoamaan ja millainen on tietoturvan taso ja sen ylläpidon hinta. Tällainen vertailu pitäisi toteuttaa ilman, että se häiritsee käyttäjää ja on sekä käyttäjälle että verkolle sillä hetkellä paras

vaihtoehto. Tilanne, jossa mobiilioperaattori työskentelee paikallisverkkojen kanssa ja käyttää hyväkseen myös niiden kapasiteettia, vähentää yleisellä tasolla investointikapasiteetin tarvetta, riskitasoa ja juoksevia kuluja. Mikäli paikallisverkoilla on jo ennestään toimiva infrastruktuuri, on suositeltavaa hyödyntää niiden olemassaolevia resursseja ja vähentää näin investointiin liittyvää riskiä. Myös maksutapahtumien kustannukset halutaan pitää käyttäjien keskuudessa edullisena. Tämä edellyttää aiempaa monipuolisempia liiketoimintasuhteita, mikäli halutaan hyödyntää myös operaattorista riippumattomia rooleja. Vaikka se lisääkin verkon monimutkaisuutta, niin se kuitenkin parantaa kilpailukykyä ja yhteistyötä (Huitema, George. Markendahl, J & Rietkerk O 2006).

8. AMBIENT NETWORKS -KONSEPTIN ARVIOINTI

8.1. Lähtökohdat arvioinnille ja sen apuvälineet

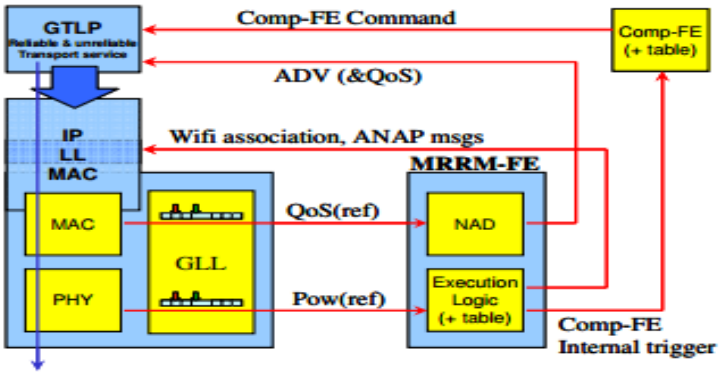
Aikaisemmin mainittiin, että Ambient Networks -projekti käynnistettiin, jotta pystyttiin arvioimaan AN-konseptin hyödyllisyyttä. Projekti sisälsi kaksi eri vaihetta. Ensimmäisessä vaiheessa (2004–2005) laadittiin AN-arkkitehtuuri, joka piti sisällään hallintatilan luonnin (Ambient Control Space), uudet funktiot sekä uudet rajapinnat tulevaisuuden verkoissa. Toisessa vaiheessa (2006–2007) suoritettiin arviointi siitä, miten kyseissä projektissa onnistuttiin. Apuna käytettiin integroitua prototyyppiä, jonka avulla pystyttiin testaamaan AN:n käyttökelpoisuutta lukuisissa eri käytännön tilanteissa. ACS-prototyyppiä käytettiin testaamaan eri komponentteja, jotka luotiin AN-arkkitehtuuriin perustuvan projektin edetessä (Akhtar, Nadeem. Bria, A. Jennen, R. Markendahl, J. Miozzo, M. Pöyhönen, P. Rembarz, R & Simon, C 2007).

Arvioinnin tarkoitus oli varmistaa, että suunnitellut toiminnallisuudet (funktiot) AN:ssa toimivat niin kuin pitää ja ne tarjoavat paremmat puitteet yhteistyölle. Tämä tarkoitti käytännössä sitä, että kokonaiskapasiteettia pystyttiin hyödyntämään aiempaa tehokkaammin, verkon saatavuus ja luotetavuus oli parempi, ja loppukäyttäjän kustannustasoa suorituskykyyn nähden oli paranneltu. Arvioinnissa mitattiin muun muassa sitä aikaa, mikä kului tukiaseman vaihtoon ja signaloinnin määrää siirrossa. Erityisesti huomiota kiinnitettiin seuraaviin seikkoihin: 1. Kuinka verkonhallintaan liittyvä tietoliikennekuorma kasvoivat käyttäjien ja tarjoajien lisääntyessä. 2. Kuinka verkonhallintaan liittyvä tietoliikennekuorma ja viiveet kasvoivat, kun käyttäjät tulivat ahneiksi. 3. Mikä oli yhtäältä varkonhallinnan ja toisaalta verkkoa käyttävien osapuolten välisen tiedonsiirron (eli kaupallisen tietoliikenteen) osuus kokonaistietoliikennekuormasta. 4. Kuinka paljon verkkoon liittymisestä aiheutuva viive vaaransi sujuvaa tukiaseman vaihtoa.

Ahneilla käyttäjillä tarkoitettiin sellaista käyttäjää, joka kulutti paljon verkon resursseja tutkimalla eri tarjoajien palveluja ja osallistumalla moniin neuvotteluihin käyden läpi

monta eri palveluntarjoajaa. Vähemmän ahne käyttäjä sen sijaan hyväksyi heti ensimmäisen verkkotarjoajan palvelun. Lopuksi vielä tutkittiin algoritmien skaalautuvuutta tilanteessa, jossa käyttäjä joutui valitsemaan lukuisten eri operaattoreiden, pääsyntarjoajien sekä palveluntarjoajien väliltä sopivimman (Akhtar, Nadeem. Bria, A. Jennen, R. Markendahl, J. Miozzo, M. Pöyhönen, P. Rembarz, R & Simon, C 2007).

Jotta tarvittavat arvioinnit pystyttiin suorittamaan käytännön tasolla, tuli siihen hankkia oikeanlaiset välineet. Eri työryhmät laativat prototyypit kehittämistään hallintatoiminnallisuuksista. Tämän jälkeen yksittäiset komponentit koottiin yhdeksi prototyypiksi, joka sisälsi tietyt hallintafunktiot. Arvioinnissa käytettiin ACS-prototyyppiä, johon integroitiin tarvittavat funktiot. Tällä kyseisellä prototyypillä pystyttiin riittävällä tasolla arvioimaan AN-konseptin onnistumista, mutta oli selvää, että sitä ei pystytty testaamaan laajassa mittakaavassa muuta kuin abstraktilla tasolla. Signaalin kuormaa ja viivettä pystyttiin mittaamaan monien pääsy- ja palveluntarjoajien ympäristössä tietyn verkkosimulaattorin avulla, joka ei tosin käsittänyt kaikkia rajapintoja ja toiminnallisuuksia. Kuvassa 29 on havainnollistettu arkkitehtuuri, joka sisälsi kaikki toiminnallisuudet ja protokollat, joita tarvittiin verkon mainostamiseen, liittymiseen sekä kompositioon liittyviin toimenpiteisiin käytännöllisesti (Akhtar, Nadeem. Bria, A. Jennen, R. Markendahl, J. Miozzo, M. Pöyhönen, P. Rembarz, R & Simon, C 2007).



Kuva 29. AN-arkkitehtuuri ja sen toteutus simulaattorissa (Akhtar, Nadeem. Bria, A. Jennen, R. Markendahl, J. Miozzo, M. Pöyhönen, P. Rembarz, R & Simon, C 2007).

AN:n komponentteja, joita testauksessa käytettiin tavanomaisen protokollapinon lisäksi olivat: siirtokerroksen toiminnallinen kokonaisuus (Generic Link Layer), moniradioresurssihallinta (Multi Radio Resource Management), yhdistymiseen liittyvä funktionaalinen kokonaisuus (Composition-FE), yleinen kuljetuskerroksen protokolla (Generic Transport Layer Protocol) ja yhdistymiseen liittyvä yleinen palvelukerrosprotokolla (Generic Service Layer Protocol). FE tulee sanoista Functional Entity, joka viittaa funktionaaliseen kokonaisuuteen.

Arkkitehtuuri mahdollisti yhteydenpidon päätelaitteiden ja tukiasemien välillä jokaisessa toiminnallisessa kokonaisuudessa. Lisäksi yhteydenpito eri funktionaalisten olioiden välillä tapahtui GTLP:n (Generic Transport Layer Protocol) välityksellä, jotka lähetettiin standardin protokollapinon kautta. Tämä tapahtui siten, että GTLP-viestit kapseloitiin IP-paketteihin. Yleisen siirtokerroksen funktionaalinen kokonaisuus oli vastuussa siitä, että se toimitti palvelunlaatua koskevat mittarit sekä MAC- (Media Access Control) että fyysiselle kerrokselle (Physical Layer). Päätelaitteella tämä tapahtui esimerkiksi vastaanoton tai tilastojen keruun yhteydessä koskien muun muassa bittivirheiden määrää tai vastaanotetun signaalin voimakkuutta. Esimerkiksi kuvassa 29 näkyy QoS(ref) ja Pow(ref), jotka molemmat viittaavat laatuindikaattoreihin. Nämä laatuindikaattorit välitettiin sen jälkeen moniradioresurssihallinnalle (MRRM). Se sisälsi verkon mainostamiseen ja löytämiseen liittyvän olion (NAD). NAD tulkitsi tulevat mainostukset ja piti huolta, että mobiilin päätelaitteen lähettämät mainostukset olivat AN standardin mukaisia. MRRM ja NAD olivat molemmat suoraan kytkettyinä prokollapinoon. Niiden toimeenpaneva logiikka oli liitetty siirtokerrokseen. Se hoiti verkon yhdistymiseen liittyviä toimenpiteitä kuten esimerkiksi WiFi:in liittyvät viestit, kun IP-yhteyttä luotiin. Lisäksi tarvittiin ANAP-viestejä (Ambient network Attachment Procedures), jotta voitiin luoda yhteys vieraisiin verkkoihin. Kompositio-oliota käytettiin vuorostaan yhdistymiseen liittyvissä toimenpiteissä (Akhtar, Nadeem. Bria, A. Jennen, R. Markendahl, J. Miozzo, M. Pöyhönen, P. Rembarz, R & Simon, C 2007).

8.2. Tietoliikennekuorman analysointi

Aikaisemmin puhuttiin pääsyntarjoajien mainostamisesta, jossa he mainostivat käyttäjille palveluitaan, jonka jälkeen käyttäjä pystyi liittymään verkkoon. Sen jälkeen osapuolten välille luotiin turvallinen yhteys ja toteutettiin eri verkkojen yhteiskäyttö eli kompositio. Tutkimuksessa selvitettiin, minkä verran tietoliikennekuormaa tästä kaikesta aiheutui ja miten se vaikutti tukiaseman vaihdon (handover) suorituskykyyn. Tiedonsiirron analyysi toteutettiin ympäristössä, jossa oli useita verkontarjoajia ja käyttäjiä. Lisäksi skenaarioon kuului myös lukuisia liityntäpisteitä (tukiasemia), jotka tässä skenaariossa oli toteutettu WLAN-tekniikalla. Tukiasema yhdisti erilaisia mobiileja päätelaitteita, jonka jälkeen muodostettiin palveluistunto mediapalvelimen kanssa (Akhtar, Nadeem. Bria, A. Jennen, R. Markendahl, J. Miozzo, M. Pöyhönen, P. Rembarz, R & Simon, C 2007). Taulukko 30 havainnollistaa, minkä verran tiedonsiirtoa vaadittiin verkkoon liittymisen ja yhdistymisen yhteydessä. ”CA Negotiation” ja ”CA Validation” liittyi kompositiosopimuksen neuvotteluun ja vahvistukseen käytännössä.

Table 1 Signaling load for different procedures

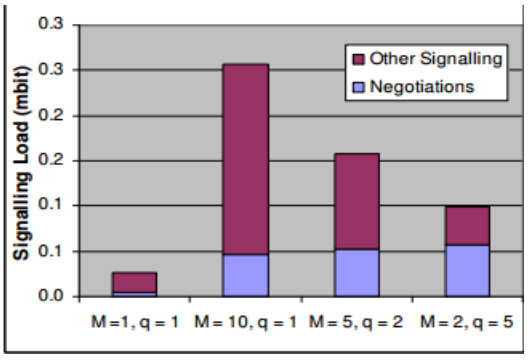
Signaling Phase	*Signaling Bits*
Network Attachment	13328
GANS Signaling Association	4587
CA Negotiation	(2q-1)*2999 + 1591
CA Validation	3182

Kuva 30. Tietoliikennekuorman jakautuminen toteutettaessa AN-konseptin mukaista tietoliikenneverkkojen yhteiskäyttöä (Akhtar, Nadeem. Bria, A. Jennen, R. Markendahl, J. Miozzo, M. Pöyhönen, P. Rembarz, R & Simon, C 2007).

