TEKNILLINEN KORKEAKOULU
SÄHKÖ- JA TIETOLIIKENNETEKNIIKAN OSASTO

Mikko Merger

Liikkuvuudenhallinta Mobile IP versio 6 -protokollalla

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi
diplomi-insinöörin tutkintoa varten Espoossa 7.12.2004

Työn valvoja	Professori Jorma Jormakka
Työn ohjaaja	TkL Markus Peuhkuri

TEKNILLINEN KORKEAKOULU **DIPLOMITYÖN TIIVISTELMÄ**

Tekijä:	Mikko Merger	
Työn nimi:	Liikkuvuudenhallinta Mobile IP versio 6 -protokollalla	
Päivämäärä:	7. joulukuuta 2004	**Sivumäärä**: 84
Osasto:	Sähkö- ja tietoliikennetekniikan osasto	
Professuuri:	Teletekniikka	**Koodi:** S-38
Työn valvoja:	Professori Jorma Jormakka	
Työn ohjaaja:	TkL Markus Peuhkuri	

Langattomien lähiverkkojen käyttö liityntätekniikkana Internetiin kasvaa nopeasti. Eräs suurimmista tekijöistä tämän kehityksen takana on se, että langaton tekniikka mahdollistaa käyttäjien liikkumisen verkon peittoalueella. Liikkuminen Internetissä aiheuttaa kuitenkin ongelmia kuten avoimien yhteyksien ylläpito ja tavoitettavuuden säilyttäminen. Tässä diplomityössä tutkitaan näitä liikkuvien päätelaitteiden käyttöön liittyviä ongelmia ja esitellään joitakin tunnettuja ratkaisumalleja sekä vertaillaan niiden soveltuvuutta eri tilanteisiin. Työssä keskitytään IETF:n ehdottamaan liikkuvuudenhallintamekanismiin Mobile IPv6, jonka toiminta käydään läpi yksityiskohtaisesti. Kirjallisuustutkimuksen jälkeen selvitetään WLAN ja MIPv6-tekniikoiden simulointimahdollisuuksia ns-2 verkkosimulaattorilla sekä suoritetaan joitakin simulaatioita.

Kirjallisuustutkimuksessa IEEE 802.11 -standardin liikkuvuusominaisuudet osoittautuu varsin rajoittuneiksi, sillä ne mahdollistavat liityntäpisteen vaihdon vain saman aliverkon sisällä. Lisäksi tavanomaiset IP-reititysmekanismit sekä kuljetuskerroksen protokollat tekevät yhteyksien ja tavoitettavuuden säilyttämisen aliverkkojen välillä liikuttaessa mahdottomaksi. Mobile IPv6 on IPv6:n laajennus, joka tarjoaa läpinäkyvän verkkokerroksella toimivan liikkuvuudenhallintaratkaisun. Se mahdollistaa laitteiden liikkumisen Internetissä ilman, että avoimet yhteydet tai tavoitettavuus menetettäisiin. Mobile IPv6:n suunnittelussa on kyetty hyödyntämään Mobile IPv4:stä saatuja kokemuksia sekä IPv6:n uusia ominaisuuksia. MIPv6 sisältää siten monia parannuksia MIPv4:ään verrattuna.

Ns-2 laajennettuna MobiWan-laajennuksella sekä joillakin lisämuutoksilla tarjoaa mahdollisuuden MIPv6-liikkuvuudenhallinnan tutkimiseen erilaisien simulaatioskenaarioiden avulla. Tässä työssä muodostettiin muutamia skenaarioita, joilla tutkittiin reitinoptimoinnilla saavutettavia etuja sekä Mobile IPv6:n rekisteröintien aiheuttamaa signalointiliikennettä. Simulaatiot osoittavat, että reitinoptimoinnilla saatava hyöty riippuu liikkuvan laitteen ja vertaislaitteen sijainnista suhteessa kotiagenttiin. Kaikissa tapauksissa sillä saavutetaan käänteistunnelointia suurempi siirtonopeus ja joissakin tapauksissa päästään jopa moninkertaiseen siirtonopeuteen käänteistunnelointiin verrattuna. Toisessa skenaariossa MIPv6-signalointiliikenteen määrä osoittautui varsin pieneksi eikä sen pitäisi aiheuttaa ongelmia IEEE 802.11 -verkoissa.

Avainsanat:	Mobile IPv6, liikkuvuudenhallinta, IEEE 802.11, WLAN, simulointi, ns-2

HELSINKI UNIVERSITY OF TECHNOLOGY **ABSTRACT OF THE MASTER'S THESIS**

Author:	Mikko Merger	
Name of the Thesis:	Mobility management with Mobile IP version 6	
Date:	December 7, 2004	**Number of pages:** 84
Department:	Department of electrical and communications engineering	
Professorship:	Telecommunication Technology	**Code:** S-38
Supervisor:	Professor Jorma Jormakka	
Instructor:	Lic.Sc.(Tech.) Markus Peuhkuri	

The use of wireless local area networks as access technology for Internet is growing rapidly. One of the driving forces behind this development is that WLANs enable user mobility within the coverage area of the network. Mobility in the Internet however presents some problems such as session continuity and reachability. In this thesis these problems associated with mobile nodes are studied. Some of the known approaches operating in different protocol layers are presented and their applicability is evaluated. The main focus is on IETF's mobility management proposal Mobile IPv6 which is studied thoroughly. After the literary research the possibilities to simulate WLANs and MIPv6 with ns-2 network simulator are examined and some simulations are performed.

In the literal study the mobility support of IEEE 802.11 is found to be limited to changes of access points only within the same subnet. Also the conventional IP routing mechanism and protocols used on transport layer make it impossible to maintain connections or reachability when moving between subnets. Mobile IPv6 is an extension to IPv6 which offers a transparent mobility management solution on the network layer. It allows nodes to move in the Internet without losing active transport layer sessions or reachability. The design of MIPv6 benefits from the experiences gathered from Mobile IPv4 and the new features provided by IPv6. Therefore it includes many enhancements compared to MIPv4.

Ns-2 combined with the MobiWan extension and some additional modifications gives the possibility to research MIPv6 mobility management through various simulation scenarios. In this thesis we present scenarios which were used to evaluate the advantages of route optimization compared to reverse tunnelling and the signalling traffic load created by Mobile IPv6. The simulations show that the advantage of route optimization depends on the locations of mobile and correspondent nodes in relation to the home agent. In all cases route optimization gives higher throughput than reverse tunnelling and in some cases even multiple times higher throughput can be reached with it. In the other scenario the signalling traffic generated by MIPv6 binding registrations is found to be fairly small and should not cause any problems in IEEE 802.11 networks.

Keywords:	Mobile IPv6, mobility management, IEEE 802.11, WLAN, simulation, ns-2

Alkulause

Tämä diplomityö on tehty Teknillisen Korkeakoulun Tietoverkkolaboratoriossa Puolustusvoimien Teknillisen Tutkimuslaitoksen rahoittamassa LATE-projektissa, jossa tutkitaan langattomien lähiverkkojen hyödyntämistä.

Haluan kiittää työn valvojana toiminutta professori Jorma Jormakkaa ripeästä palautteesta sekä rakentavista kommenteista. Hänen mutkaton ja kannustava asenteensa on edesauttanut työn tekemistä. Lisäksi haluan kiittää työn ohjaajaa, TkL Markus Peuhkuria, työn aikana saamistani tuesta ja neuvoista sekä luottamuksesta työtäni kohtaan.

Lopuksi haluan kiittää erityisesti perhettäni opintojen aikana saamastani tuesta.

Espoossa 7.12.2004

Mikko Merger

Sisällysluettelo

Lyhenteet

ACK	Acknowledgement
AH	Authentication Header
AID	Association Identifier
AP	Access Point
ARP	Address Resolution Protocol
BPSK	Binary Phase Shift Keying
BSA	Basic Service Area
BSS	Basic Service Set
BSSID	Basic Service Set Identification
CA	Collision Avoidance
CCA	Clear Channel Assessment
CCK	Complementary Code Keying
CCMP	Counter mode with Cipher block chaining Message authentication code Protocol
CD	Collision Detection
CN	Correspondent Node
CRC	Cyclic Redundancy Code
CSMA	Carrier Sense Multiple Access
CTS	Clear To Send
DA	Destination Address
DARPA	Defense Advanced Research Projects Agency
DBPSK	Differential Binary Phase Shift Keying
DCF	Distributed Coordination Function
DECT	Digital Enhanced Cordless Telecommunications
DHAAD	Dynamic Home Agent Address Discovery
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DIFS	DCF Interframe Space
DNS	Domain Name System
DQPSK	Differential Quadrature Phase Shift Keying
DS	Distribution System Service
DSSS	Direct Sequence Spread Spectrum
EIFS	Extended Interframe Space
EIRP	Equivalent Isotropically Radiated Power
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
FCS	Frame Check Sequence

FHSS	Frequency-Hopping Spread Spectrum
FMIPv6	Fast Handovers for Mobile IPv6
FTP	File Transfer Protocol
GFSK	Gaussian Frequency Shift Keying
GPRS	General Packet Radio System
GSM	Global System for Mobile Communications
HA	Home Agent
HAWAII	Handoff-Aware Wireless Access Internet Infrastructure
HEC	Header Error Check
HMIPv6	Hierarchical Mobile IPv6
IAPP	Inter-Access Point Protocol
IBSS	Independent Basic Service Set
ICMPv6	Internet Control Message Protocol for the Internet Protocol Version 6
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFS	Interframe Space
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	IP Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IR	Infra Red
ISM	Industrial, Scientific, and Medical
ISO	International Organization for Standardization
ISP	Internet Service Provider
LAN	Local Area Network
MAC	Medium Access Control
MAP	Mobility Anchor Point
mip4	Mobility for IPv4 Working Group
mip6	Mobility for IPv6 Working Group
mipshop	MIPv6 Signaling and Handoff Optimization Working Group
MIPv4	Mobile IPv4
MIPv6	Mobile IPv6
MMPDU	MAC Management Protocol Data Unit
MN	Mobile Node
MPDU	MAC Protocol Data Unit
MSDU	MAC Service Data Unit
NAV	Network Allocation Vector
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
OTcl	MIT Object Tool Command Language
PBCC	Packet Binary Convolutional Coding
PC	Point Coordinator
PCF	Point Coordination Function
PDA	Personal Digital Assistant
PHY	Physical Layer
PIFS	PCF Interframe Space
PLCP	Physical Layer Convergence Protocol
PLW	PSDU Length Word
PMD	Physical Medium Dependent

PPDU	PLCP Protocol Data Unit
PSDU	PLCP Service Data Unit
PSF	PSDU Signaling Field
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RA	Receiver Address
RFC	Request For Comments
RTS	Request To Send
SA	Source Address
SAP	Service Access Point
SFD	Start Frame Delimiter
SIFS	Short Interframe Space
SIP	Session Initiation Protocol
SS	Station Service
STA	Station
SWAP	Shared Wireless Access Protocol
TA	Transmitter Address
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
UNII	Unlicensed National Information Infrastructure
VoIP	Voice over IP
VoWLAN	Voice over WLAN
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network

1 Johdanto

Langattomat lähiverkot (WLAN) ja niiden kautta Internetiä käyttävät kannettavat tietokoneet ja kämmentietokoneet (PDA) sekä tulevaisuudessa myös langattomia lähiverkkoja hyödyntävät matkapuhelimet (ns. VoWLAN-puhelimet) lisääntyvät, mikä lisää myös vaatimuksia langattomille verkoille sekä yhä kasvavassa määrin niiden tarjoamille päätelaitteiden liikkuvuusominaisuuksille. Langattomien verkkojen määrän kasvua ajavat niiden tuomat edut perinteisiin langallisiin lähiverkkoihin (LAN) verrattuna. Näitä ovat esimerkiksi joustavuus niin käytössä kuin verkon suunnittelussa ja rakentamisessakin sekä edulliset kustannukset. Langattomien yhteyksien heikkouksia toisaalta ovat langallista verkkoa heikompi palvelun laatu, radiotaajuuksien käyttöä rajoittavat säädökset sekä tietoturva. Langattomat verkkotekniikat kehittyvät jatkuvasti ja myös edellä mainittujen haasteiden kanssa työskennellään, mikä näkyy mm. kasvavina tiedonsiirtonopeuksina.

Liikkuvuuden mahdollistaminen on eräs olennaisimmista langattomien verkkojen eduista perinteisiin lankaverkkoihin verrattuna. Lähiverkkotekniikoiden itsessään tarjoamat liikkuvuusominaisuudet ovat kuitenkin varsin rajoittuneet ja määrittelevät liikkuvuuden vain saman aliverkon liityntäpisteiden välillä, mikä tarkoittaa käytännössä verkkokerroksen IP-osoitteen vaihtumista ja sitä kautta ylemmän tason kuljetusprotokollia käyttävien yhteyksien katkeamista langattoman päätelaitteen vaihtaessa verkon liityntäpistettään kahden eri aliverkon välillä. Pelkkä WLAN ei ole siten riittävä ratkaisu käyttäjien liikkuessa laajemmissa verkoissa.

Internetissä nykyisin käytettävää verkkotason protokollaa Internet Protocol version 4:ää (IPv4) [1] suunniteltaessa ei osattu ottaa huomioon liikkuvia päätelaitteita eikä sekään siten tue liikkuvuutta. IP-verkossa pakettien reititys perustuu IP-osoitteen verkkotunnisteeseen, joka määrittelee kunkin osoitteen fyysisen aliverkon ja mistäpäin verkkoa kyseisen osoitteen omaava kone pitäisi löytyä. Tämän vuoksi paketit eivät enää löydä perille siirrettäessä kone osoitetta vaihtamatta alkuperäisestä aliverkosta toiseen

aliverkkoon, jolla on oma verkkotunnisteensa. Kone tarvitsee ns. topologisesti oikean osoitteen ja saman IP-osoitteen verkko-osan omaavat koneet pitäisi siis aina löytyä samasta aliverkosta. Käyttämällä reititykseen verkkotunnistetta, on saavutettu merkittävästi vähäisempi reititysliikenne sekä pienemmät reitittimien reititystaulut ja sitä kautta parempi skaalautuvuus.

Jos taas IP-osoite vaihdetaan aina verkon liityntäpistettä vaihdettaessa esimerkiksi DHCP:n (Dynamic Host Configuration Protocol) [2] avulla, katkeavat käynnissä olevat yhteydet. Lisäksi muut kyseisen koneen kanssa liikennöimään pyrkivät koneet eivät voi enää tavoittaa konetta, koska ne eivät tiedä sen uutta IP-osoitetta. Tämä toiminnallisuus riittää silti useimmille käyttäjille, jotka tarvitsevat vain yhteyden Internetiin sijainnista riippumatta ja vaihtavat sijaintiaan harvoin. Saumatonta ja läpinäkyvää liikkuvuutta tai tavoitettavuutta näin ei kuitenkaan saavuteta. Niinpä Internet Engineering Task Force (IETF) [3] kehitti Mobile IPv4:n (MIPv4) [4], joka on liikkuvuustuen IPv4-protokollaan lisäävä laajennus.

Tässä työssä keskitytään IP-protokollan uudempaan versioon Internet Protocol version 6:een (IPv6) [5], jota on jo jossain määrin otettu käyttöön ja johon tullaan tulevaisuudessa mitä todennäköisimmin vähitellen siirtymään kokonaan. Tämä johtuu pääasiassa IPv4:n osoiteavaruuden koosta, joka on Internetin ja sen käytön jatkuvasti kasvaessa osoittautunut liian pieneksi. Huomattavasti suuremman osoiteavaruuden lisäksi IPv6 tuo mukanaan myös monia muita etuja IPv4:ään verrattuna. Esimerkiksi kehittyneempi laitteiden automaattinen konfigurointi sekä integroitu tietoturva ovat eduksi myös liikkuvuudenhallinnassa. IPv6:n perustoimintaperiaatteet periytyvät IPv4:stä ja se kärsii samoista liikkuviin laitteisiin liittyvistä ongelmista kuin protokollan nykyinen versio, joten yksinomaan siirtyminen uuteen protokollaversioon ei ratkaise kyseistä ongelmaa. IPv6:tta kehitettäessä on liikkuvuusongelma kuitenkin huomioitu, mikä on mahdollistanut Mobile IPv4:ää kehittyneemmän liikkuvuudenhallintamekanismin integroinnin IPv6-protokollaan.

Mobile IPv6 (MIPv6) [6] on IETF:n määrittelemä skaalautuva ja käytetystä tiedonsiirtomediasta riippumaton verkkotason protokolla, joka lisää liikkuvuudenhallintaominaisuudet IPv6-verkkoihin. Toteuttamalla liikkuvuus verkkokerroksella saavutetaan läpinäkyvyys sovelluksille ja saumaton verkkovierailu IPv6-protokollaa käyttävien verkkojen välillä. Mobile IPv6:n avulla liikkuva päätelaite voi sijainnistaan riippumatta käyttää yhtä kiinteää osoitetta, jonka kautta se on tavoitettavissa. Tämä kotiosoite kuuluu koneen kotiverkon osoiteavaruuteen. Lisäksi

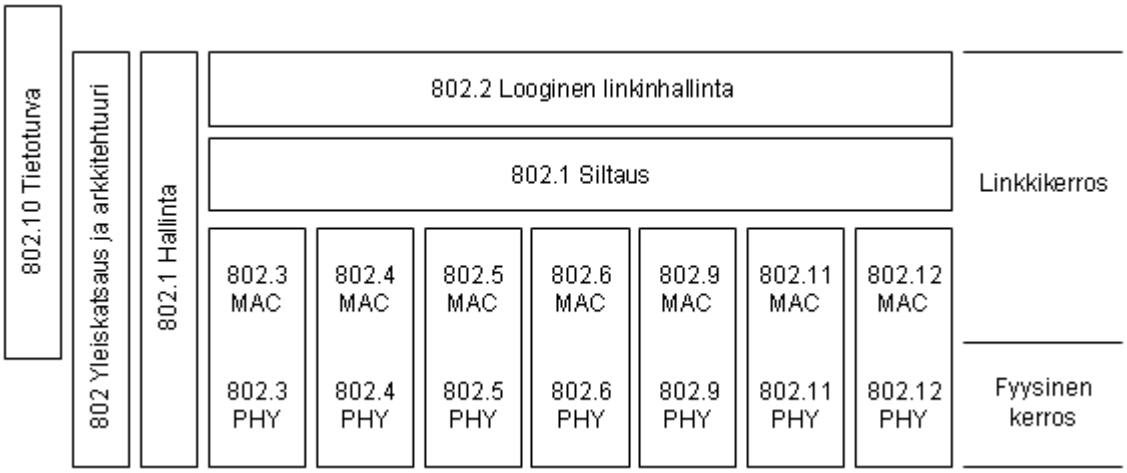
liikkuvan laitteen ollessa poissa kotiverkostaan tarvitaan toinen osoite, joka määrittelee laitteen sijainnin. Tätä osoitetta käytetään liikkuvalle laitteelle osoitettujen pakettien reitittämiseksi verkkoon, johon se on kulloinkin liittyneenä.

Mobile IPv6 tarjoaa mahdollisuuden useiden eri verkkotekniikoiden käyttöön linkkikerroksella sekä yhteydenvaihdot niiden välillä, jolloin voidaan aina hyödyntää tilanteesta ja olosuhteista riippuen sopivinta tarjolla olevaa liityntäverkkoa. Jos kannettava tietokone sisältää esimerkiksi sekä langattoman lähiverkkokortin että GPRS:ää tukevan GSM-kortin, voidaan yrityksen tiloissa käyttää WLAN-yhteyttä ja siirtyä käyttämään GPRS-verkkoa lähdettäessä yrityksen WLAN-verkon peittoalueen ulkopuolelle.

Tämän työn tavoitteena on perehtyä WLAN- ja Mobile IPv6 -tekniikoihin sekä niiden käyttöön mahdollisesti liittyviin ongelmiin. Lisäksi tutkitaan em. tekniikoiden simulointimahdollisuuksia ns-2 [7] verkkosimulaattorilla sekä suoritetaan joitakin simulaatioita. Työ sisältää ensin teoriaosuuden, jossa on suoritettu käytettyjen tekniikoiden kirjallisuusselvitys, jonka materiaalina on käytetty standardeja sekä alan kirjallisuutta ja julkaisuja. Johdannon jälkeen luvussa 4. on esitelty IEEE:n 802.11-WLAN-tekniikan perusteet ja sen tarjoamat liikkuvuusominaisuudet. Mobile IPv6 -protokollan toiminta käydään kokonaisuudessaan läpi luvussa 5. Luvussa 6. perehdytään edellä mainittujen tekniikoiden simulointiin ja esitellään käytetty simulointiympäristö sekä suoritetut simuloinnit ja niiden tulokset. Lopuksi on työn yhteenveto luvussa 7.