Näiden tietojen avulla laskettiin kokonaistietoliikennekuorman määrä tilanteessa, jossa tietty määrä käyttäjiä yritti päästä yhteen verkkoon tiettynä ajanjaksona. Skenaariossa jokainen käyttäjä neuvotteli vain yhden kierroksen verran (q=1) tietyn verkontarjoajan kanssa, mutta käyttäjä pystyi käymään neuvottelukierroksia usean eri palveluntarjoajan kanssa. Palveluntarjoajat olivat puolestaan yhteydessä mediapalvelimeen 128kbit/s nopeudella. Session kesto oli keskiarvoltaan noin 5 minuuttia. Kun käyttäjä päätti, kenen palveluntarjoajan verkkoon hän halusi liittyä, niin sen jälkeen muodostettiin

mediaistunto. Suhteellista tietoliikennekuormaa laskettiin jakamalla kompositioon vaativat bitit mediasessioon vaativilla biteillä. Siinä huomattiin, että vaikka tietoliikennekuorma kasvaakin lineaarisesti eri palveluntarjoajien lisääntyessä käyttäjää kohti, niin se ei kuitenkaan nostanut merkittävästi tietoliikennekuormaa suhteessa mediasession vaatimaan datamäärään. Suhde datamäärään pysyi jopa alle 1 %, vaikka käyttäjä olisi käynyt yhden neuvottelukierroksen jopa 10 eri palveluntarjoajan kanssa ja käytetty datamäärä olisi ollut vähäinen (Akhtar, Nadeem. Bria, A. Jennen, R. Markendahl, J. Miozzo, M. Pöyhönen, P. Rembarz, R & Simon, C 2007).

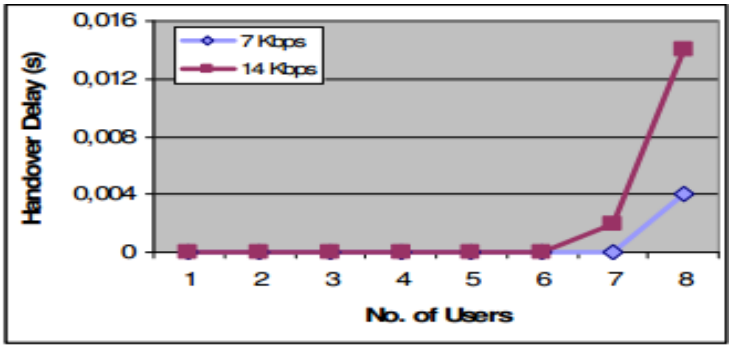
Aiemmin puhuttiin ”ahneista” käyttäjistä ja sillä viitattiin siihen, että käyttäjä käy useita eri neuvottelukierroksia läpi lukuisten eri palveluntarjoajien kanssa. Arvioinnissa haluttiin selvittää, että mikä vaikutus tällä olisi tietoliikennekuormaan. Tulokset saavutettiin pitämällä verkkojen määrää (M) ja neuvottelukierrosten (Q) tulo vakiona, joka oli 10 (M*Q=10). Havaintona huomattiin, että lukuisat neuvottelukierrokset harvempien palveluntarjoajien kanssa kulutti vähemmän resursseja kuin harvemmat neuvottelukierrokset monien eri palveluntarjoajien kanssa. Tämä johtui siitä, että verkkoon liittyminen (network attachment), kompositiosopimuksen vahvistaminen (CA validation) ja toteuttaminen vaativat aina enemmän tiedonsiirtoa kuin pelkät neuvottelukierrokset (CA negotiations), kuten taulukosta 30 näkyy. Kuva 31 havainnollistaa käyttäjän ”ahneuden” vaikutusta tietoliikennekuormaan (Akhtar, Nadeem. Bria, A. Jennen, R. Markendahl, J. Miozzo, M. Pöyhönen, P. Rembarz, R & Simon, C 2007).



Kuva 31. Käyttäjän ”ahneuden” aiheuttama signaalikuorma (Akhtar, Nadeem. Bria, A. Jennen, R. Markendahl, J. Miozzo, M. Pöyhönen, P. Rembarz, R & Simon, C 2007).

8.3. Viiveanalyysi tukiaseman vaihdon yhteydessä

Käyttäjän pitäisi pystyä siirtymään tukiasemalta toiselle ilman, että yhteys katkeaisi tai häiriytyisi merkittävästi. Toisaalta verkon ei tulisi tuhlata liian paljon resursseja tukiaseman vaihtoon ja vuorostaan käyttäjän päätelaite ei saisi kuluttaa liikaa virtaa tukiasemanvaihtoprosessiin (handover). Viiveanalyysissa käytettiin WLAN-tekniikkaa IEEE 802.11b ja siinä tarkasteltiin mobiilaitteen siirtymistä operaaraattori 1:sen kantavuusalueelta operaattori 2:sen kantavuusalueelle. Etenemisen oletettiin tapahtuvan lineaarisesti ja vakionopeudella. Tiedonsiirto tapahtui mediapalvelimen välityksellä UDP:n (User Datagram Protocol) avulla. UDP on yhteydetön protokolla, joka ei vaadi yhteyttä laitteiden välille, mutta mahdollistaa tiedostojen siirron. Analyysissa käyttäjä alkoi siirtyä vähitellen liityntäpiste 1:ltä (AP1) liityntäpiste 2:selle. Mikäli päätelaitteita olisi ollut useampi, niin kaikki laitteet olisivat aloittaneet siirtymisen yhden tukiaseman alueelta toisen alueelle samaan aikaan samalla nopeudella ja suunnalla. Mobiililaitteen liikenopeus oletettiin olevan 2km/h ja tiedonsiirtonopeudet mediapalvelimelle 7Kb/s ja 14Kb/s. Oli selvää, että mitä enemmän käyttäjiä liikkui tukiasemalta toiselle samaan aikaan, niin sitä enemmän oli kuormaa verkossa. Testissä havaittiin, että mikäli samanaikaisesti liikkuvia käyttäjiä oli alle neljä, niin viive oli käytännössä nolla. Kun puhuttiin nollaviiveestä, niin sillä tarkoitettiin sitä, että paketin siirtymisaika oli pidempi mediapalvelimen ja mobiililaitteen välillä kuin se aika, mitä kului itse tukiaseman vaihdossa. Käytännössä tätä viivettä ei siis huomattu sovelluskerroksella. Kun käyttäjien määrä kasvoi yli kahdeksaan, niin ei voitu puhua enää saumattomasta tukiaseman vaihdosta, koska viive kasvoi liian suureksi (viive yli 0,004s). Tämä johtui törmäyksistä MAC-kerroksella. Luonnollisesti suurempi tiedonsiirtonopeus (14Kb/s) kasvatti viivettä vielä entisestään. Tämä on havainnollistettu kuvassa 32 (Akhtar, Nadeem. Bria, A. Jennen, R. Markendahl, J. Miozzo, M. Pöyhönen, P. Rembarz, R & Simon, C 2007).



Kuva 32. Tukiaseman siirrosta aiheutunut viive tiedonsiirtonopeuksilla 7 ja 14 Kb/s (Akhtar, Nadeem. Bria, A. Jennen, R. Markendahl, J. Miozzo, M. Pöyhönen, P. Rembarz, R & Simon, C 2007).

8.4. Verkkojen yhteiskäytön vaikutus kuorman jakamiseen ja käytettävyyteen

8.4.1. Simulaation lähtökohdat

Viimeiseksi arvioitiin, että miten AN-konseptissa oli onnistuttu jakamaan resursseja paremmin eri verkkotoimijoiden kesken hyödyntämällä tehokkaampaa pääsyverkon valitsemistapaa ja näin ollen mahdollistaen paremman käytettävyyden sekä tehokkaamman tietoliikennekuorman jakamisen eri toimijoiden kesken. Toisin kuin nykytekniikassa AN-konseptissa päätös tukiaseman vaihdosta ei riipu ainoastaan signaalin laadusta vaan siinä otetaan huomioon myös yhteiskäytön merkitys, kustannukset, palvelujen jatkuvuus sekä operaattorin politiikka. Käytännössä liiketoimntakriteereihin perustuville ratkaisuille annetaan paljon enemmän jalansijaa. Skenaariossa oli käytössä lukuisia erilaisia verkko-operaattoreita ja palveluntarjoajia. Käyttäjillä oli testin aikana mahdollisuus olla mihin tahansa verkkoon yhteydessä. Käyttäjät olivat jatkuvasti yhteydessä vierasverkkoihin sillä oletuksella, että kotiverkoilla oli verkkovierailusopimukset (roaming) vierasverkkojen kanssa ja palvelutason sopimukset palveluntarjoajien kanssa. Arvioinnissa mobiililaitteet joko pysyivät omissa verkoissaan tai yhdistyivät toisiin verkkoihin riippuen siitä, minkä kriteerin perusteella tukiaseman vaihto suoritettiin tai sopimuksista eri operaattoreiden välillä. Näitä eri kriteerejä arvioitiin ja tutkittiin, mikä niistä on paras ja tehokkain sekä verkon että käyttäjän kannalta. Signaalikuormaa eri operaattoreiden keskuudessa ja

käyttäjän vaikutusta signaalikuormaan mitattiin jokaisen eri strategian kohdalla, jonka perusteella tukiaseman vaihto päätettiin suorittaa. Mittausten perusteella osattiin valita paras strategia liittyen päätökseen verkkoon liittymisestä. Kertauksena vielä, että verkon valintaa edelsi ensin verkon löytäminen ja palveluntarjoajan mainostamisvaihe sekä siihen liittyminen. AN joko mainosti itseään toiselle AN:lle, tarjosi resurssejaan ja palvelujaan käytettäväksi tai sitten AN sattumalta löysi toisen AN:n ja tiedusteli, mitä palveluja toiselta löytyi. Mikäli kyseessä oli mahdollisesti vierasverkko, niin siitä piti olla erillinen verkkovierailusopimus. Tämän jälkeen tehtiin valinta sopivasta kandidaatista. Verkkoon liittyminen piti sisällään yhteyden määrittelemisen sekä tietoturvan varmistuksen. Lopuksi neuvoteltiin kompositiosopimuksesta sekä sen toteuttamisesta, jonka jälkeen varsinainen tukiaseman vaihto voitiin aloittaa. Tässä yhteydessä tehtiin erikseen eri kompositiosopimukset vierasverkon ja kotiverkon vuorovaikutuksesta sekä vierasverkkoon liittymisestä (Markendahl, Jan. Pöyhönen, P & Strandberg, O 2007).

Simulaatiossa käyttäjälle annettiin vapaus valita haluamansa verkko eikä sitä haluttu pakottaa käyttämään oman operaattorin palveluja. Käyttäjä pystyi vapaasti valitsemaan vieraan verkon, mikäli se tuki sen strategiaa. On huomioitava, että käyttäjällä ei tarvinnut olla mitään liiketoimintasopimusta vieraan operaattorin kanssa. Sen sijaan käyttäjällä täytyi silloin olla liiketoimintasuhteet palveluntarjoajien kanssa tai oman operaattorinsa kanssa ja omalla operaattorilla oli puolestaan kumppanuus vierasverkkoa tarjoavan operaattorin kanssa.

Jotta pystyttäisiin valitsemaan optimaalisin päätöksentekoprosessi, luotiin eräänlainen jaettu päätöksentekomalli, jossa sekä laitteessa että verkossa sijaitsevat protokollan toiminnalliset kokonaisuudet (functional entities) ottivat osaa päätöksentekoprosessiin. Nämä toiminnalliset kokonaisuudet määrittelivät kriteerit pääsyvalinnalle ja ne koskivat moniradiotieresurssienhallintaa (MRRM), tukiaseman vaihdon ja sijainnin hallintaa sekä reitin valintaa. Nämä päätöksentekostrategiat olivat joko verkkoon perustuvia (network centric) tai päätelaitteeseen perustuvia (terminal centric). Analyysissä näitä kahta eri strategiaa verrattiin nykypäivän strategiaan, joka perustuu pitkälti siihen, että

tukiaseman vaihto tehdään signaalin vahvuuden perusteella, eikä niinkään ajatella liiketoimintaa (Markendahl, Jan. Pöyhönen, P & Strandberg, O 2007).