2 WLAN-standardi

Institute of Electrical and Electronics Engineersin (IEEE) [8] 802.11-standardi [9] on noussut selvästi suosituimmaksi langattomaksi lähiverkkotekniikaksi. Se on osa IEEE:n paikallisverkkotekniikoita käsittelevää 802-standardiperhettä (kts. kuva 1), johon kuuluu myös Ethernetinä paremmin tunnettu käytetyin langallinen lähiverkkotekniikka IEEE 802.3 [10]. Kuten kuvasta näkyy, keskittyvät kaikki 802-standardit ISOn OSI-mallin [11] kahdelle alimmalle kerrokselle: fyysinen kerros ja linkkikerros. 802.11-standardi on ominaisuuksiltaan ja toiminnaltaan verrattavissa Ethernetiin ja sitä kutsutaankin langattomaksi Ethernetiksi. Standardiperheen eri verkkotekniikat on suunniteltu yhdenmukaisiksi toiminnaltaan, mikä mahdollistaa esimerkiksi Ethernet-verkkojen ja langattomien lähiverkkojen yksinkertaisen yhteen liittämisen siltojen avulla. IEEE 802.11 -standardia kehitetään jatkuvasti, mikä näkyy mm. standardin uusien kehitysversioiden jatkuvasti paranevissa siirtonopeuksissa. Parhaimmillaan voidaan saavuttaa jopa 54 Mbps teoreettinen siirtonopeus. Tekniikan kasvavan suosion johdosta myös sen kustannukset ovat kehittyneet suosiolliseen suuntaan ja IEEE 802.11 -standardin mukaiset verkot ovat siten tulleet myös tavallisen kuluttajan saataville.

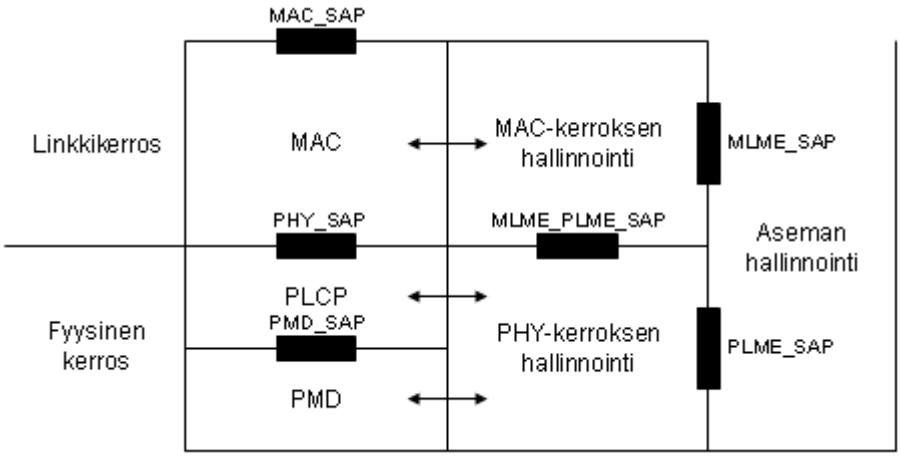


Kuva 1. IEEE:n 802-standardiperhe [8]

Muita langattomia lähiverkkotekniikoita ovat mm. HiperLAN2 [12], HomeRF [13] ja Bluetooth [14]. ETSIn [15] standardoima HiperLAN2 toimii 5 GHz:n taajuusalueella ja tarjoaa parhaimmillaan 54 Mbps teoreettisen siirtonopeuden. Sen etuja ovat palvelunlaatu-ominaisuudet (Quality of Service, QoS), integroitu vahva tietoturva sekä yhteensopivuuden useiden eri verkkotekniikoiden kanssa mahdollistavat konvergenssikerrokset. Hyvistä teknisistä ominaisuuksista huolimatta kaupallisia HiperLAN2-tuotteita ei vielä ole markkinoilla. HomeRF perustuu SWAP-protokollaan ja sen viimeisin 2.0-versio toimii 2.4 GHz:n alueella 10 Mbps teoreettisella siirtonopeudella. Protokollan erikoisuus on sen puhekanavat, jotka pohjautuvat langattomissa puhelimissa käytettyyn DECT-tekniikkaan. Muita HomeRF:n etuja ovat vahva salaus ja QoS-tuki. Heikon markkinatilanteen takia tekniikan kehitystyö kuitenkin lopetettiin vuonna 2002. Myös Bluetooth toimii 2.4 GHz:n taajuuskaistalla. Sen kantama on vain 10 metriä ja siirtokapasiteetti alle 1 Mbps. Bluetooth onkin tarkoitettu lähinnä erilaisten pienten kannettavien laitteiden, kuten matkapuhelimet ja PDA:t, väliseen langattomaan viestintään johtojen ja infrapuna-yhteyksien sijasta. Sen suunnittelun päätavoitteita ovat olleet mm. edullisuus, helppokäyttöisyys ja pieni virrankulutus.

IEEE 802.11 -standardi määrittelee Medium Access Control -kerroksen (MAC) ja fyysisen kerroksen (PHY). Järjestelmän tarkempi rakenne ilmenee kuvasta 2. MAC-kerroksen tehtäviä ovat siirtotielle pääsyn hallinta, käyttäjädatan fragmentointi ja salaus. Fyysinen kerros on jaettu kahteen alikerrokseen: Physical Layer Convergence Protocol (PLCP) ja Physical Medium Dependent sublayer (PMD). PLCP tarjoaa kantoaallon kuuntelusignaalin Clear Channel Assessment (CCA), jota käytetään kanavan tilan

ilmaisemiseen. PMD-alikerros taas hoitaa modulaation sekä koodauksen ja dekoodauksen. Palvelupisteet (Service Access Point, SAP) määrittelevät kerrosten väliset rajapinnat. Lisäksi standardissa on määritelty MAC- ja PHY-kerroksen hallinnointikokonaisuus sekä niiden toimintaa koordinoiva aseman hallinnointi.



Kuva 2. IEEE 802.11 -standardin protokolla-arkkitehtuuri [8]

Seuraavissa kappaleissa käydään läpi 802.11-standardin perusversion eri verkkoarkkitehtuurit, protokollakerrokset, palvelut sekä liikkuvuusominaisuudet. Lopuksi on esitelty lyhyesti standardin uudemmat kehitysversiot kuten IEEE 802.11b sekä niiden tuomat lisäominaisuudet.

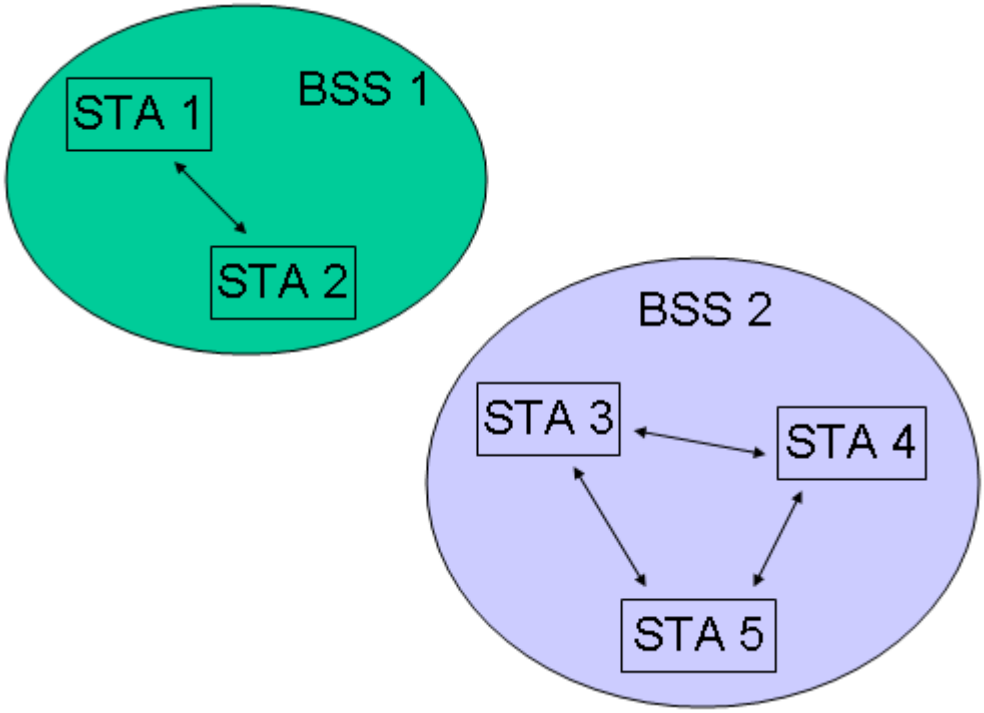
2.1 Verkkoarkkitehtuuri

IEEE 802.11 -standardin verkkoarkkitehtuuri koostuu useista eri komponenteista, jotka muodostavat WLAN-verkon. Peruspalveluryhmä (Basic Service set, BSS) on verkon peruselementti, joka sisältää asemia (Station, STA) sekä mahdollisesti liityntäpisteen (Access Point, AP) verkon topologiasta riippuen. Tyypillisimmillään asemat ovat langattomalla verkkokortilla varustettuja kannettavia tietokoneita. Liityntäpisteitä taas käytetään pääasiassa langattoman ja langallisen verkon yhdistämiseen.

802.11-standardi määrittelee kaksi erilaista perusverkkotopologiaa: itsenäinen peruspalveluryhmä (Independent BSS, IBSS) ja infrastruktuuri peruspalveluryhmä. Näiden lisäksi on laajennettu palveluryhmä (Extended Service Set, ESS), joka yhdistää useita infrastruktuuri peruspalveluryhmiä yhdeksi verkoksi.

IBSS on 802.11-standardin yksinkertaisin verkkoarkkitehtuuri, joka koostuu kahdesta tai useammasta asemasta, jotka viestivät keskenään suoraan toistensa kanssa.

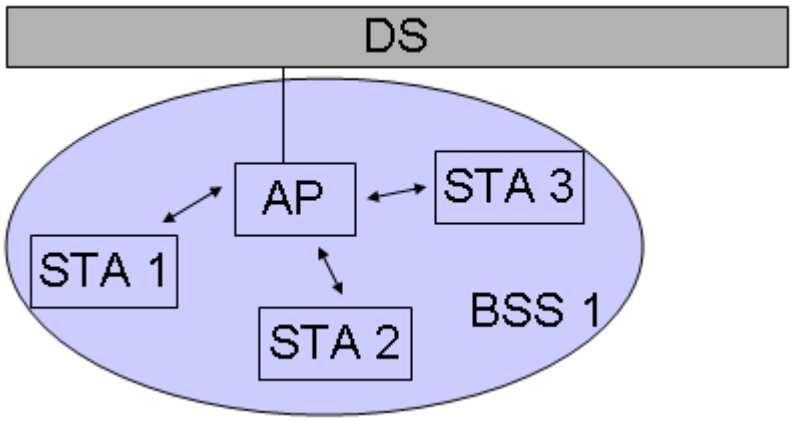
Tämä on luonnollisesti mahdollista vain kun asemat ovat toistensa radiosignaalin kantaman sisällä. Kuvassa 3 on esitetty kaksi erillistä itsenäistä peruspalveluryhmää, joista toisessa on kaksi asemaa ja toisessa kolme. Kummankin IBSS:n asemat pystyvät keskustelemaan keskenään kaikkien oman ryhmän asemien kanssa, mutta ei IBSS:tä toiseen. Jos jokin asema liikkuu ryhmän peittoaluetta kuvaavan soikion ulkopuolelle, ei se enää voi viestiä ryhmän asemien kanssa. Tällaista topologiaa edustava verkko rakennetaan useimmiten ilman erillistä suunnittelua tai valmistelua rajoitetuksi ajaksi ja sitä kutsutaan myös ad hoc -arkkitehtuuriksi.