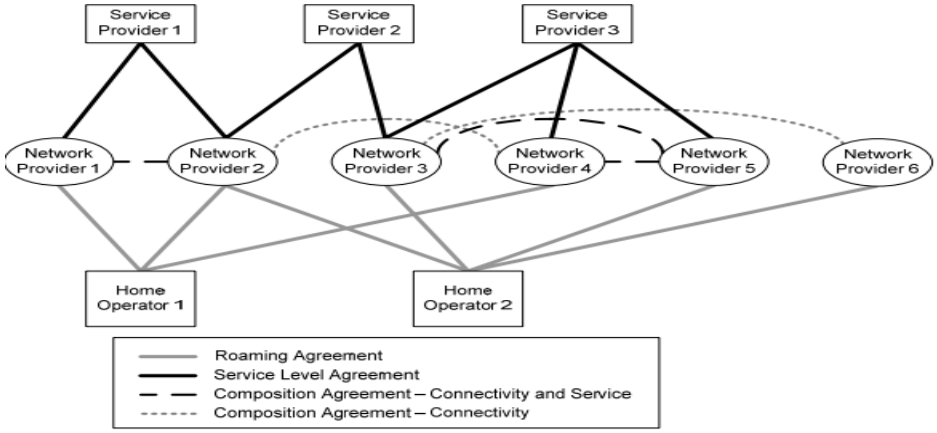
Päätelaitteeseen ja verkkoon perustuva strategia ottaa huomioon paremmin sekä verkon että käyttäjän intressit. Päätelaitteeseen perustuvassa valinnassa päätelaite havaitsee ensin esimerkiksi viisi mielestään hyvää yhteyttä, joista se päättää ensin valita kolme hyvää kandidaattia omien etujensa mukaisesti. Sen jälkeen päätelaite välittää näistä valinnoista tiedon verkolle, joka vuorostaan päättää jättää yhden kolmesta verkosta pois omien intressien mukaisesti. Jäljelle jää tämän jälkeen enää kaksi yhteyttä ja verkko välittää tiedot valinnoistaan päätelaitteelle. Näistä kahdesta yhteydestä päätelaite valitsee ”paremman” ja suorittaa tukiaseman vaihdon. ”Paremmalla” verkolla tarkoitaan AN-konseptissa sitä, että otetaan tukiaseman vaihdon yhteydessä huomioon signaalin laadun lisäksi myös muita tekijöitä liittyen verkkoon. Näitä tekijöitä voi olla muun muassa palvelun jatkuvuus, kustannukset ja operaattorin liiketoimintasuhteet. Verkkoon perustuvassa valinnassa puolestaan tilanne menee ihan samalla periaatteella kuin päätelaitekeskeisessä tilanteessa mutta päinvastaisella tavalla. Verkko valitsee ensiksi sopivat kandidaatit, välittää tiedon siitä päätelaitteelle, joka tekee omat valintansa ja lopulta verkko tekee lopullisen päätöksen sopivasta yhteydestä (Markendahl, Jan. Pöyhönen, P & Strandberg, O 2007).

Kun vertaamme näitä kahta AN-konseptin mukaisia tukiasemanvaihtoalgoritmeja käytössä oleviin tukiasemanvaihtoalgoritmeihin, niin voidaan sanoa, että nämä uudet tukiasemanvaihtoalgoritmit palvelevat paremmin lukuisia käyttäjien etuja. Käytössä olevissa tukiasemanvaihtoalgoritmeissa päätelaite ensiksi havaitsee saatavilla olevat yhteydet ja välittää tästä tiedon verkolle, joka saman tien tekee päätöksen sopivasta yhteydestä ja tämän jälkeen neuvoo päätelaitetta suorittamaan tukiaseman vaihdon. Tällainen valintapa ei anna jalansijaa muille kriteereille ja yleensä verkko tekee päätöksen sekä yhteydestä että palveluista. Tämä johtaa siihen, että erillisiä palveluntarjoajia ei huomioida lainkaan valintaprosesseissa. Tässä on myös asian liiketoiminnallinen kääntöpuoli; monet operaattorit ovat halunneetkin sitä, että asiakas on sidoksissa heidän verkkopalveluihinsa, eikä voi valita muuta. Siksi AN-konseptin pitäisi tarjota myös operaattoreille uusia ansaintamahdollisuuksia, tai muuten ne eivät

suostu sen mahdollistamiseen kuin laisäädännöllä määrätyllä pakolla. Tämä asettaa haasteita AN:lle. Verkon näkökulmasta katsottuna on äärimmäisen tärkeää, että AN-konseptissa hyödynnetään liiketoimintasopimuksia sekä vaaka- että pystytasolla. Tällä tarkoitetaan yhteistyösopimuksia palveluntarjoajien lisäksi myös muiden operaattoreiden kanssa (kts. kuva 24). Olemassa olevien liiketoimintasopimusten avulla verkko ja päätelaite saavat enemmän informaatiota, jonka perusteella sopiva yhteys voidaan valita. Näiden sopimusten lukumäärät määrittelevät, kuinka paljon tekijöitä pitää ottaa huomioon valintaprosessissa (Markendahl, Jan. Pöyhönen, P & Strandberg, O 2007).

Eri strategioiden arvioinnissa käytettiin simulointia, joissa käytettiin malleina satunnaisia käyttäjien tekemiä valintoja. Simuloinnissa oli käytössä 1000 mobiilia päätelaitetta satunnaisilla reittivalinnoilla 5x5 kilometrin alueella. Lisäksi mukana oli neljä laajalla alueella toimivaa operaattoria tarjoten palveluja ja kaksi WLAN-tukiasemaa. Simulointi suoritettiin kerran jokaista strategiaa kohden ja sen kesto oli 240s, jonka aikana tehtiin 2400 mittausta.

On olemassa kahdenlaisia sopimuksia joista toinen liittyy vain tarjottavaan yhteyteen ja toinen sekä yhteyteen että palveluihin. Nämä sopimukset voivat olla horisontaalisia tai vertikaalisia. Horisontaalisella sopimuksella tarkoitetaan eri operaattoiden välisiä liiketoimintasopimuksia, kun taas vertikaalisilla sopimuksilla tarkoitetaan operaattorin ja palveluntarjoajan välisiä liiketoimintasopimuksia (Markendahl, Jan. Pöyhönen, P & Strandberg, O 2007). Tämä on havainnollistettu kuvassa 33.



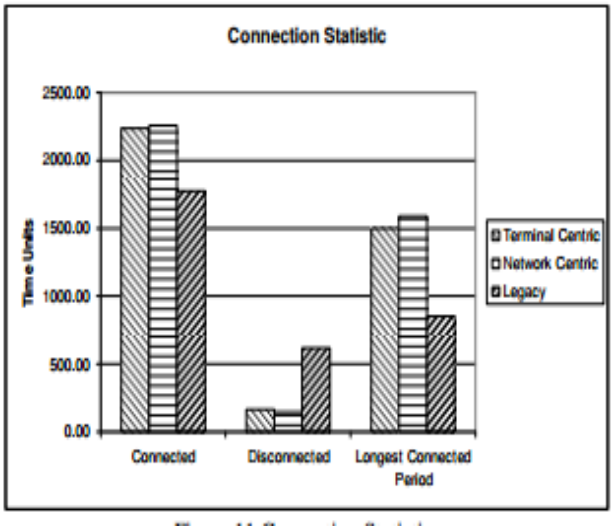
Kuva 33. Verkkotarjoajien ja palveluntarjoajien väliset liiketoimintasuhteet (Markendahl, Jan. Pöyhönen, P & Strandberg, O 2007).

Kun tarkastellaan vaakatasolla tapahtuvia verkontarjoajien välisiä sopimuksia, niin havaitaan kaksi kilpailevaa leiriä. Toiseen leiriin kuuluvat verkontarjoaja 1 ja verkontarjoaja 2, kun taas toiseen leiriin kuuluvat verkontarjoaja 3 ja verkontarjoaja 5. Kuvasta huomataan, että eri leirien osapuolten välille on muodostettu kompositio-sopimus sekä yhteydestä että palveluista. Näillä leireillä ei ole kuitenkaan keskenään mitään molemminpuolisia sopimuksia vaakatasolla, joiden avulla voitaisiin mahdollistaa saumaton tukiaseman vaihto vieraileville verkoille. Sen sijaan leireillä on vertikaaliset liiketoimintasuhteet ylhäällä oleviin palveluntarjoajiin ja se mahdollistaa kilpailun näiden kahden leirin välille. Vaakatasolla ja pystytasolla tehdyt sopimukset ovat äärimmäisen tärkeässä roolissa AN-konseptissa, sillä sopimusten avulla saadaan kerättyä tarvittava data jaettuun päätöksenvalintaprosessiin (Markendahl, Jan. Pöyhönen, P & Strandberg, O 2007).

8.4.2 Simuloinnin tulokset

Simuloinnin tuloksissa havaittiin selkeästi, että sekä verkkoon perustuva että päälaitteeseen perustuva pääsyvalinta takaa huomattavasti paremman resurssien hyödyntämisen nykystrategiaan verrattuna. Verkkoon perustuvassa ja päätelaitteeseen perustuvassa pääsyvalinnassa ei havaittu mitään merkittäviä eroja keskenään.

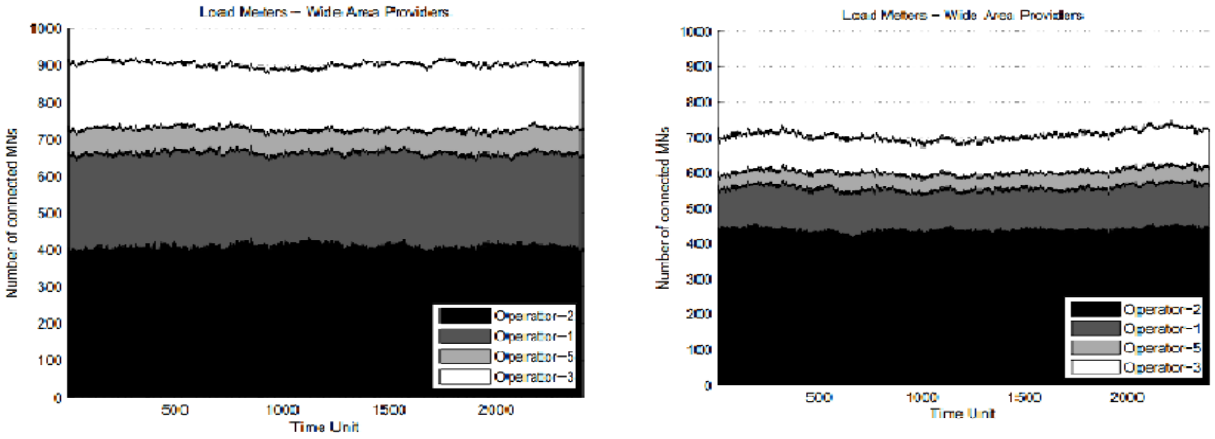
Tehokkaampi verkkojen hyödyntäminen mahdollisti aiempaa suuremman pääsyverkkojen kapasiteetin käytön palvelemaan useampaa käyttäjää ja avasi mahdollisuuden uudentyyppiseen liiketoimintaan, jolla voitiin saavuttaa nykyistä suurempia tuloja. Uusi jaettu pääsynvalinta-algoritmi mahdollisti tämän. Uuden strategian käyttö edellytti kuitenkin aiempaa useampia tukiaseman vaihtoja ja useampien päätelaitteiden hyödyntämistä kuorman tasaamisessa, sillä verkon tiedonsiirtomäärät lisääntyivät huimasti. Käytettäessä nykypäivän tekniikkaa pääsynvalinnassa, oli verkkoyhteyden menettäneiden mobiilien päätelaitteiden määrä (disconnected) huomattavasti korkeampi AN-konseptin mukaisiin strategioihin verrattuna. Lisäksi tarjolla olevien verkkojen tiedonsiirtokapasiteettia onnistuttiin uusien strategioiden ansiosta hyödyntämään tehokkaammin ja yhteyssessiot kestivät pidempään nykytekniikkaan verrattuna. Alla olevat kaaviot havainnollistavat tilannetta, miten eri strategiat vaikuttivat yhteyteen ja miten eri operaattorit hyötyivät resursseista (Markendahl, Jan. Pöyhönen, P & Strandberg, O 2007).



Kuva 34. Tilastoa **v**erkkoyhteyden saaneiden ja menettäiden päätelaitteiden määrästä eri strategioita kohden (Markendahl, Jan. Pöyhönen, P & Strandberg, O 2007).

Kuvan 34 diagrammi esittää, kuinka suuren osan simulaatioajasta (2400ms) päätelaitteet olivat yhteydessä verkkoon strategiaa kohden. Kaaviosta huomataan, että verkkoon perustuva valinta on aavistuksen verran parempi vaihtoehto yhteyden kannalta verrattuna päälaitteeseen perustuvaan valintaan. Kaavio 35 havainnollistaa periaatteessa

samaa asiaa kuin kuva 34, eli vertaa verkon hyödyntämistä uuden ja vanhan strategian välillä, mutta se kertoo myös tarkemmin, miten verkon hyödyntäminen jakautui neljän eri operaattorin kesken. Operaattorit, joihin viitataan olivat kuvassa 33. Operaattoreiden väliset liiketoimintasuhteet toisiinsa ja palveluntarjoajiin vaikuttivat lopputulokseen, miten verkon hyödyntäminen jakautui neljän eri operaattorin kesken. Operaattorit olivat operaattori 1, operaattori 2, operaattori 3 ja operaattori 5. Päätelaitteeseen perustuvaa strategiaa ei näissä kaavioissa huomioitu, sillä sen ero verkkoon perustuvassa strategiassa oli vähäinen.



Kuva 35. Verkkoon perustuva strategia vs. nykystrategia (Markendahl, Jan. Pöyhönen, P & Strandberg, O 2007).

Vasemmalla puolella verkkoon perustuvassa strategiassa oli keskimäärin 900 päätelaitetta yhteydessä verkkoon simulaation aikana, kun taas oikealla tällä hetkellä käytössä oleva strategiassa päälaitteita oli verkossa keskimäärin noin 700. Operaattorien yhteistyön avulla pystyttiin kuorman tasaamistakin tekemään huomattavasti paremmin. Ei ole sattumaa, että operaattorit 1 ja 2 olivat yhteistyön ansiosta parhaimmilla sijoilla. Erityisesti operaattori 2 onnistui saamaan omaan verkkoonsa 40–45 % päätelaitteista. Pitää ottaa huomioon, että sama päätelaite voi kuulua useaankin verkkoon samaan aikaan. Mielenkiintoisia tuloksista teki se, että vaikka operaattori 5:lla ja operaattori 3:lla oli yhdessä sama kattavuusalue kuin operaattori 2:lla, niin silti molemmat onnistuivat saamaan vain 15% päätelaitteista verkkoonsa. Tästä voi päätellä sen, että suuri kattavuusalue ei ole suoraan verrannollinen liittyneiden laitteiden määrään.