Kuva 3. Kaksi itsenäistä peruspalveluryhmää

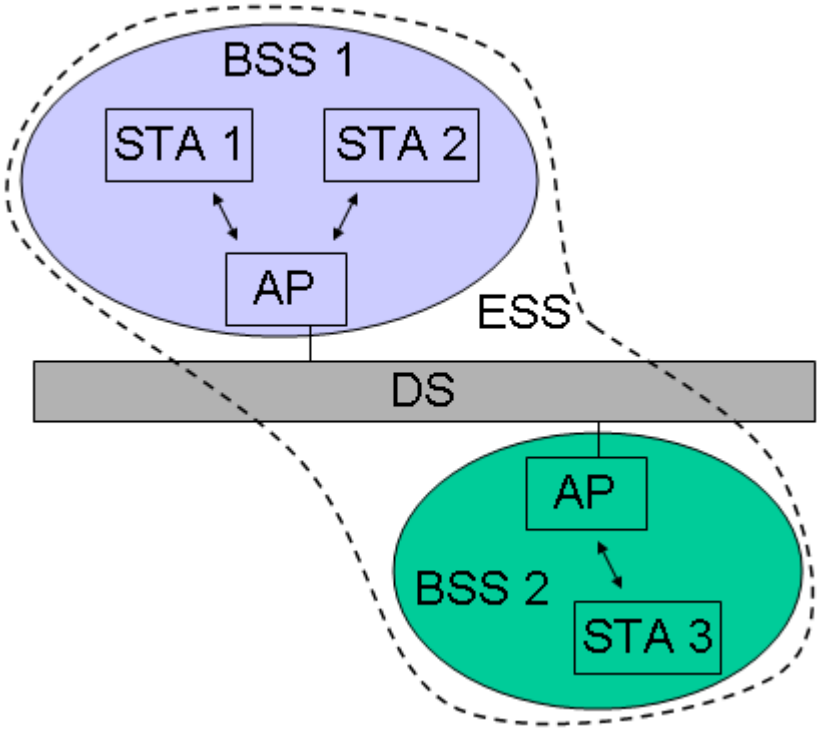
Infrastruktuuri peruspalveluryhmä muodostuu yhdestä liityntäpisteestä ja siihen liittyneistä asemista. Kuvan 4 peruspalveluryhmässä on AP, johon on liittynyt kolme asemaa. Kaikki liikenne kulkee tässä verkkoarkkitehtuurissa AP:n kautta eivätkä asemat voi viestiä suoraan toistensa kanssa vaan AP kontrolloi ryhmän viestiliikennettä. Tällöin riittää, että asemat ovat radioyhteydessä liityntäpisteeseen ja ryhmän peittoalueen määrittelee siten AP:n peittoalue. Liityntäpiste voi lisäksi olla liitetty jakelujärjestelmään (Distribution System, DS), jota käytetään erillisten verkkojen yhdistämiseen. 802.11-standardi ei määrittele jakelujärjestelmän arkkitehtuuria, mutta siltä vaaditut palvelut on määritelty. Useimmiten se on kuitenkin toteutettu Ethernet-tekniikalla. AP toimii siltana eri verkkotekniikoiden välillä ja näin voidaan yhdistää langaton lähiverkko esimerkiksi Ethernetiin. AP hoitaa pakettien välityksen verkkojen

välillä, jolloin peruspalveluryhmän asemat voivat liikennöidä muiden jakelujärjestelmään liittyneiden koneiden kanssa ja päinvastoin.



Kuva 4. Infrastruktuuri peruspalveluryhmä

Jakelujärjestelmää voidaan käyttää myös infrastruktuuri peruspalveluryhmien yhdistämiseen yhdeksi loogiseksi verkoksi, jolloin langattoman verkon peittoaluetta saadaan laajennettua yhden AP:n peittoaluetta suuremmaksi. Tällaista verkkoarkkitehtuuria kutsutaan laajennetuksi palveluryhmäksi (ESS). Kuvassa 5 on esitetty ESS, joka koostuu kahdesta infrastruktuuri peruspalveluryhmästä. Peruspalveluryhmien peittoalueet voivat olla myös limittäin, jolloin muodostuu yhtenäinen peittoalue. ESS:n asemat voivat keskustella toistensa kanssa aivan kuin ne olisivat samassa peruspalveluryhmässä. Tämä vaatii kuitenkin sen, että runkoverkkona toimiva jakelujärjestelmä tarjoaa linkkikerroksen yhteyden liityntäpisteiden välille. Liityntäpisteet tukevat roamingia eli liityntäpisteen vaihtoa, mikä mahdollistaa asemien liikkumisen ESS:n peittoalueen sisällä BSS:stä toiseen. Jakelujärjestelmälle määritellyt palvelut vastaavat asemien sijainnin seuraamisesta ja kehysten välittämisestä oikealle AP:lle. IEEE 802.11 -standardin liikkuvuusominaisuuksista enemmän tämän luvun loppupuolella liikkuvuutta käsittelevässä kappaleessa.



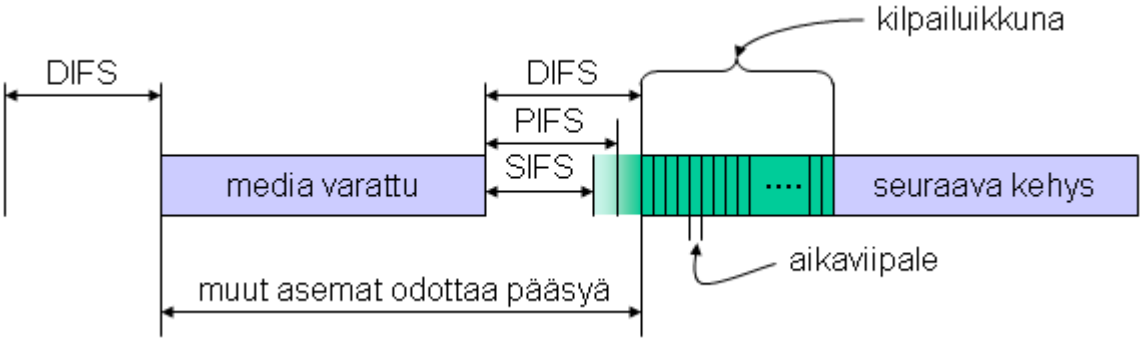
Kuva 5. Laajennettu palveluryhmä

2.2 MAC-kerros

IEEE 802.11 -standardi määrittelee sekä pakollisen asynkronisen datapalvelun että valinnaisen aikarajoitetun kilpailuttoman palvelun. Asynkroninen palvelu toimii ns. best effort -periaatteella eikä esimerkiksi siirtoviiveestä ole siten mitään takuita. Aikarajoitettu palvelu on käytettävissä vain infrastruktuuritopologian mukaisissa verkoissa, joissa liityntäpiste kontrolloi liikennettä. Nämä palvelut tarjoaa Medium Access Control -kerros, joka nimensä mukaisesti hallitsee käyttäjädatan lähettämistä siirtomedialle. Siirtomedialle pääsyä kontrolloivat MAC-kerroksen koordinointifunktiot: hajautettu koordinointifunktio (Distributed Coordination Function, DCF) ja sen päälle rakennettu pistekoordinointifunktio (Point Coordination Function, PCF). DCF:n kanssa voidaan lisäksi valinnaisesti käyttää menetelmää, jolla vältetään piilossa olevan päätelaitteen ongelma. DCF tarjoaa vain asynkronista palvelua, kun taas PCF tarjoaa molempia standardin määrittelemiä palveluita.

802.11-standardi määrittelee neljä eripituista kehysten välistä taukoa (Interframe Space, IFS), joilla saadaan aikaan eri prioriteettitasoja langattomalle medialle pääsyyn. Korkean prioriteetin liikenteen ei tarvitse odottaa yhtä kauan kanavan vapautumisen jälkeen, jolloin se pääsee siirtotielle ennen matalan prioriteetin liikennettä. Tauot ovat järjestyksessä lyhyimmästä pisimpään: short interframe space (SIFS), PCF interframe

space (PIFS), DCF interframe space (DIFS) ja extended interframe space (EIFS). SIFS on lyhin kehysten välinen tauko ja sitä käyttävät suurimman prioriteetin lähetykset kuten datapakettien kuittausviestit. Aikarajoitetun palvelun prioriteetti on suurempi kuin asynkronisen, joten siinä käytetään seuraavaksi lyhintä PIFSiä. Matalimman prioriteetin tarjoavaa DIFS-taukoa taas käytetään asynkronisen liikenteen kehysten välissä. EIFSiä käytetään vain, kun kehyksen siirrossa tapahtuu virhe. IFS-parametrien arvot määräytyvät käytetyn fyysisen kerroksen ominaisuuksien mukaan. Kuvassa 6 on esitetty taukojen väliset suhteet. IFS:n jälkeinen kilpailuikkuna on jaettu aikaviipaleisiin, jonka pituus määräytyy myös fyysisen kerroksen mukaan.