Operaattori 2:lla oli parhaimmat liiketoimintasuhteet. Sillä oli jopa tiettyjä paikkoja, jossa se oli ainoa toimija, joka tarjosi kattavuutta (Markendahl, Jan. Pöyhönen, P & Strandberg, O 2007).

Yleisesti voidaan todeta, että vertikaalisesti solmitut sopimukset ovat tärkeämpiä kuin vaakatasolla tapahtuvat, sillä operaattorin toimiessa esimerkiksi yksin, se ei välttämättä tarvitse siinä tilanteessa horisontaalisia sopimuksia muiden operaattoreiden kanssa. Tällaisessa tilanteessa ei tukiaseman vaihtaminen ole järkevää. Horisontaaliset sopimukset ovat kuitenkin tärkeitä yhteyden ja palveluiden ylläpitämiseksi siirryttäessä operaattorilta toiselle ja sillä tavalla operaattorilla on mahdollisuus päästä käsiksi uusiin asiakkaisiin ja asiakkailla vuorostaan on aina halutut palvelut käytettävissä. Horisontaaliset sopimukset myös vahvistavat tietyllä tapaa vertikaalisiakin liiketoimintasuhteita. Pitää muistaa, että AN-visiossa ideana on nimenomaan se, että tehdään yhteistyötä sillon, kun kaikki osapuolet hyötyvät siitä, mutta myös kilpaillaan tietyillä tasoilla keskenään. Pitäisi keksiä motivaatio sille, miksi operaattori haluaisi päästää omia asiakkaitaan toisen operaattorin verkkoon. Tämä motivaatio voisi olla esimerkiksi jokin erillislaskutus osapuolten välillä. Vaikka operaattorit haluaisivatkin omistaa omat asiakkaansa, niin pidemmällä aikavälillä se ei välttämättä ole tehokasta liiketoiminnan kannalta. Lisäksi asiakkaat tulevat vaativimmiksi, eivätkä halua joutua omistetuksi. Tämä asettaa operaattoreille lisähaasteita tietoturvan kannalta, kun määritellään sopimuksia ja strategioita verkkoon liittymiselle. On kuitenkin selvää, että AN-visio on mahdollista toteuttaa vain silloin, mikäli operaattorit saavat siitä lisätuloja. Toisena vaihtoehtona on pakottaa operaattorit mukaan lainsäädännöllä. (Markendahl, Jan. Pöyhönen, P & Strandberg, O 2007).

9. PÄÄTELAITTEIDEN KOMMUNIKAATIO NYKYTEKNIIKOILLA

Aikaisemmassa osiossa arvioitiin, miten AN:n soveltaminen vaikutti verkkojen väliseen yhteistyöhön, verkon resurssien hyödyntämiseen ja kuorman tasaamiseen päätelaitteiden välillä. Seuraavaksi olisi tarkoitus käydä läpi käytännössä, miten nykytekniikalla onnistuu eri verkkojen tiedonsiirto ja Internet-yhteyden jako. Tarkoitus on selvittää, kuinka paljon käyttäjän pitää itse tehdä päätelaitteeseensa säätöjä, jotta voidaan jakaa tiedostoja tai mahdollisesti jopa Internet-yhteys muille päätelaitteille. Lisäksi testataan, pystyykö muut päätelaitteet lennosta hyödyntämään isäntäkoneen nopeampaa Internet-yhteyttä, jos isäntäkone siirtyy 3G:sta WLAN:iin. Koska esitetyissä AN-testiskenaarioissa käytetyt tekniikat Bluetooth, WLAN ja matkapuhelinverkko (3G), niin niitä käytetään myös tämän työn yhteydessä toteutetussa testauksessa. Testauksessa tulee olemaan yksi Android käyttöjärjestelmällä varustettu taulutietokone eli tablet (Nexus 7), Windows 7:lla varustettu kannettava tietokone (Samsung RC510) sekä Meego käyttöjärjestelmällä varustettu Nokia N9. Verkkoina tullaan käyttämään likiverkkoa (PAN) sekä ad hoc -/infrastruktuuriverkkoa. Likiverkossa on aina kaksi laitetta yhteydessä toisiinsa. Halusin tarkoituksella ottaa erityyppisiä laitteita eri käyttöjärjestelmillä, jotta nähdään, mikä vaikutus sillä on laitteiden yhteensopivuuteen. Tarkoituksena on testata, miten näiden laitteiden välinen tiedonsiirto ja Internet-yhteyden jakaminen onnistuu käyttäen eri tekniikoita erilaisissa ympäristöissä.

Arvioinnissa tullaan kiinnittämään huomiota siihen, kuinka vaivalloista näiden eri verkkojen pystyttäminen on ja tarjoaako AN merkittävää hyötyä nykytekniikkoihin nähden. Kun eri laitteiden välisiä yhteyksiä testataan, niin vaatimuksena on, että yhteydenmuodostus onnistuu mahdollisimman kivuttomasti ja helposti ilman, että tarvitsee muokata käyttöjärjestelmää tai luoda omia skriptejä yhteyden muodostamiseksi. Mikäli laitteisiin pitää asentaa joitain lisäohjelmia yhteyden saamiseksi, niin se sallittakoon, mutta vaativimpiin toimenpiteisiin testauksessa ei ryhdytä. Ensin testataan, kuinka helposti onnistuu kahden laitteen yhdistäminen Bluetoothin välityksellä, jossa toinen laite tarjoaa Internet-yhteyttään toiselle. Internet-yhteytenä toimii Samsungin kannettavassa tietokoneessa ja Nokia N9:ssa sekä WLAN että 3G, mutta Nexus 7 tablet-laitteessa tuki löytyy ainoastaan WLAN:ille. Bluetooth-

testauksen jälkeen siirrytään testaamaan laitteita ad hoc -verkossa. Ad hoc -verkon testauksessa kukin laite luo vuorollaan oman ad hoc -verkkonsa, johon muut päätelaitteet yrittävät yhdistyä.

On selvää, että vaikka kyseessä on vain kolme eri päätelaitetta, niin ei voida mitenkään käydä läpi kaikkia mahdollisia skenaarioita, mitä näiden laitteiden välillä voi tapahtua AN-visioon perustuen, sillä skenaarioita olisi lukemattomia määriä. Tarkoitus on saada tuntumaa siihen, että miten laitteet osaavat keskustella keskenään nykypäivänä ja kuinka paljon käyttäjä joutuu määrittelemään asetuksia päätelaitteelleen. Laitteista Nokia N9 ja Nexus 7 hyödyntävät Bluetooth 4 tekniikkaa ja Samsungin kannettava tietokone Bluetooth 3:sta.

9.1. Internet-yhteyden jakaminen Bluetoothilla

Testauksen alussa tiedettiin jo ennestään, että useimmat matkapuhelimet osaavat toimia hyvin modeemina ja tarjota Internet-yhteyttään muille laitteille. Ne eivät kuitenkaan itse helposti havaitse muiden laitteiden DUN-/PAN-verkkoja, eivätkä näen ollen osaa hyödyntää toisen laitteen Internet-yhteyttä. DUN/PAN ovat profiileja, jotka luodaan Internet-yhteyden jakoon Bluetooth-yhteyttä muodostaessa. Jotkut toimillaitteet, kuten tietokoneet, hallitsevat molemmat profiillit. Esimerkiksi Android-laitteet hallitsevat vain PAN-verkon, ja Symbian-laitteet vain DUN-verkon. Jotkut laitteet osaavat toimia vain palvelimena, toiset asiakkaina ja jotkut osaavat toimia molempina. Tähän asiakas-palvelin malliin palataan myöhemmin. PAN (Personal Access Network) toimii nopeammin kuin DUN (Dial-Up Networking), mutta se vaatii yleensä erillisten sovelluspakettien asennuksen. Yleisin skenaario on se, että puhelin toimii modeemina eli palvelimena (DUN-server) ja tietokone asiakkaana (DUN-client) käyttäen kyseisen palvelimen eli puhelimen Internetiä.

Aluksi kaikkiin laitteisiin kytkettiin Bluetooth päälle ja määriteltiin asetuksissa laite näkyväksi muille Bluetooth-laitteille. Kun haluttiin muodostaa yhteys kahden eri laitteen välille, niin se vaati aina erillisen yhteydenmuodostuksen.

Yhteydenmuodostuksessa kummaltakin laitteelta kysyttiin, saako toinen laite ottaa yhteyttä ja kummassakin laitteessa piti hyväksyä erikseen kyseinen yhteydenmuodostus. Näin varmistettiin, että kumpikin laite näkee saman koodin, jotta voidaan varmistua toisen laitteen identiteetistä. Kun yhteydenmuodostus oli tehty, niin sen jälkeen laitteet pystyivät automaattisesti aina lähettämään toisilleen tiedostoja ilman, että pyyntöjä tarvitsi erikseen hyväksyä. Tämän ominaisuuden pystyi asettamaan jokaisen päätelaitteen asetuksista päälle. Päätelaitetta ainoastaan informoitiin, että kyseinen päätelaite on lähettämässä tiedostoja. Tämä oli hyödyllistä. Vaikka laite välillä poistuikin kantaman ulkopuolelle, niin silti se ei kuitenkaan vaatinut yhteydenmuodostusta toistamiseen löytääkseen saman laitteen uudelleen. Yhteys pysyi luotettavana niin kauan, kunnes toinen laite päätti purkaa sen. Tässä vaiheessa voitiin jo todeta, että ainakin tiedonsiirto onnistui melko jouhevasti eri laitteiden välillä, kunhan tiedostot eivät olleet liian suuria. Toki olisi ollut kätevämpää, mikäli yhteydenmuodostustakaan ei olisi tarvinnut erikseen tehdä, vaan se olisi tapahtunut automaattisesti ennaltamäärättyjen sääntöjen mukaan. Mutta tämä ei ole vielä nykypäivänä mahdollista.

Seuraavaksi yritettiin jakaa Internet-yhteyttä kahden päätelaitteen kesken, sillä Bluetooth-tekniikka ei tiedonsiirtorajoitustensa takia pysty tarjoamaan yhteyttä kuin yhdelle laitteelle kerrallaan (Microsoft). Ideana oli se, että toinen laitteista toimisi palvelimena ja toinen asiakkaana. Samsungin kannettava tietokone toimi asiakkaana ja Nokian matkapuhelin N9 palvelimena. Kun kannettavan tietokoneen ja matkapuhelimen välille oli muodostettu yhteys, niin kannettava tietokone alkoi välittömästi asentaa tarvittavia profiileja ja se osasi automaattisesti määrittää N9:n DUN-profiilin. Lisäksi tietokoneessa ei tarvinnut erikseen määrittää N9:sen käyttämän mobiiliyhteyden Soneran yhteyspistettä ”internet”, vaan tietokone osasi määrittää yhteysasetukset automaattisesti ja yhdistää yhdellä klikkauksella N9:n modeemiin, jonka jälkeen Internet-yhteys oli valmis käytettäväksi. Sen sijaan yhdistäessä Nexukseen, ei Internet-yhteyden jakaminen onnistunut yhtä sujuvasti. Tietokone osasi asentaa DUN-profiilin Nexus 7-laitteesta, mutta ei kuitenkaan onnistunut yhdistämään kyseiseen laitteeseen. Testauksessa jouduttiin asentamaan Nexuksen Androidiin PDANet niminen sovellus, jotta DUN-profiilin käyttö olisi mahdollista tablet-laitteessa. Tämän jälkeen yhteyden

muodostus onnistui ongelmitta. Tietokone onnistui käyttämään Android-laitteen WLAN-yhteyttä.