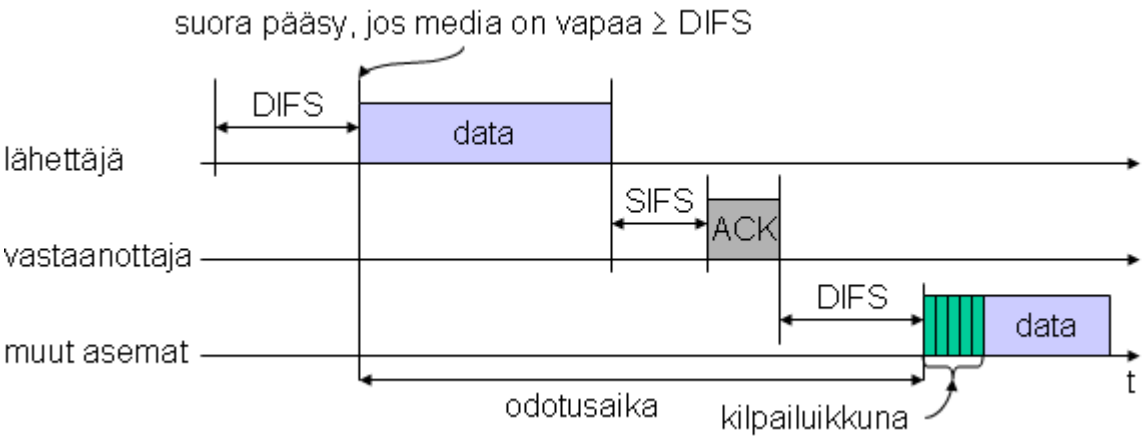
Kuva 6. Siirtotielle pääsy ja kehysten väliset tauot [16]

2.2.1 DCF

DCF on 802.11-standardin peruspääsymenetelmä ja pakollinen kaikissa standardin mukaisissa laitteissa. Kuten Ethernet, käyttää DCF siirtotielle pääsyn hallintaan carrier sense multiple access -menetelmää (CSMA). Siirtomediana käytetty radiotie tekee kuitenkin lähetysten törmäysten havaitsemisen (collision detection, CD) vaikeaksi eikä Ethernetin CSMA/CD-protokollaa voida siten käyttää 802.11:ssa. Sitä vastoin otetaan avuksi törmäysten välttäminen (collision avoidance, CA), jolloin törmäyksiä ei pitäisi tulla ja siirtomedian rajallinen tiedonsiirtokapasiteetti saadaan paremmin hyötykäyttöön. Törmäykset pyritään välttämään satunnaisen peräytymisajan avulla. Lisäksi kaikissa yksittäislähetyksissä käytetään positiivisia kuittauksia (Acknowledgement, ACK) lähetyksen onnistumisen varmistamiseen.

Protokollan toiminta on esitetty kuvassa 7. Jos media on vapaa vähintään ajan DIFS, pääsee asema siirtotielle välittömästi. Kun vastaanottaja on saanut kehyksen ja todennut sen virheettömäksi, lähettää se ajan SIFS jälkeen ACK-viestin. Jos siirtotie on varattu, kun asema pyrkii lähettämään, pitää sen odottaa kunnes media on jälleen vapaa ajan DIFS. Tämän jälkeen seuraa kilpailuvaihe. Jokainen asema valitsee satunnaisen

peräytymisajan, joka on aikaviipaleen (kts. kuva 6) monikerta ja määrää aseman odotusajan DIFSin jälkeen. Kilpailuvaiheessa voi olla useita medialle pyrkiviä asemia, joista lyhimmän peräytymisajan saanut pääsee ensimmäisenä lähettämään. Havaitessaan lähetyksen muut asemat peräytyvät ja lopettavat peräytymisajan laskemisen. Seuraavan kilpailuvaiheen aikana nämä asemat eivät valitse uutta satunnaista peräytymisaikaa vaan käyttävät edellisestä kerrasta jäljellä olevaa peräytymisaikaa. Näin jo jonottaneilla asemilla on suurempi todennäköisyys päästä lähettämään.



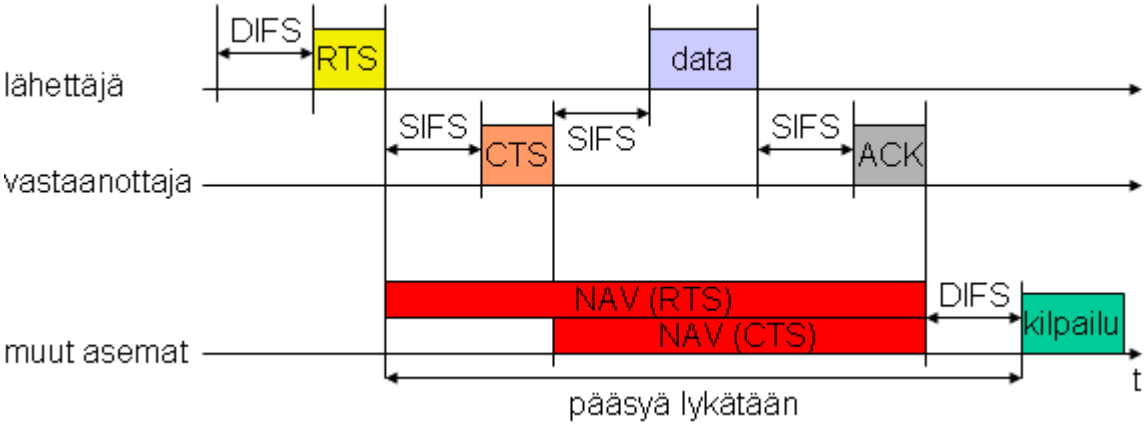
Kuva 7. Yksittäislähetys DCF-protokollalla [16]

DCF hyödyntää myös eksponentiaalista peräytymistä, mikä tarkoittaa että aina kun kehyksen lähetys epäonnistuu, tuplataan kilpailuikkunan koko kunnes saavutetaan ikkunan koon maksimiarvo. Näin kilpailuvaiheeseen saadaan lisää vaihtoehtoisia peräytymisaikoja ja todennäköisyys, että kaksi asemaa saa saman satunnaisen peräytymisajan pienenee. Tällä tavoin pyritään vähentämään törmäyksiä vaikka lähettävien asemien lukumäärä kasvaisi. Kun lähetys jälleen onnistuu tai määrätty määrä uudelleenlähetysyrityksiä on tehty, palautetaan kilpailuikkunan koko alkuarvoonsa. Kilpailuikkunan koon ala- ja ylärajat määräytyvät käytetyn fyysisen kerroksen mukaan.

2.2.2 DCF ja RTS/CTS

Kuten edellä todettiin, voidaan DCF:n kanssa käyttää menetelmää, jolla vältetään piilossa olevan päätelaitteen ongelma. Tämä on toteutettu kahdella kontrolliviestillä: request to send (RTS) ja clear to send (CTS). Mekanismin käyttäminen on valinnaista, mutta se täytyy olla toteutettu jokaisessa standardin mukaisessa laitteessa. Kuvassa 8 on esitetty mekanismin toiminta. Kun media on ollut vapaa vähintään ajan DIFS, pyytää asema lupaa datan lähettämiseen RTS-paketilla.

RTS-viesti sisältää tiedon tulevan data-kehyksen vastaanottajasta sekä koko lähetyksen keston kuittausviesteineen. Kaikki RTS-paketin vastaanottaneet asemat asettavat network allocation vector -ajastimen (NAV) RTS-paketin kesto-kentän mukaisesti. NAVia käytetään virtuaalisena kantoaallon kuuntelusignaalina ja se määrittelee ajan, jonka jälkeen asema voi jälleen yrittää pääsyä siirtotielle. Vastaanotettuaan RTS-paketin datan vastaanottaja odottaa ajan SIFS, jonka jälkeen se lähettää CTS-paketin. Myös CTS-paketti sisältää kesto-kentän ja paketin vastaanottajat asettavat jälleen NAVin sen mukaisesti. CTS:n vastaanotettuaan datan lähettäjä odottaa ajan SIFS, minkä jälkeen datakehyksen lähetys ja kuittaus tapahtuu samoin kuin DCF:llä. CTS-paketin vastaanottajien joukossa saattaa olla joitakin eri asemia kuin RTS-paketilla, koska ne voivat olla RTS:n lähettäjän kantaman ulkopuolella. Menettelemällä näin vältytään siltä, että kaksi toistensa kantaman ulkopuolella olevaa asemaa lähettäisivät yhtä aikaa kolmannelle niiden välissä olevalle asemalle, jolloin tapahtuisi törmäys.



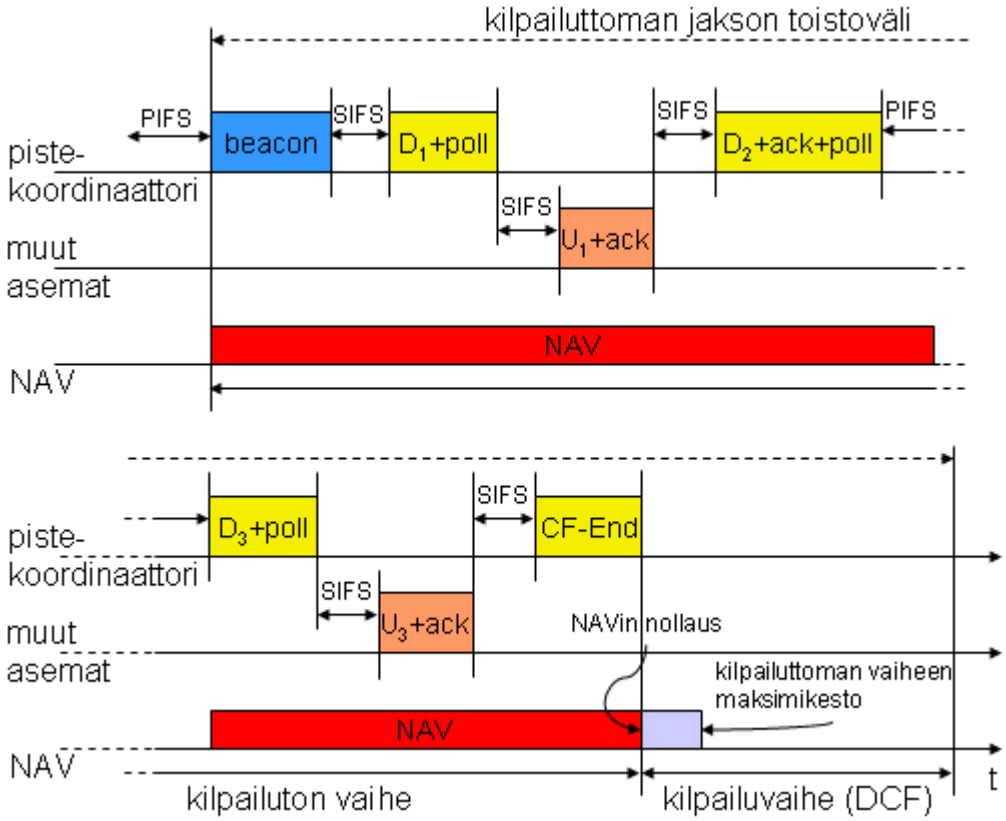
Kuva 8. DCF ja RST/CTS-mekanismi [16]

2.2.3 PCF

PCF:n avulla voidaan siis tarjota sekä asynkronista että kilpailutonta aikarajoitettua palvelua. Se on valinnainen pääsymenetelmä eikä sitä ole toteutettu kovinkaan monissa IEEE 802.11 -laitteissa. PCF vaatii toimiakseen pistekoordinaattorin (Point Coordinator, PC), joka toimii BSS:n liityntäpisteessä. PCF:ää voidaan käyttää siten vain infrastruktuuritopologian mukaisissa verkoissa. PC kontrolloi BSS:n liikennöintiä ja antaa kullekin ryhmän asemalle vuorollaan lähetysluvan kiertokyselyperiaatteella. Koska PC määrää kulloinkin lähettämään pääsevän aseman, ei kilpailutilannetta synny. Kilpailuttoman vaiheen jälkeen seuraa kilpailuvaihe, joka käyttäytyy DCF-mekanismin mukaisesti. Em. vaiheiden kestojen suhde voidaan määritellä parametrilla. PC ottaa siirtomedian hallintaansa kilpailuttoman vaiheen ajaksi

käyttämällä NAVia, joten myös vain DCF:n sisältävät asemat pystyvät toimimaan pistekoordinaattorin kanssa.