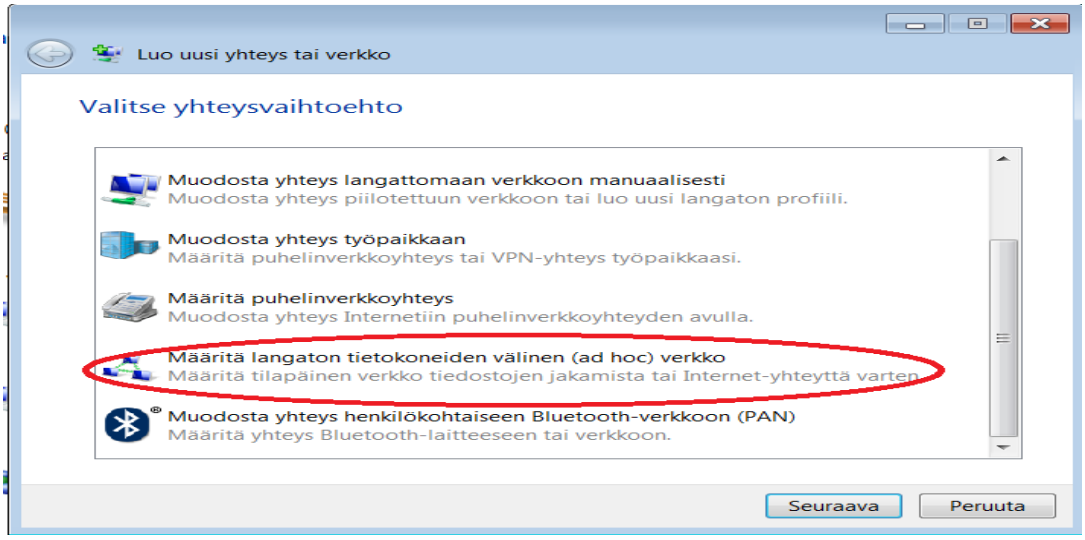
Kun Android-laitteesta tehtiin asiakas, niin se ei oletuksena osannut tukea DUN-asiakkaana olemista, vaan vaati erillisen ohjelman siihen. Ohjelma, jota käytettiin, oli nimeltään BlueVPN. Sen ansiosta Nexus 7 pystyi yhdistämään toiseen puhelimeen eli Nokiaan ja käyttämään sitä modeemina. Edellytyksenä oli, että päätelaite (palvelin) tuki DUN-profiilia. Android-laite onnistui ottamaan yhteyttä Nokia N9:ään ja BlueVPN:ään ei tarvinnut edes luoda mitään yhteyspistettä, vaan Nexus osasi automaattisesti tunnistaa N9:n käyttämän mobiiliyhteyden. Oli mielenkiintoista huomata, että BlueVPN ei suostunut käyttämään mitään muuta kuin N9:n mobiiliyhteyttä. Vaikka N9:n olisi laittanut yhdistämään WLAN:iin, niin BlueVPN olisi silti suostunut käyttämään vain N9:n 3G-yhteyttä. Käytettäessä BlueVPN:ää tietokoneeseen yhdistäessä ei Android-laite onnistunut Bluetoothin välityksellä yhdistymään siihen ja käyttämään tietokoneen Internetiä. Syitä tähän voi olla monia. Eräs epäilys on, että tietokoneen Bluetooth-pinosta ei yksinkertaisesti löydy tällaista DUN-server profiilia, vaan ainoastaan DUN-client. Ilmeisesti myöskään Windows 7 ei osaa toimia PAN-serverinä Androidin kanssa, vaikka Windowsin Bluetooth-asetuksista laittaisikin, että sallitaan PAN-laitteiden käyttää Windowsin modeemia Internet-yhteyden muodostamiseen. Xda-developers-foorumilla käytiin keskustelua asiasta ja tämän epäiltiin olevan syy, miksi Bluetooth-jako ei onnistu tietokoneesta.

PAN-serverin saa luotua tietokoneelle, mutta se vaatii lisäohjelmien asentamista Windowsiin muun muassa jonkinlaisen välityspalvelinserverin. Nexus 7 pitäisi puolestaan rootata, mikäli haluttaisiin käyttää sitä PAN-clientina. Roottauksella tarkoitetaan toimenpidettä, jossa laitteelta poistetaan ylimääräiset suojaukset ja hankitaan pääkäyttäjän oikeudet, jotta voidaan asentaa kyseisiä oikeuksia vaativia ohjelmia. Nokia N9:ä ei edes yritetty yhdistää kumpaakaan päätelaitteeseen, sillä se ei tukenut sitä oletuksena, vaan olisi vaatinut lukuisia toimenpiteitä ja konfiguroimista, jotta sen olisi saanut toiminaan asiakkaana. AN-visiossahan on nimenomaan ideana se, että tällaisia ylimääräisiä konfigurointeja ei tarvittaisi.

9.2. Internet-yhteyden jakaminen ad hoc- ja infrastruktuuriverkossa

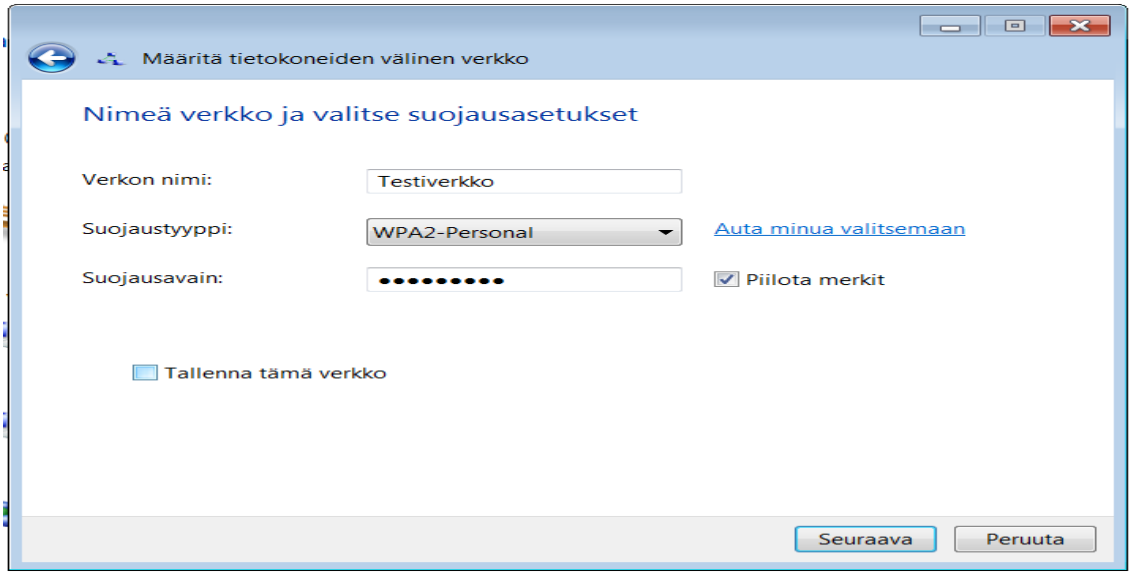
Ad hoc -verkossa tietokoneet ovat toisiinsa yhteydessä suoraan, eikä tieto kulje minkään reitittimen, palvelimen tai keskittimen kautta. Se on äärimmäisen nopea ja tehokas tapa saada esimerkiksi kaksi konetta yhdistettyä toisiinsa. Sen voi pystyttää joko väliaikaisesti tai pysyvästi käyttötarkoituksesta riippuen. Ad hocia voidaan käyttää esimerkiksi silloin, kun halutaan jakaa nopeasti tiedostoja tietokoneiden välillä tai työpaikalla, jossa vain yhdellä käyttäjällä on käytössä Internet-yhteys ja sitä halutaan jakaa muille koneille. Tällöin ei jokaiselle tarvitse erikseen järjestää Internet-yhteyttä (Netgear 2005). Testauksessa tullaan kiinnittämään huomiota siihen, kuinka paljon toimenpiteitä vaaditaan tällaisen verkon pystyttämiseen ja miten tiedonsiirto toimii laitteiden välillä. Isäntäkoneena käytetään vuorotellen jokaista aikaisemmin käytettyä kolmea päätelaitetta, joihin luodaan kyseinen ad hoc -verkko. Nokia N9 osaa luoda oletuksena oman ad hoc -verkkonsa, johon kaikki kyseistä verkkoa tukevat päätelaitteet voivat yhdistyä. Nexus 7:n Android sen sijaan ei osaa muodostaa omaa ad hoc -verkkoa, vaan sen muodostamaa verkkoa kutsutaan infrastruktuuriverkoksi (infrastructure network). Erona ad hoc -verkkoihin on, että infrastruktuuriverkossa tieto ei kulje laitteelta toiselle, vaan mukana on virtuaalinen palvelin, jonka kautta kaikki liikenne kulkee. Se on ad hociin verrattuna laadukkaampi ja turvallisempi verkko ja sillä on laajempi tuki. Ad hoc sopiikin ainoastaan sellaisiin sovelluksiin, joissa siihen liittyvien laitteiden määrä on vähäinen (Netgear 2005). Windows 7 osaa muodostaa sekä ad hoc- että infrastruktuuriverkon. Erilaiset WLAN-tukiasemat muodostavat aina infrastuktuuriverkon jakaessaan Internet-yhteyttään. Seuraavaksi kerrotaan vaihe vaiheelta, miten ad hoc -verkon luonti tapahtui tietokoneessa.

Ensiksi avattiin verkko- ja jakamiskeskus ohjauspaneelista, jossa määritettiin uusi yhteys tai verkko.

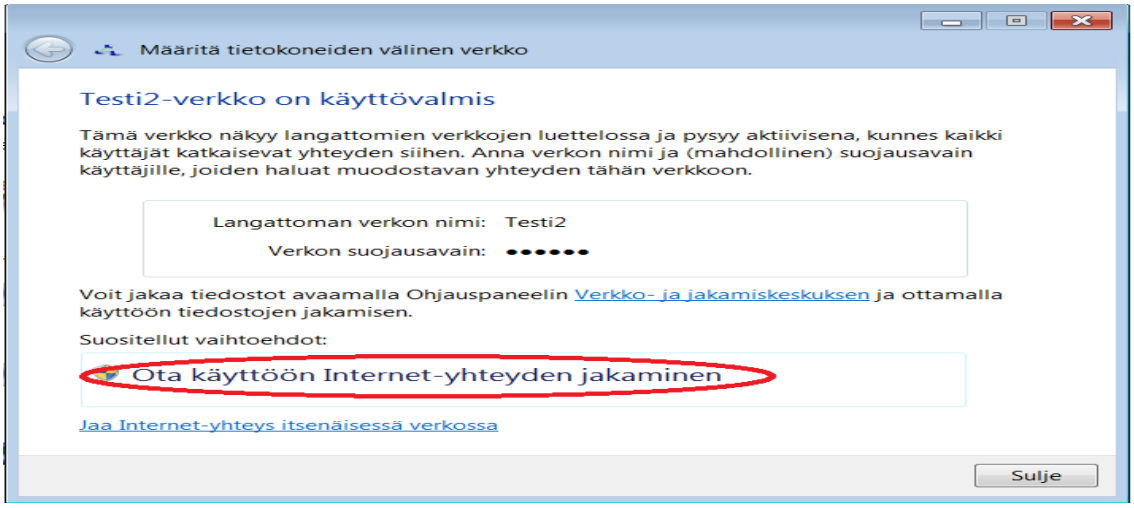


Kuva 36. Ad hoc -verkon luonti.

Sen jälkeen valittiin yhteysvaihtoehdoista ad hoc -verkko. Tämän jälkeen määritettiin suojausasetukset. Suojaustyyppinä käytettiin WPA2:sta, joka on turvallisin suojausmenetelmä WLAN:issa. Aika moni päätelaite tukee kyseistä suojaustapaa. Mikäli verkko haluttiin pystyttää pidemmäksi aikaa, pystyi asetukset tallentamaan. Mikäli verkon asetuksia ei tallennettu, niin verkko automaattisesti katosi sen jälkeen, kun yhteys siihen katkaistiin. Suojausasetusten jälkeen piti vielä erikseen määritellä verkolle Internetin jako. Tämän jälkeen ad hoc -verkko oli luotu.

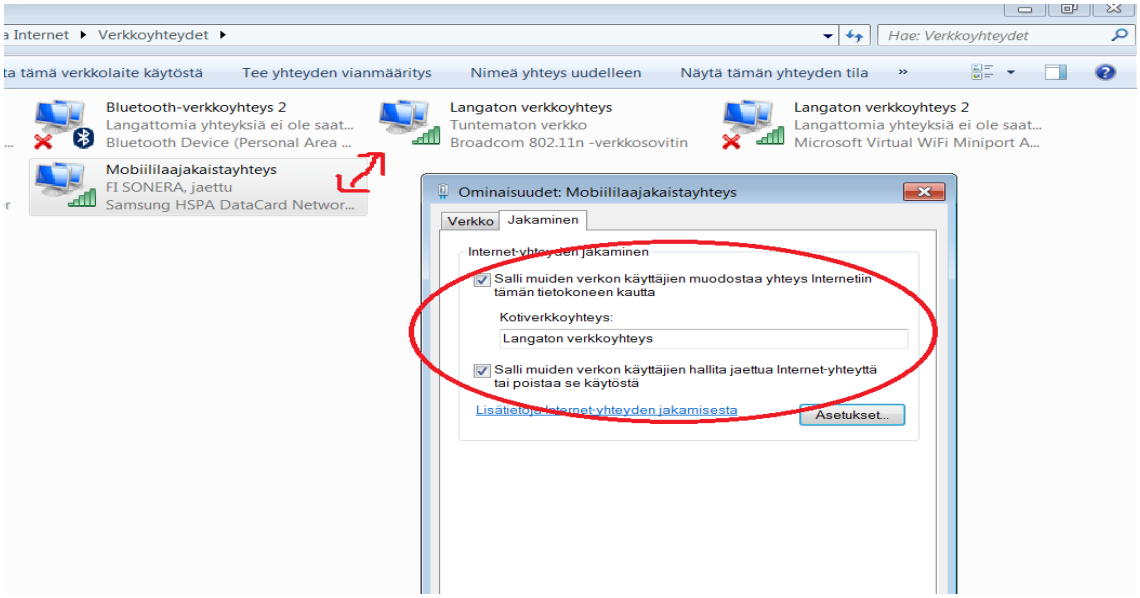


Kuva 37. Suojausasetusten asettaminen ad hoc -verkkoon.