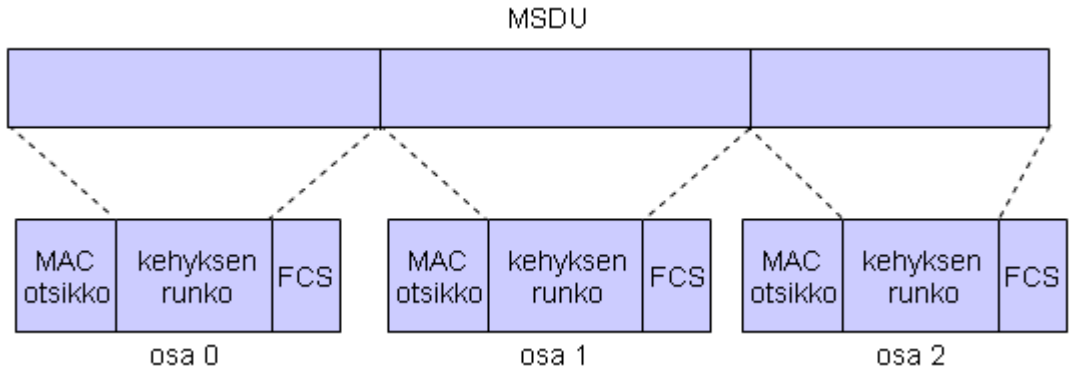
Esimerkki PCF:n toiminnasta on esitetty kuvassa 9. Kilpailuton ja kilpailullinen vaihe muodostavat jakson, joka toistuu tietyin aikavälein ja eri vaiheet seuraavat toisiaan vuoronperään. Kilpailuton vaihe alkaa median oltua vapaana kilpailuvaiheen jälkeen ajan PIFS pistekoordinaattorin lähettämällä majakka-viestillä (beacon), joka varaa siirtomedian NAV-laskurin avulla kilpailuttomaan käyttöön. Seuraavaksi PC lähettää datakehyksen (D_1) ensimmäiselle asemalle ja kysyy (poll) siltä datalähetystä. Asema vastaa omalla datakehyksellä (U_1) ja kuittauksella (ack). Ajan SIFS jälkeen PC kuittaa ensimmäisen aseman datan ja lähettää dataa (D_2) sekä kyselyn toiselle asemalle. Toisella asemalla ei ole kuitenkaan mitään lähetettävää ja ajan PIFS jälkeen PC lähettää dataa (D_3) ja kyselyn kolmannelle asemalle. Kolmas asema vastaa kuten ensimmäinen datakehyksellä (U_3) ja kuittauksella. CF-End päättää kilpailuttoman jakson ja DCF:ää käyttävä kilpailuvaihe alkaa. Kilpailuton vaihe saattaa olla lyhyempi kuin sille alussa NAVin avulla varattu maksimikesto, minkä vuoksi CF-End myös nollaa samalla asemien NAV-laskurit.



Kuva 9. PCF:n jakso sisältää kilpailuttoman ja kilpailullisen vaiheen [8]

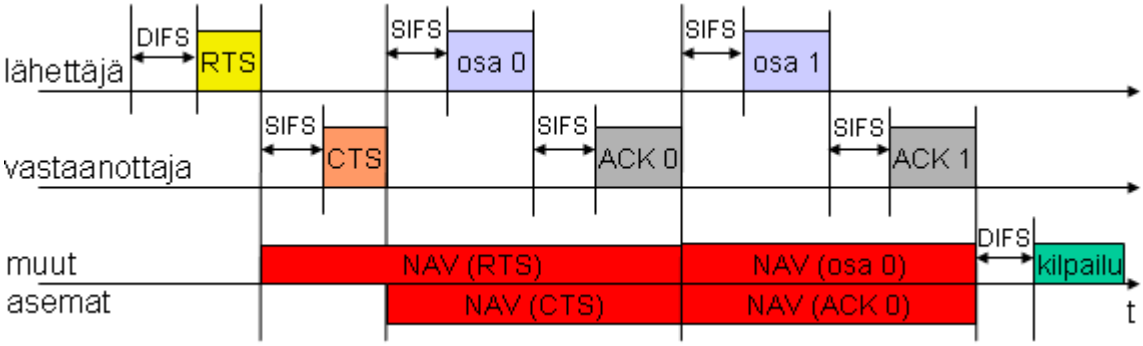
2.2.4 Fragmentointi

Ennen lähetystä MAC-kerros pilkkoo ylemmältä kerrokselta tulevan datan (MSDU tai MMPDU) pienempiin MAC-tason kehyksiin (MPDU). Lyhyemmillä kehyksillä saavutetaan suurempi onnistumistodennäköisyys lähetyksille ja sitä kautta parempi toimintavarmuus myös vaihtelevissa siirtotien olosuhteissa. Jos bittivirhesuhde pysyy samana, parantavat pienemmät kehykset kehysvirhesuhdetta ja lisäksi virheellisissä kehyksissä hukataan vähemmän dataa. Kuvassa 10 on esitetty MSDU:n pilkkominen kolmeen MAC-kehykseen. Fragmentin maksimikoko voidaan määritellä parametrin avulla.



Kuva 10. Fragmentointi

Pilkotun kehyksen osat voidaan lähettää kilpailuvaiheen aikana peräkkäin yhdessä purskeessa (kts. kuva 11) varaamalla siirtomedia NAVin avulla. Tässä tapauksessa data- ja kuittauskehyksiä käytetään varaamaan media aina seuraavan kehyksen kuittaukseen asti kunnes kaikki osat on lähetetty. Koska jokainen osa kuitataan erikseen, ei virheen tapahtuessa kuitenkaan tarvitse lähettää koko MSDU:ta tai MMPDU:ta uudelleen vaan vain virheellinen fragmentti. PCF:n kilpailuttoman vaiheen aikana osia voidaan lähettää pistekoordinaattorin määrittelemien rajojen puitteissa.

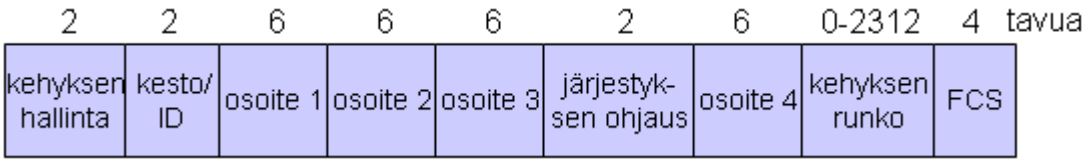


Kuva 11. Kahteen osaan pilkotun MSDU:n lähetys yhdessä purskeessa [8]

2.2.5 MAC-kehys

Jokainen MAC-kehys koostuu kolmesta perusosasta: otsikko, runko ja tarkistussumma (Frame Check Sequence, FCS). Kehyksen yleismuoto on esitetty kuvassa 12 ja se sisältää seuraavat kentät:

- Kehyksen hallinta: sisältää useita kehyksen hallintaan liittyviä kenttiä, jotka on esitelty tarkemmin alla.
- Kesto/ID: voi sisältää kehystyypistä riippuen joko assosiaatioidentiteetin (Association Identity, AID) tai lähetyksen keston, jota käytetään NAV-laskurin asettamiseen.
- Osoite 1-4: kehys sisältää neljä osoitekenttää, jotka määrittelevät BSSID:n (Basic Service Set Identification), lähteen (Source Address, SA), kohteen (Destination Address, DA), lähettävän aseman (Transmitter Address, TA) ja vastaanottavan aseman (Receiver Address, RA). Kenttien merkitys ilmenee hallintakentästä. 802.11-standardi käyttää MAC-osoitteina samoja 48-bittisiä IEEE 802 -osoitteita kuin muutkin 802-perheen lähiverkot.
- Järjestyksen ohjaus: Sisältää MSDU/MMPDU:n järjestysnumeron ja kyseisen kehyksen sirpaleen numeron. Tarvitaan kehysten järjestyksen säilyttämiseen sekä kaksoiskappaleiden poistamiseen.
- Kehyksen runko: kentän pituus vaihtelee välillä 0-2312 tavua ja sisältö riippuu kehyksen tyypistä sekä alityypistä. Esimerkiksi datakehyksen runko sisältää lähetettävän datan.
- FCS: sisältää 32-bittisen CRC-tarkistussumman, joka lasketaan kaikista kehyksen kentistä.



Kuva 12. Yleinen MAC-kehys

Edellä esitetyn yleiskehyksen lisäksi standardi määrittelee lukuisia pienempiä kontrolli- ja hallinnointi-kehystyyppejä, jotka eivät välttämättä sisällä kaikkia yleiskehyksen kenttiä.

MAC-kehyksen kehyksen hallinta kenttä (kuva 13) on jaettu edelleen alikenttiin seuraavasti:

- Protokollaversio: määrittelee kehyksen käyttämän protokollaversion, joka on tällä hetkellä 0.
- Tyyppi ja alityyppi: määrittelevät yhdessä kehyksen funktion. Kehyksiä on kolmea eri tyyppiä: kontrolli, hallinta ja data. Kullakin kehystyypillä on useita alityyppejä.
- DS:ään ja DS:stä: määrittelevät MAC-kehyksen eri osoitekenttien merkityksen. Jakelujärjestelmään osoitettujen datakehysten DS:ään kenttä on 1, muulloin 0. Vastaavasti jakelujärjestelmästä tulevien datakehysten DS:stä kenttä on 1 ja muiden 0. Eri vaihtoehdot ja niiden käyttötarkoitus on esitetty taulukossa 1.
- Lisää osia: ilmaisee onko kyseisestä MSDU:sta tai MMPDU:sta vielä tulossa lisää osia, jolloin tämä bitti on 1. Muulloin 0.
- Uudelleenlähetys: jos kehys joudutaan lähettämään uudelleen, asetetaan tämän kentän arvoksi 1. Muulloin 0.
- Tehonhallinta: määrittelee aseman tehonhallintatilan onnistuneen kehysten lähetysten jälkeen. Jos kentän arvo on 1, tulee asema siirtymään tehonsäästötilaan. Jos taas arvo on 0, pysyy asema aktiivitilassa. Kaikissa AP:n lähettämissä kehyksissä kenttä on 0.
- Lisää dataa: ilmaisee tehonsäästötilassa olevalle asemalle, että AP:lla on puskurissa lisää dataa lähetettävänä asemalle. Lisäksi PCF-mekanismia käytettäessä asema voi kertoa kentän avulla AP:lle, että sillä on lisää dataa lähetyspuskurissa.
- WEP: kertoo, onko kehyksen rungon salaamiseen käytetty 802.11-standardin määrittelemää Wired Equivalent Privacy -algoritmia.
- Järjestys: jos kentän arvo on 1, pitää kehykset ja sirpaleet käsitellä järjestyksessä.