Kuva 38. Internet-yhteyden lisääminen ad hoc -verkkoon.

Windows 7 osasi automaattisesti luoda linkin 3G-modeemin ja WLAN-sovittimen välille ja se mahdollisti Internet-yhteyden jaon muille koneille WLAN-yhteyden kautta. Jotta Internetin jako onnistuisi automaattisesti, niin tietokoneen piti olla yhteydessä 3G-verkkoon ennen ad hocin luontia. Muussa tapauksessa Internetin jakaminen piti tehdä manuaalisesti. Manuaalinen konfigurointi näytetään infrastruktuuriverkkojen yhteydessä. Arvioinnissa piti käyttää kannettavan tietokoneen 3G-modeemia Internet-yhteytenä, koska se ei suostunut jakamaan tietokoneen omaa WLAN:ia ad hoc -moodissa. Kannettavassa tietokoneessa oli käytettävissä Soneran 3G-yhteys. Kuvassa 39 näkyy mobiilaajakaistayhteyden ominaisuudet-välilehdellä, että valinnat ovat molemmissa Internet-yhteyttä koskevissa kohdissa ja kotiverkkoyhteydeksi on valittu ”langaton verkkoyhteys”, joka on Broadcom 802.11n-sovitin. Tämä luo yhteyden (linkin) 3G-modeemin ja Broadcomin välille.



Kuva 39. Jaettu mobiililaajakaistayhteys ad hoc -moodissa.

Mikäli tiedostonjako haluttiin kytkeä päälle, niin se piti tehdä erikseen verkko- ja jakamiskeskuksessa ja muuttaa jakamisen lisäasetuksia. Lisäksi päätelaitteisiin piti asentaa erikseen tiedostonhallintaohjelmat, jolla päästiin lähiverkon koneisiin.

Kun N9:ä ja Nexusta yritettiin saada liittymään verkkoon, niin kummankaan kohdalla se ei onnistunut ensimmäisellä kerralla. Nexuksen kohdalla se johtui siitä, että Android ei tue ad hoc -verkkoon yhdistämistä vaan ainoastaan infrastruktuuriverkkoa. Infrastruktuuriverkkoa näyttävät tukevan lähes kaikki laitteet. N9 osaa myös yhdistää infrastruktuuriverkkoon, mutta ei luoda sellaista. Ainoat laitteet, jotka kykenivät muodostamaan ad hoc -tukiaseman olivat Symbian-laitteet (v2 ja 3) ja testissä käytetty Nokia N9. Uudet Windows-puhelimetkin muodostavat infrastruktuuriverkon. Kun salaukseksi muutettiin heikompi WEP-salaus, niin sen jälkeen N9 onnistui yhdistämään verkkoon, mutta Android ei edelleenkään löytänyt edes ad hoc -verkon SSID:tä. N9 tukee WPA2:sta, mutta jostain syystä se ei osannut yhdistää kyseistä suojausta käyttävään verkkoon. Toki ongelma voi olla Windowsissakin. Kun N9 toimi tukiasemana, niin kannettava tietokone osasi yhdistää siihen ongelmitta ja käyttää N9:n matkapuhelinverkkoa, mutta Nexus ei osannut yhdistää siihen johtuen edellä mainituista syistä. Nexuksen luomaan infrastruktuuriverkkoon osasi yhdistää sekä kannettava että Nokia N9 ja Internet-yhteyden jako onnistui myös. Tässä yhteydessä N9 osasi käyttää

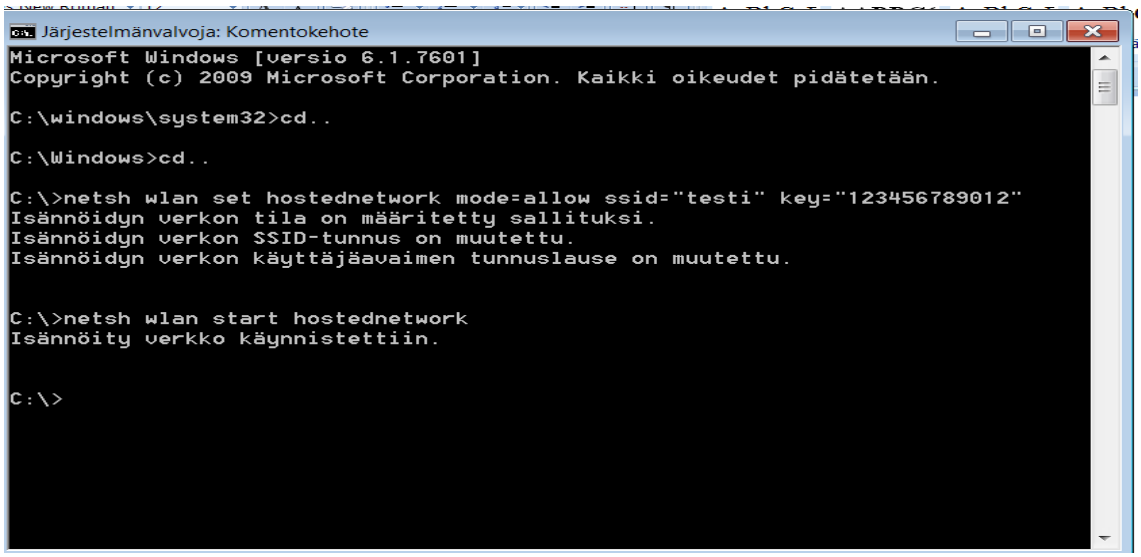
Nexuksen WPA2-suojausta, joten ilmeisesti Windowsissa oli jotain ongelmaa kyseistä suojausta käyttäessä N9:n kanssa.

Seuraavaksi testattiin, miten laitteiden välinen vuorovaikutus ja Internetin jakaminen onnistui infrastruktuuritilassa. Android-laitteella tämä jo testattiin, mutta nyt oli tietokoneen vuoro toimia isäntänä. Tietokone oli edelleen yhteydessä 3G-verkkoon. Infrastruktuuriverkon luominen aloitettiin avaamalla cmd-exe järjestelmänvalvojan oikeuksilla eli ”suorita” ja kirjoitettiin ”cmd”. Sen jälkeen kirjoitettiin seuraavat komennot:

Ensiksi tarkistettiin, onko WLAN-ajuria asennettu koneeseen:
c:> netsh wlan show drivers

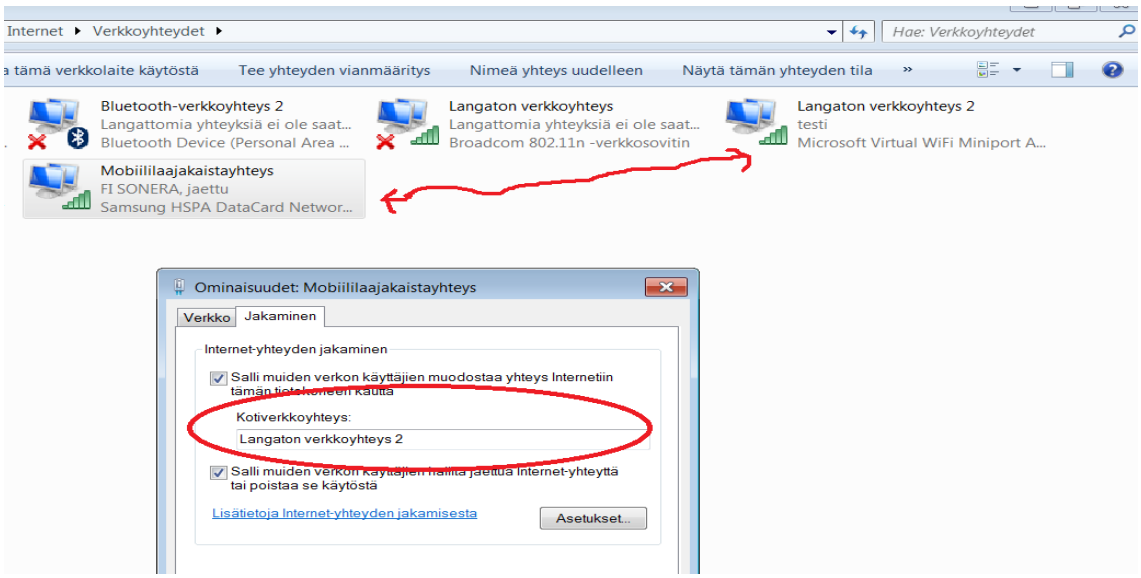
Sen jälkeen syötetiin SSID:ksi ”testi” ja salasanaksi ”123456789012”:
c:> netsh wlan set hostednetwork mode=allow ssid=”test” key=”123456789012”

Verkon käynnistyskomento:
c:> netsh wlan start hostednetwork



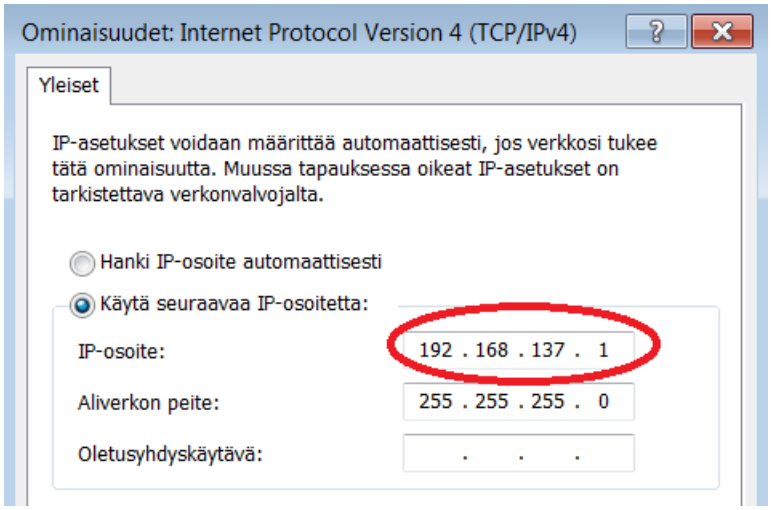
Kuva 40. Infrastruktuuriverkon luonti.

Tällä kertaa Windows ei osannut automaattisesti lisätä Internet-jakoa verkkoon, vaan se piti tehdä manuaalisesti. 3G-modeemia ei linkitetty Broadcomin kanssa vaan virtuaalisen Wi-Fi -portin kanssa (Microsoft Virtual Widi Miniport Adapter), joka viittaa juuri tähän virtuaaliseen liityntäpisteeseen infrastruktuuriverkossa. Alla olevassa kuvassa 41 näkyy tämä yhteys.



Kuva 41. Jaettu mobiililaajakaistayhteys infrastruktuuriverkossa.

Sekä ad hoc- että infrastruktuuriverkossa laitteiden pitäisi löytää samaan IP-osoiteavaruuteen kuin isäntäverkko. Päätelaitteiden pitäisi löytää IP automaattisesti, mutta tässä tilanteessa niin ei käynyt, vaan jouduttiin IP asettamaan manuaalisesti päätelaitteisiin. Esimerkiksi infrastruktuuriverkkoa luodessa IP osoite on yleensä muotoa 192.168.137.X. Tässä tapauksessa isäntäkoneen IP oli 192.168.137.1, joten Nexuksen IP voitiin määrittää olemaan esimerkiksi 192.168.137.5 ja N9:n 192.168.137.7. Tällä kertaa WPA-salaus ei tuottanut ongelmia kummankaan päätelaitteen kohdalla. Isäntäverkon IP:n sai selville avaamalla virtuaaliadapterista ominaisuudet ja siirtymällä kohtaan ”Internet Protocol Version 4 (TCP/IPv4)” ja klikkaamalla sen ominaisuudet.



Kuva 42. Isäntäverkon IP.

Infrastruktuuriverkko suljettiin komennolla: ”*netsh wlan stop hostednetwork*”.

Ad hoc- ja infrastruktuuriverkkoon yhdistäessä oli mahdollista tallentaa verkkoasetukset päätelaitteelle siten, että aina kun päätelaite saapui kuuluvuusalueelle, niin se osasi automaattisesti yhdistää ennestään tuttuun verkkoon. Tämä on hyödyllinen ominaisuus WLAN-verkoissa, sillä verkkoon ei tarvitse joka kerta erikseen yhdistää, vaan se tapahtuu itsestään, mikäli käyttäjä niin haluaa. Tiedonsiirron osalta WLAN- ja matkapuhelinverkko toimivat melko saumattomasti keskenään. Kun alettiin ladata tiedostoa päätelaitteen (N9) ollessa ad hoc- ja infrastruktuuriverkossa, niin tiedostonlataus ei missään vaiheessa keskeytynyt, vaikka poistuttiin kyseisten verkkojen kuuluvuusalueelta, vaan päätelaite siirtyi automaattisesti käyttämään 3G-verkkoa. Sama toimi myös toisinpäin, eli N9:n ladatessa tiedostoa 3G-verkossa, se osasi automaattisesti lennosta vaihtaa nopeampaan ad hoc- ja infrastruktuuriverkkoon ilman, että lataus katkesi. Samalla laitteet myös viestittivät toisilleen olevansa Bluetooth-kuuluvuusalueella keskenään. Tässä mielessä kommunikaatio toimi hyvin ja päätelaitteet hyvin nopeasti yhdistyivät keskenään, mikäli havaitsivat, että ennestään tuttu laite oli ilmestynyt kuuluvuusalueelle.