Kuva 13. Kehyksen hallinta kenttä

Taulukko 1. Osoitekenttien merkitys eri käyttötapauksissa [16]

Käyttö	DS:ään	DS:stä	osoite 1	osoite 2	osoite 3	osoite 4
ad hoc verkon asemien välillä	0	0	DA	SA	BSSID	-
infrastruktuuri, jakelujärjestelmästä	0	1	DA	BSSID	SA	-
infrastruktuuri, jakelujärjestelmään	1	0	BSSID	SA	DA	-
infrastruktuuri, jakelujärjestelmässä	1	1	RA	TA	DA	SA

2.3 Fyysinen kerros

IEEE 802.11 -standardi tarjoaa kolme vaihtoehtoista fyysistä kerrosta: taajuushyppely hajaspektri (Frequency-Hopping Spread Spectrum, FHSS), suorasekvenssi hajaspektri (Direct Sequence Spread Spectrum, DSSS) ja infrapuna (Infrared, IR). Kukin näistä koostuu kahdesta osasta: langattomasta siirtomediasta riippuvainen PMD sekä MAC-kerroksen ja PMD:n välisestä sovituksesta vastaava PLCP.

2.3.1 Taajuushyppely hajaspektri

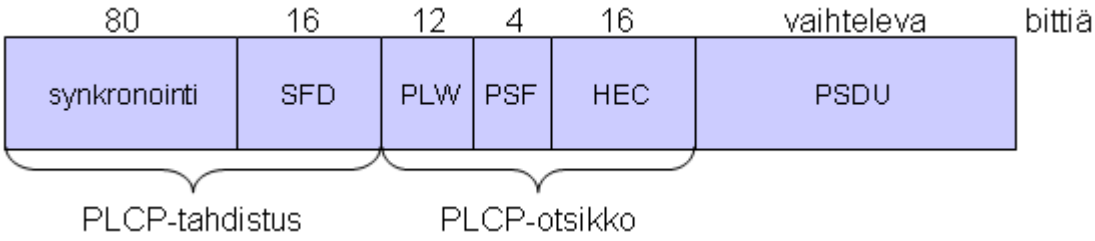
Taajuushyppely hajaspektri toimii 2.4 GHz:n ISM-taajuusalueella, joka on maailmanlaajuisesti vapaasti käytettävissä ilman lisensointia. FHSS hyödyntää taajuushyppelyä, jossa lähettäjä ja vastaanottaja ovat yhdellä taajuudella määrätyn ajan ja hyppäävät sitten jollekin toiselle taajuudelle. Hyppely mahdollistaa eri peruspalveluryhmien erottamisen toisistaan erilaisilla taajuushyppelysekvensseillä. Näin BSS:t voivat toimia samalla alueella toisiaan häiritsemättä. Standardi määrittelee Euroopan käyttöön 79 kanavaa, joiden kaistanleveys on 1 MHz. Kukin hyppelysekvenssi muodostaa pseudosatunnaisen hyppelykuvion, jossa peräkkäisten taajuuksien väli on vähintään 6 MHz ja joka käyttää samalla tasaisesti koko taajuusaluetta. Hyppelysekvenssit on jaettu kolmeen ryhmään, joista kukin sisältää 26 hyppelysarjaa. Ryhmät on suunniteltu siten, että ryhmän eri hyppelysekvenssien välillä olisi mahdollisimman vähän törmäyksiä. FHSS:n suurin sallittu lähetysteho Euroopassa on 100 mW EIRP.

FHSS tarjoaa kaksi palvelunopeutta: 1 ja 2 Mbps. Pakollinen yhden megabitin palvelu käyttää kaksitasoista 2GFSK-modulaatiota (Gaussian Frequency Shift Keying),

jossa yksi taajuus vastaa yhtä bittiä. Valinnainen 2 Mbps palvelu on toteutettu nelitasoisella 4GFSK-modulaatiolla, jossa kukin taajuus vastaa kahta bittiä.

PLCP lisää MAC-kerrokselta tulevaan MPDU:hun oman kehystyksensä, jota tarvitaan kehysten lähettämiseen radiotietä pitkin. Kuvassa 14 oleva PPDU (PLCP Protocol Data Unit) koostuu kolmesta osasta: PLCP-tahdistus ja -otsikko sekä PSDU (PLCP Service Data Unit). Eri palvelunopeuksien yhteensopivuuden takaamiseksi PLCP-tahdistus ja -otsikko lähetetään aina nopeudella 1 Mbps, kun taas hyötykuorman sisältävä PSDU voidaan lähettää joko nopeudella 1 Mbps tai 2 Mbps. PSDU:n sisältämä MAC-kehys sekoitetaan polynomilla $S(x)=x^7+x^4+1$, jolla pyritään satunnaistamaan dataa sekä välttämään tasavirtasignaalin muodostuminen. PLCP-tahdistus ja -otsikko sisältää seuraavat kentät:

- Synkronointi: sisältää 80-bittiä pitkän 0-1-jaksoa toistavan bittijonon, jonka avulla vastaanottaja havaitsee vastaanotettavan signaalin ja tahdistaa kellonsa.
- SFD (Start Frame Delimiter): 16-bittinen binäärikuvio 0000 1100 1011 1101, joka ilmaisee kehyksen alkamisen ja kehystahdin.
- PLW (PSDU Length Word): kentän sisältö tulee MAC-kerrokselta ja määrittelee PSDU:n koon okteteissa.
- PSF (PSDU Signaling Field): määrittelee PSDU:n lähetykseen käytetyn siirtonopeuden.
- HEC (Header Error Check): 16-bittinen CRC-tarkistussumma, jonka avulla tarkistetaan PLCP-otsikon virheettömyys.



Kuva 14. FHSS:n PLCP-kehys

2.3.2 Suorasekvenssi hajaspektri

Suorasekvenssitekniikassa signaalin hajautus laajemmalle taajuusalueelle suoritetaan koodin avulla. Jokainen lähetettävä databitti korvataan pitemmällä bittijonolla, joka saadaan XOR-operaatiolla lähetettävästä bitistä ja koodista. Sopivalla koodilla hajautettu signaali näyttää satunnaiselta kohinalta, mikä vaikeuttaa sen

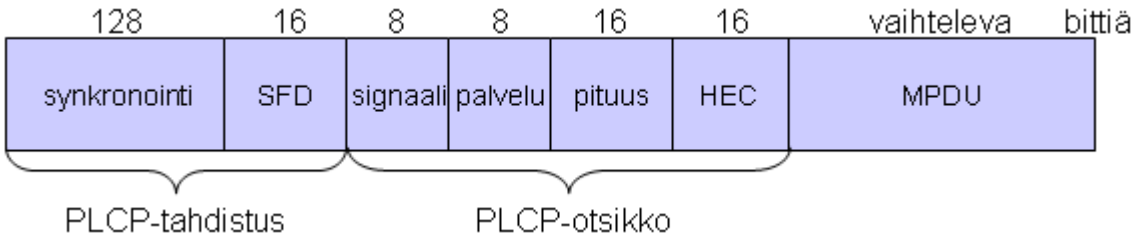
havaitsemista. IEEE 802.11 -standardissa hajautukseen käytetään 11 sirun (chip) Barker-koodia (+1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1), jonka etuja ovat hyvä häiriöidensietokyky sekä epäherkkyys monitie-etenemisen vaikutuksille. Koska lähetettävien bittien määrä kasvaa, kasvaa myös tarvittava lähetyskaista vastaavasti; esimerkiksi 1 MHz symbolinopeus vaatii 11 MHz:n kaistan.

Myös suorasekvenssi hajaspektri toimii 2.4 GHz:n taajuuskaistalla, joka on jaettu Euroopassa 13 kanavaan 5 MHz:n keskitaajuusvälein. Koska kanavien pääkeilat ovat leveydeltään 22 MHz, ei vierekkäisiä kanavia voida käyttää samalla alueella häiriöttä. Häiriöttömyys vaatii vähintään 22 MHz:n eron keskitaajuuksien välille, jolloin käyttöön jää vain kolme kanavaa (1, 7 ja 13). DSSS:n suurin sallittu lähetysteho on 100 mW EIRP.

DSSS tarjoaa FHSS:n tapaan sekä 1 Mbps että 2 Mbps palvelua, jotka on toteutettu eri modulointitekniikoilla. 1 Mbps palvelu käyttää DBPSK-modulointia (Differential Binary Phase Shift Keying) ja 2 Mbps palvelu DQPSK-modulointia (Differential Quadrature Phase Shift Keying).

DSSS:n käyttämä PLCP-kehysrakenne (kuva 15) poikkeaa hieman FHSS:n kehyksestä. PLCP-tahdistus ja -otsikko lähetetään edelleen aina nopeudella 1 Mbps, mutta datan sisältävä MPDU voidaan lähettää myös nopeudella 2 Mbps. DSSS:ssä sitä vastoin koko PLCP-kehys sekoitetaan polynomilla $G(z)=z^{-7}+z^{-4}+1$. Kehys sisältää seuraavat kentät:

- Synkronointi: sisältää 128 bittiä sekoitettuja ykkösiä. Vastaanottaja käyttää kenttää tahdistamiseen.
- SFD: sisältää 16-bittisen bittijonon 1111001110100000, joka merkitsee kehyksen alkua.
- Signaali: määrittelee MPDU:n lähetykseen käytetyn modulaation.
- Palvelu: kenttä on varattu mahdollista tulevaa käyttöä varten.
- Pituus: määrittelee mikrosekunneissa MPDU:n lähettämiseen kuluvan ajan.
- HEC: sisältää 16-bittisen CRC-tarkistussumman, jolla suojataan PCLP-otsikko.



Kuva 15. DSSS:n PLCP-kehys

2.3.3 Infrapuna

802.11-standardin infrapunalla toteutettu fyysinen kerros toimii lähes näkyvällä valolla, jonka aallonpituus on 850–950 nm. Samaa aallonpituutta käytetään mm. kaukosäätimissä eikä sen käyttöä ole säännelty muuten kuin turvallisuusmääräyksin. IR:n lähettämä signaali ei kuitenkaan ole suunnattua, mikä tarkoittaa että lähettäjän ja vastaanottajan ei tarvitse olla suunnattu toisiaan kohti eikä niiden välillä tarvitse olla suoraa näköyhteyttä. Infrapunan kantama on enimmillään 10 metriä, joten se soveltuu käytettäväksi lähinnä sisätiloissa. Koska infrapunasäteily ei läpäise seiniä, voidaan verkon peittoalue rajata helposti ja sijoittaa IR:ää käyttävät erilliset verkot vierekkäisiin huoneisiin ilman häiriöitä tai mahdollisuutta salakuunteluun. Edullisista infrapunalähettimistä ja -vastaanottimista huolimatta IR:ää käyttäviä 802.11-päätelaitteita ei ole markkinoilla, koska radiotietä käyttävät fyysisen kerroksen ratkaisut tarjoavat enemmän joustavuutta ja liikkuvuutta.