9.3. Johtopäätökset

Testauksessa haluttiin selvittää, miten saumattomasti päätelaitteiden ja ylipäänsä verkkojen yhteistyö onnistuu nykytekniikoilla ja tarvitaanko AN:n kaltaista konseptia ylipäänsä verkkojen väliseen kommunikaatioon. Testissä käytettiin kolmea eri päätelaitetta, jotka olivat Samsungin kannettava tietokone, Nokia N9 matkapuhelin ja Nexus 7-tablet. Jokaisessa päätelaitteessa oli käytössä eri käyttöjärjestemä, Kannettavassa tietokoneessa se oli Windows 7, Nexuksessa Android ja Nokia N9:ssa Meego. Jokaisessa päätelaitteessa oli käytössä myös Internet-yhteys. Kannettavassa tietokoneessa ja Nokia N9:ssa oli käytössä sekä 3G- että WLAN-yhteys, kun taas Nexus 7:ssa oli ainoastaan WLAN-yhteys. Uusin Bluetooth 4 oli käytössä Nokiassa ja Nexuksessa, mutta kannettavan versio oli Bluetooth 3.

Heti alkuun voidaan todeta, että Ambient Networks:in kaltaiselle toteutukselle on tarvetta. Testauksessa havaittiin selviä ongelmia jo Internet-yhteyden jakamisessa Bluetoothin välityksellä johtuen käyttöjärjestelmien tavasta tukea tiettyjä protokollia (DUN/PAN). Esimerkiksi tietokone sisälsi DUN-/PAN-profiilit, mutta se ei kuitenkaan osannut toimia palvelimena, koska siltä puuttui tarvittavat DUN- ja PAN-serverit. Tämän vuoksi se ei ainakaan oletuksena pystynyt toimimaan palvelimena ja jakamaan Internet-yhteyttään muille. Lisäksi muista päätelaitteista ei löytynyt oletuksena edes tarvittavia DUN-clienteja, jotta ne olisivat edes kyenneet käyttämään toisen laitteen modeemia. Android-laite tuki oletuksena vain PAN-profiilia. Ainut päätelaite, joka osasi toimia asiakkaana (client) oletuksena oli tietokone, joka onnistui käyttämään sekä Nexuksen että N9:n Internet-yhteyttä. Tälläiset clientit olisi saanut asennettua muihinkin päätelaitteisiin, mutta asentaminen olisi vaatinut paljon työtä erityisesti N9-laitteessa. Android-laitteen kohdalla riitti, että piti asentaa erillinen DUN-client-ohjelma, jonka avulla se onnistui käyttämään N9:sen DUN-profiilia ja täten N9 onnistui jakamaan Internet-yhteyttään Nexukselle. N9 sisälsi oletuksena DUN-serverin ja osasi oletusarvoisesti jakaa Internet-yhteyttään muille päätelaitteille. Ongelmaksi muodostui se, kun N9 yhdistettiin WLAN:iin, niin siitä huolimatta kannettava tietokone ja Nexus 7 eivät osanneet hyödyntää N9:sen parempaa yhteyttä, vaan hyödynsivät edelleen hitaampaa mobiiliyhteyttä. N9 pystyi itse käyttämään nopeampaa WLAN-yhteyttään,

mutta ei kuitenkaan jakamaan sitä muille päätelaitteille. Tietokoneen osalta tätä asiaa ei pystytty testaamaan, koska sen Internet-yhteyden jakoa ei saatu toimimaan Bluetoothilla. Jos otetaan kantaa laitteiden väliseen tiedostonsiirtoon, niin siitä ei ole mitään pahaa sanottavaa. Laitteiden keskenäinen yhteydenmuodostus vaati ensimmäisellä kerralla töitä, mutta sen jälkeen tiedostonsiirrot onnistuivat helposti, kun laitteet olivat toisilleen ennestään tuttuja ja päätelaitteet hyvin nopeasti aistivat toistensa läsnäolon ja ilmoittivat siitä käyttäjälle. Toisaalta AN-visiossa keskenäinen yhteydenmuodostuskin pitäisi tapahtua lennosta ilman käyttäjän sekaantumista.

Mitä tulee ad hoc -verkkoihin, niin niiden pystyttäminen Internet-yhteyden jaolla ei ollut mitenkään vaikeaa, ja se tarjosi nopeamman ja yhteensopivamman tavan laitteiden vuorovaikutukseen Bluetoohiin verrattuna. Tässäkään yhteydessä ei kuintenkaan vältytty ongelmilta. Android-laite ei osannut tukea ad hoc-verkkoa, koska sitä tukea ei ole haluttu lisätä Android-käyttöjärjestelmään. Android ei löytänyt edes SSID:tä, johon se olisi voinut yhdistää päästäkseen verkkoon. Sen sijaan N9 tuki ad hocia ja onnistui yhdistämään verkkoon, tosin ei ensimmäisellä kerralla, sillä N9 ei halunnut yhdistää WPA2-salattuun verkkoon, vaikka se sitä tukeekin. Kun suojaus vaihdettiin heikompaan WEP-salaukseen, niin ongelmia ei enää ilmennyt. N9 onnistui jakamaan kannettavalle tietokonelle Internet-yhteyttään ad hoc -moodissa, mutta ei Nexukselle. Nexus vuorostaan jakoi yhteyttään muille päätelaitteille onnistuneesti infrastruktuuriverkossa.

Kun luotiin infrastruktuuriverkko virtuaalireitittimellä kannettavassa tietokoneessa, niin molemmat päätelaitteet onnistuivat yhdistymään siihen, koska infrastruktuuriverkolla on laaja tuki. Mikäli päätelaite ei osannut automaattisesti hakea IP-osoitetta, niin se piti määritellä staattisena päätelaitteen asetuksiin, jotta IP olisi samassa osoiteavaruudessa kannettavan kanssa.

Yleinen ongelma, joka ilmeni sekä ad hoc- että infrastruktuuriverkkossa liittyi myös Internet-yhteyden jakoon. Laitteet osasivat jakaa erinomaisesti yhteyttään muille osapuolille sekä 3G- että WLAN-verkossa. Ongelmana kuitenkin oli, että mikäli kannettava siirtyi infrastruktuuriverkossa 3G:sta WLAN-yhteyteen, niin se ei osannut automaattisesti jakaa uutta nopeampaa yhteyttään muille päätelaitteille. Tämä johtui

siitä, että kannettava tietokone suostui jakamaan muille vain sitä Internet-yhteyttä, johon oli määritelty kyseinen jako-ominaisuus. Internet-jakoa ei pystynyt määrittelemään etukäteen kahteen verkkoon samanaikaisesti, vaan ensiksi piti poistaa jako mobiililaajakaistayhteydeltä ja vasta sitten siirtää se langattomaan verkkoyhteyteen eli WLAN:iin. AN:ssä tällaista ongelmaa ei saisi olla, vaan Internet-jaon tulisi tapahtua automaattisesti myös uudessa nopeammassa verkossa. Ad hoc -verkossa ei edes onnistunut Internet-jako WLAN-yhteydessä lainkaan, vaan ainoastaan matkapuhelinverkon välityksellä.

Kun otetaan huomioon kaikki epäkohdat ja ongelmat, mitä tähän mennessä on käyty läpi, niin ei voida puhua mistään saumattomasta verkkojen yhteistyöstä, jollainen AN-visiossa tulisi olla. Jokaisessa yhteysskenaariossa ilmeni ongelmia yhdessä tai useammassa päätelaitteessa. Joko yhteensopivuus oli puutteellinen tai sitten se puuttui kokonaan. Päätelaitteet hallitsivat tiedostojen vaihdon keskenään melko hyvin erityisesti Bluetoothilla, mutta sitten kun mukaan otettiin Internet-jako, niin ilmeni huomattavasti enemmän ongelmia erityisesti Bluetoothin kohdalla. Kun käytettiin ad hoc- ja infrastruktuuriverkkoja, niin Internetin jakaminen helpottui, mutta siltikin ongelmia vielä riitti. Internet-jako Bluetooth-verkolla olisi tehonkulutukseltaan taloudellisempi vaihtoehto, mutta nykyisellään Bluetooth ei siihen valitettavasti sovellu, vaan se toimii pikemminkin tiedonsiirtovälineenä. Tosin tiedostot eivät saa olla liian suuria, sillä testien mukaan Bluetoothilla 35 Mt:n tiedoston siirto päätelaitteelta toiselle (eli kannettavalta taulutietokoneelle) kesti 10 min, kun taas ad hoc- ja infrastruktuuriverkossa siihen meni vain 40 sekuntia WLAN:in välityksellä.

Bluetooth 3 pystyy teoriassa jopa 24 Mbit:n nopeuteen (Microsoft). Käytännössä tiedonsiirtonopeus oli kuitenkin huomattavasti hitaampi, mutta Internetiä jakaessa eivät Bluetoothin rajoitukset merkittävästi suoraan vaikuttaneet Internet-yhteyden nopeuteen 3G-yhteyteen verrattuna. Tietoturvan osalta Bluetooth soveltuu hyvin tiedostojen vaihtoon. Bluetooth-verkossa tietoturva muodostuu uuden laitteen autentikoinnista sekä siirrettävän tiedon salauksesta. Näiden hallintaan käytetään laitteen MAC-osoitetta, kahta salaista avainta sekä autentikoinnissa muodostettavaa satunnaislukua. Autentikointi perustuu kättelyviestien vaihtoon, joka voidaan suorittaa molempiin

suuntiin. Näin pienennetään niin sanotun naamioinnin mahdollisuutta. Varsinainen salaus tapahtuu E0-nimisellä jonosalaimella (Microsoft).

WLAN soveltuu puolestaan paremmin Internet-yhteyden jakoon suuremman nopeuden ja yhteensopivuuden ansiosta. Jokainen päätelaite osasi kuitenkin luoda oman hotspottinsa. Mikäli AN-visio saataisiin toteutettua täydellisesti, niin varmasti verkko ja päätelaite tietäisivät itse aina, millä tekniikalla missäkin tilanteessa on tehokkainta ja turvallisinta jakaa Internet-yhteyttä tai millä tavalla jakaa tiedostoja keskenään. Tekniikat eivät kuitenkaan ole toisiaan poissulkevia, vaan tilanteesta riippuen voidaan aina käyttää sitä parasta vaihtoehtoa, mikä verkon tai päätelaitteen asetuksiin sopii.

YHTEENVETO

Työssä perehdyttiin Ambient Networks:in visioon ja sen hyödyntämiseen liiketoimintaympäristössä. AN:n ideana on, että päätelaitteet pystyisivät olemaan ympäristöstä ja verkkotypistä riippumatta aina yhteydessä toisiinsa ja sitä kautta myös Internetiin. AN:ssa operaattorit olisivat keskenään tiiviimmin yhteistyössä ja konsepti mahdollistaisi operaattoreille uudentyyppisiä liiketoimintamalleja. Jokainen käyttäjä voisi toimia tiiviimmin yhteistyössä operaattorin kanssa tai toimia jopa itse operaattorina tai laskuttajana, mikäli joku toinen käyttäjä haluaisi käyttää kyseisen käyttäjän päätelaitteen Internet-yhteyttä.

Ensimmäisiä merkittäviä AN-vision kokeiluja on ollut samanniminen EU-projekti, jonka ensimmäisessä vaiheessa luotiin yhteinen hallintafunktio (ACS) AN:n sisällä, joka käsitti erilaisia toiminnallisuuksia liittyen laadunvalvontaan, eri verkkojen yhteensopivuuteen, turvallisuuteen ja sopimuksiin osapuolten välillä. Tarkoitus oli, että jokainen päätelaite (verkko) pitäisi sisällään tällaisen hallintafunktion, jonka avulla pystyttäisiin lisäämään eri verkkojen yhteensopivuutta ja takaamaan turvallinen verkkojen yhdistyminen. Sopimukset pitivät sisällään muun muassa sen, missä olosuhteissa yhdistyminen voisi tapahtua sekä muita ehtoja yhdistymiselle. Tutkijat testasivat projektin toisessa vaiheessa AN-vision hyödyllisyyttä ja siinä todettiin, että hyödyntämällä uusia verkkoon ja päätelaitteisiin perustuvia strategioita pystyttiin verkon kuormaa jakamaan tasaisemmin eri päätelaitteiden välillä ja useampia päätelaitteita oli yhteydessä verkkoon. Lisäksi yhteyden kestot olivat pidempiä verrattuna nykystrategiaan. Liiketoiminnassa erilaiset sopimukset operaattoreiden ja palveluntarjoajien välillä sekä vaaka- että pystytasolla lisäävät operaattoreiden tuloja ja myös käyttäjä hyötyi siitä pääsemällä aina haluamiinsa palveluihin oikealla hetkellä.

Nykypäivänä lukuisat erilaiset verkkotyypit ja -ympäristöt (esim. Bluetooth, WLAN, 3G) erilaisine protokollineen aiheuttavat sen, että verkkojen välinen vuorovaikutus ei toimi saumattomasti keskenään, vaan vaaditaan paljon manuaalisia konfiguraatioita päätelaitteeseen. Tämä huomattiin myös ”proof on concept” -testauksissa, jotka

suoritettiin kolmen eri päätelaitteen kesken. Jokaisessa päätelaitteessa oli eri käyttöjärjestelmä. Testeissä ilmeni, että eri käyttöjärjestelmien tuki erityyppisille tekniikoille tuotti suuria vaikeuksia laitteiden välisessä yhteistyössä ja erityisesti Internet-yhteyden jakaminen ja siihen yhdistäminen saumattomasti tuotti ongelmia eri päätelaitteille. Päätelaitteilla ei ollut yhteneväistä tukea eri tyyppisille tekniikoille. Joissain tilanteissa jopa toisen päätelaitteen luomaan verkkoon liittyminen tuotti vaikeuksia ja vaadittiin hyvin paljon manuaalisia toimenpiteitä, jotta saatiin aikaiseksi päätelaitteiden välinen keskinäinen verkko Internet-yhteydellä. Vaikka tällainen Internet-yhteys saatiin jaettua muille laitteille, niin siitä huolimatta nopeampi WLAN-yhteyden jako ei onnistunut saumattomasti isäntäkoneen siirtyessä 3G-yhteydestä WLAN-yhteyteen. Puutteita löytyi paljon nykytekniikoista, vaikka tiedonsiirto toimiikin nykyään melko hyvin siirtyessä verkosta toiseen. Nykytekniikoista kuitenkin puuttuu kuitenkin Ambient Networks -vision mukainen yhteinen hallintaprotokolla, joka mahdollistaisi sen, että nämä verkot pystyisivät paremmin keskustelemaan keskenään ja osaisivat paremmin ottaa huomioon käyttäjän asetuksissaan määrittelemät tarpeet.

AN-arkkitehtuuri vaikuttaa erittäin hyödylliseltä päivitykseltä nykytekniikoihin, mutta on vielä paljon asioita, joita tulee ottaaa huomioon, jotta tällaista aina läsnä olevaa verkkoa voitaisiin soveltaa käytännössä. AN on käsitteenä äärimmäisen laaja ja tässä työssä ei suuresta kiinnostuksesta huolimatta pystytty käsittelemään kaikkia siihen liittyviä asioita. Erilaisia jatkotutkimuksia tästä kyseisestä aiheesta voi olla useita. Jatkotutkimuksena voitaisiin esimerkiksi selvittää, miten pystytään varmistamaan tietoturvan kannalta kahden verkon liittyessä toisiinsa yhteiskäyttöä varten, että toinen osapuoli on luotettava. Työssä todettiin, että WLAN- ja 3G-verkko itsessään ovat turvallisia verkkoja, mutta miten pystytään määrittämään, että toisen osapuolen verkko on turvallinen käyttää? Toinen tutkimusaihe voisi liittyä asetuksiin, joiden perusteella verkko tai päätelaite päättää liittyä tai jättää liittymättä toiseen verkkoon. Millä tavalla käyttäjää voitaisiin informoida toisen verkon kiinnostuksesta vai tarvitseeko käyttäjää aina edes informoida? Ohjelmoinnista kiinnostunut voisi paneutua erilaisten liikkuvien sovelluksien arkkitehtuuriin. Millä tavalla ohjelmat pitäisi suunnittella, että niiden suorittamista pystyttäisiin jatkamaan lennosta toisessa verkossa tai mahdollisesti jopa toisessa päätelaitteessa? AN tarjoaa erilaisia kiinnostuksen kohteita johtuen sen laajoista

sovellusmahdollisuuksista liiketoiminnassa ja teknologiassa koskien lähes kaikkia käyttäjiä.

LÄHDELUETTELO

Abramowicz, Henrik. Karl, H. Niebert, N. Prehofer, C & Schieder A (2007). Ambient Networks-An Architecture for Communication Networks Beyond 3G. Berliini: Teknillinen yliopisto. Tietoliikenne.[Online][siteerattu 10.01.2013]. Saatavana World Wide Webistä: <URL: http://www2.tkn.tu-berlin.de/publications/papers/karl_ambient_networks.pdf

AK media (2012). Tietoverkot. [Online][siteerattu 28.11.2012]. Saatavana World Wide Webistä: <URL: http://www.2kmediat.com/tietoverkot/tekijat2.asp>.

Akhtar, Nadeem. Bria, A. Jennen, R. Markendahl, J. Miozzo, M. Pöyhönen, P. Rembarz, R & Simon, C (2007). Validation of the Ambient Networks System Architecture. [online][siteerattu 12.02.2013]. Saatavana World Wide Webistä: <URL: http://www.ericsson.com/res/thecompany/docs/journal_conference_papers/service_layer/Validation_of_the_Ambient_Networks_System.pdf>.

Boman, G. Horn, P. Howard & V. Niemi (2002). UMTS security.[online][siteerattu 11.12.2012].Saatavana World Wide Webistä: URL:< http://www.tkn.tu-berlin.de/curricula/ws0405/vl-umts/UMTS%20Security%20IEE.pdf>.

Campos, Rui. Kappler, C. Pinho, C. Pöyhönen, P. Ricardo, M & Ruela, J (2005). INESC Teknologia & Tiede. Dynamic and Automatic Interworking between Personal Area Networks using Composition. [Online][siteerattu 30.12.2012]. Saatavana World Wide Webistä: <URL: http://telecom.inescporto.pt/~rcampos/Dyn_and_Automatic_Interworking_between.pdf >.

Colliander, Andreas (1999). ISOn OSI-mallin rakenne ja käyttö. Aalto-yliopisto. Teknillinen korkeakoulu: Sähkö- ja tietoliikennetekniikan osasto. [Online][siteerattu 29.11.2012]. Saatavana World Wide Webistä: <URL: http://www.tml.tkk.fi/Studies/Tik-110.300/1999/Essays/essee_OSI.html>.

Digitodayn artikkeli (2010). Kännykän vakoilu onnistuu reilun tonnin laitteilla [Online][09.12.2012].Saatavana World Wide Webistä:<URL: http://www.digitoday.fi/tietoturva/2010/08/02/kannykan-vakoilu-onnistuu-reilun-tonnin-laitteilla/201010625/66>.

Haavisto, Henri (2009). Tietoturva mobiiliverkoissa [Online][siteerattu 11.12.2012]. Seinäjoki: Seinäjoen ammattikorkeakoulu. Saatavana World Wide Webistä: URL:<https://publications.theseus.fi/bitstream/handle/10024/3331/Haavisto_Henri.pdf?sequence=1>.

Havukainen, Kalle (2010). WLAN-salausmenetelmät ja tietoturva. [Online][siteerattu 13.12.2012]. Opinnäytetyö. Mikkelin ammattikorkeakoulu: Tietotekniikan koulutusohjelma. Saatavana World Wide Webistä: URL: <http://publications.theseus.fi/bitstream/handle/10024/12660/ Havukainen_Kalle.pdf?sequence=1>.

Heikkilä Jussi & Pasi Korhonen (1999). Matkapuhelinten sukupolvet. Aalto-yliopisto. Teknillinen korkeakoulu: Sähkö- ja tietoliikennetekniikan osasto. [Online][siteerattu 05.12.2012]. Saatavana World Wide Webistä: <URL: http://www.netlab.tkk.fi/opetus/s38118/s99/htyo/47/index.shtml >.

Heikkilä, Tommi (1999). GSM –verkon salaus [Online][siteerattu 09.12.2012]. Opinnäytetyö. Espoo: Aalto- yliopisto teknillinen korkeakoulu. Saatavana World Wide Webistä: URL:<http://www.netlab.tkk.fi/opetus/s38118/s99/htyo/10/harj_6.shtml>.

Huitema, George. Markendahl, J & Rietkerk O (2006). Business roles enabled by Ambient Networking to provide access for anyone to any network and service. Ruotsi: Kuninkaallinen teknillinen korkeakoulu. [Online][siteerattu 09.02.2013]. Saatavana World Wide Webistä:<URL: http://sprouts.aisnet.org/482/1/ Policy_Issues_2_3.pdf>.

Jacquet, Philippe (2002). Ambient Network. [Online][siteerattu 28.12.2012]. Saatavana World Wide Webistä: http://www.ercim.eu/publication/Ercim_News/enw48/jacquet.html>.

Kanniainen, Topi (2011). Sinunkin puhelintasi saatetaan salakuunnella. [online][siteerattu 09.12.2012]. URL: <http://www.taloussanomat.fi/tietoliikenne/2011/01/08/sinunkin-puhelintasi-saatetaan-salakuunnella/2011199/12>.

Kerttula, Esa (1998). Tietoverkkojen tietoturva. Helsinki: Oy Edita Ab. 510s. ISBN 951-37-2672-x.

Lappeenrannan teknillinen yliopisto (2000). OSI. [Online][siteerattu 29.11.2012]. Saatavana World Wide Webistä <URL: http://www2.it.lut.fi/kurssit/03-04/010602000/virtuaalimateriaali/04-protokolla/osi.html>.

Leino, Raili (2005). Mobiilitietoturva ei anna aihetta paniikkiin [Online][siteerattu 09.12.2012]. Saatavana World Wide Webistä:<URL: http://www.tekniikkatalous.fi/ict/article33293.ece >.

Markendahl, Jan. Pöyhönen, P & Strandberg, O (2007). Impact of operator cooperation on traffic load distribution and user experience in Ambient Networks business scenarios. [Online][siteerattu 24.2.2013]. <URL: http://msbpwp01.marshall.usc.edu/assets/006/5589.pdf>.

Mcfarlane, Steve (2011). The Differences Between Intranet, Internet, and Extranet. BRIGHT HUB.[Online][siteerattu 02.12.2012]. Saatavana World Wide Webistä: <URL:http://www.brighthub.com/computing/enterprise-security/articles/63387.aspx>.

Microsoft (2012). Mitä eroa on keskittimellä, kytkimellä, reitittimellä ja tukiasemalla? [Online][siteerattu 28.11.2012].Saatavana World Wide Webistä: <URL: http://windows.microsoft.com/fi-FI/windows-vista/How-do-hubs-switches-routers-and-access-points-differ>.

Mitchell 2003. Introduction to Network Types. [Online][siteerattu 05.12.2012].Saatavana World Wide Webistä: <URL:http://compnetworking.about.com/ od/basicnetworkingconcepts/a/network_types.htm>.

Netgear (2005). Selecting Between Infrastructure and Ad Hoc Wireless Modes.[Online][siteerattu 29.02.2013]. Saatavana World Wide Webistä: <URL:http://kb.netgear.com/app/answers/detail/a_id/954/~/ selecting-between-infrastructure-and-ad-hoc-wireless-modes>.

Networkworld (2010). ITU softens on the definition of 4G mobile. [Online][siteerattu 05.12.2012]. Saatavana World Wide Webistä:<URL:http://www.networkworld.com/ news/2010/121710-itu-softens-on-the- definition.html >.

Niemi, Valtteri & Kaisa Nyberg (2003). UMTS security [Online][siteerattu 11.12.2012]. Saatavana World Wide Webistä: URL:<http://www.scribd.com/doc/52478879/38/MAPsec>.

Oulun kauppaoppilaitos (2004). Verkon topologiat. [Online][siteerattu 27.11.2012]. Saatavana World Wide Webistä: <URL:http://www.okol.org/verkkokurssit/datanomi/ tietojarjestelmien_kaytto_ja_kehittaminen/lahiverkko_internet/lanjaint/ johdanto_verkkotekniikkaan/jvt.htm>.

Rantala (2006). Sensoriverkot älykkäissä ympäristöissä. [Online][siteerattu 05.12.2012]. Harjoitustyö. Saatavana World Wide Webistä: < http://www.ele.tut.fi/teaching/ele-7100/vuosi06-07/harjoitustyot/Rantala_Sensoriverkot.pdf >.

Takala (2012). Matkapuhelinten tietoturva. [siteerattu 05.05.2013]. Kandidaatintutkielma.

Tukiainen, Kimmo (2005). Wireless LAN. [Online][siteerattu 27.11.2012]. Lappeenrannan teknillinen yliopisto: Tietotekniikan osasto. Saatavana World Wide Webistä: <URL: http://www2.it.lut.fi/kurssit/04-05/010626000/linux-tyot/WLAN-Kimmo_Tukiainen-raportti.pdf>.

Tuominen, Toni (2005). WLAN-tietoturva. [Online][siteerattu 13.12.2012]. Opinnäytetyö. Tampereen ammattikorkeakoulu: Tietotekniikan koulutusohjelma. Saatavana World Wide Webistä: <URL: https://publications.theseus.fi/bitstream/handle/10024/10334/TMP.objres.226.pdf?sequence=2>.

Vesanen Ari (2003), Langattomien verkkojen tietoturva. [Online][siteerattu 27.11.2012]. Oulun yliopisto: Tietojenkäsittelytieteiden laitos. Saatavana World Wide Webistä: <http://www.tol.oulu.fi/users/ari.vesanen/Langaton_TT/luennot/kalvot/WLAN.pdf>.