2.4 Palvelut

IEEE 802.11 -standardissa on määritelty yhdeksän palvelua, jotka on jaettu palveluntarjoajan mukaan kahteen ryhmään: asemapalvelut (Station Service, SS) ja jakelujärjestelmäpalvelut (Distribution System Service, DSS). Asemapalvelut ovat autentikointi, autentikoinnin purku, yksityisyys ja MSDU-toimitus. Nämä on toteutettu jokaisessa IEEE 802.11 -standardin mukaisessa asemassa mukaan lukien liityntäpisteet. Jakelujärjestelmäpalvelut ovat assosiointi, assosioinnin purku, jakelu, integrointi sekä uudelleenassosiointi. DSS-palveluita käytetään AP:n kautta ja ne voivat myös sijaita AP:ssa. Palveluista vain kolmea käytetään datan siirtämiseen, loput palvelut ovat datansiirtoa tukevia hallinnointipalveluita. Jokaista palvelua varten on olemassa yksi tai useampia MAC-kehystyyppejä, joita palvelut käyttävät.

MSDU-toimituspalvelu vastaa datan tiedonsiirrosta vastaanottajalleen.

Jakelupalvelua käytetään aina datakehyksen välityksessä infrastruktuuriverkon asemalta toiselle. Vastaanotettuaan kehyksen liityntäpiste käyttää jakelujärjestelmän jakelupalvelua kehyksen toimittamiseen oikealle vastaanottajalle. Palvelua kutsutaan riippumatta siitä kulkeeko kehys fyysisesti jakelujärjestelmän kautta AP:lta toiselle vai sijaitseeko lähettäjä ja vastaanottaja samassa BSS:ssä.

Integrointia käytetään, jos viestin lähettäjä tai vastaanottaja sijaitsee jakelujärjestelmään liitetyssä toisella tekniikalla toteutetussa lähiverkossa. Se vastaa verkkojen välisen liikennöinnin vaatimasta sovituksesta. Palvelun toteutus on riippuvainen jakelujärjestelmästä eikä sitä ole määritelty 802.11-standardissa.

Jotta jakelupalvelu osaa välittää viestit oikealle vastaanottajalle, pitää sen tietää mihin liityntäpisteeseen kukin asema on liittynyt. Tämän vuoksi aseman pitää suorittaa assosiointi assosiointipalvelun avulla ennen kuin se voi lähettää dataa AP:n kautta. Palvelu välittää aseman sijaintitiedon DS:lle. Asema voi olla assosioitunut vain yhteen liityntäpisteeseen kerrallaan, mutta yhteen liityntäpisteeseen voi olla assosioitunut useita asemia.

Uudelleenassosiointia käytetään, kun asema siirtyy BSS:stä toiseen saman ESS:n sisällä. Näin DS:n sijaintitiedot pysyvät ajan tasalla. Palvelua voidaan myös käyttää assosiointiattribuuttien muuttamiseen vaikka asema ei vaihtaisi AP:ta.

Assosioinnin purku mahdollistaa olemassa olevan assosioinnin purkamisen. Sitä käytetään, kun asema halutaan poistaa verkosta.

Autentikointipalvelua käytetään asemien identiteetin todentamiseen. Näin pyritään estämään luvattomien asemien pääsy verkkoon. Standardi tukee useita autentikointiprosesseja ja tarjoaa kaksi linkkitason autentikointimenetelmää. Verkko voi toimia joko avoimena järjestelmänä, jolloin mikä tahansa asema voi autentikoitua, tai sitten käyttää jaetun avaimen autentikointia. Autentikointi suoritetaan ennen assosiointia ja vain todennetut saavat luvan käyttää verkkoa.

Olemassa oleva autentikointi puretaan vastaavasti kuin assosiointi autentikoinnin purku -palvelulla. Samalla myös mahdollinen assosiointi purkautuu.

Yksityisyyspalvelulla voidaan salata viestien sisältö, jotta luvattomat eivät pääse lukemaan niiden sisältöä. Palvelua tarvitaan, koska langattoman verkon peittoalueella kuka tahansa voi salakuunnella verkon liikennettä vaikka ei olisikaan assosioitunut verkkoon. Standardi määrittelee WEP-algoritmin, jolla pyritään saavuttamaan lankaverkkoa vastaava yksityisyys. WEPissä on kuitenkin heikkouksia, jotka

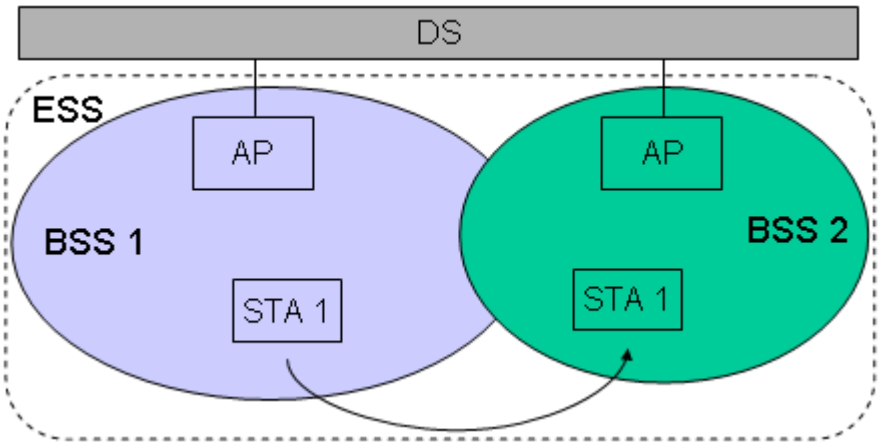
mahdollistavat salauksen purkamisen [17]. Salausta käytetään vain datakehyksiin sekä joihinkin autentikointikehyksiin. Oletusarvoisesti palvelu ei ole käytössä.

2.5 Liikkuvuus

Edellä esitetyt assosiointi- ja uudelleenassosiointipalvelut mahdollistavat asemien liikkumisen peruspalveluryhmien välillä. IEEE 802.11 -standardissa on määritelty kolme liikkuvuustyyppiä: ei siirtymää, BSS-siirtymä ja ESS-siirtymä.

Yksinkertaisin ei siirtymää -liikkuvuustyyppi käsittää tilanteet, joissa asema on joko paikallaan tai liikkuu yhden BSS:n peittoalueen (Basic Service Area, BSA) sisällä. Tämän tyypin tukemiseen riittää pelkkä assosiointipalvelu, sillä aseman tarvitsee assosioitua vain kerran yhteen liityntäpisteeseen.

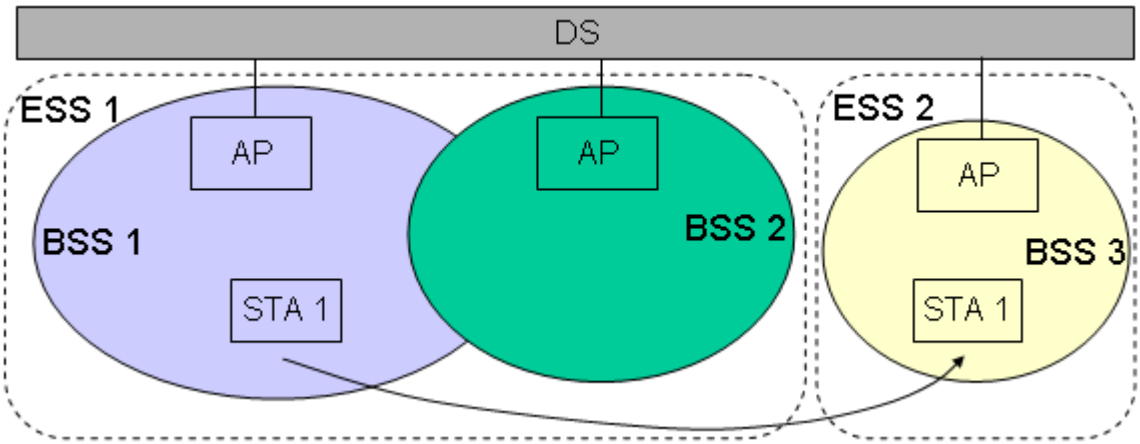
Kun asema liikkuu yhdestä BSS:stä toiseen saman ESS:n sisällä, on kyseessä BSS-siirtymä. Siirtyminen tapahtuu saumattomasti yhteyksien katkeamatta. Siirtymätyypin tukemiseen vaaditaan myös uudelleenassosiointipalvelun tuomia lisätoimintoja. Kuvassa 16 on esitetty BSS-siirtymä, jossa asema STA 1 liikkuu BSS 1:stä BSS 2:een. BSS 1 ja BSS 2 kuuluvat samaan laajennettuun palveluryhmään. Asema on alun perin assosioitunut BSS 1:en liityntäpisteeseen ja siirryttyään asema assosioituu BSS 2:en AP:n kanssa uudelleenassosiointipalvelun avulla. BSS-siirtymä vaatii liityntäpisteiden välistä tietojen vaihtoa, jotta myös vanha liityntäpiste saa tiedon aseman siirtymisestä. 802.11-standardi ei kuitenkaan määrittele liityntäpisteiden välistä viestintää, mikä saattaa aiheuttaa yhteensopivuusongelmia käytettäessä eri valmistajien liityntäpisteitä.



Kuva 16. BSS-siirtymä

Myös ESS-siirtymässä (kuva 17) asema liikkuu BSS:stä toiseen, mutta tässä tapauksessa peruspalveluryhmät kuuluvat eri ESS:iin. Tämän tyypin liikkumista ei

kuitenkaan tueta yhtä saumattomasti kuin BSS-siirtymää vaan standardi antaa vain mahdollisuuden siirtymään, mutta ei takaa ylemmän kerroksen yhteyksien säilymistä. Käytännössä tämä tarkoittaa, että kaikki käynnissä olevat tiedonsiirtoyhteydet katkeavat siirryttäessä ja ne joudutaan aloittamaan uudelleen assosioinnin jälkeen. Yhteyksien säilyttäminen vaatisi liikkuvuustukea 802.11:sta päällä toimivilta protokollilta.



Kuva 17. ESS-siirtymä

Siirtyessään asemat valitsevat seuraavan liityntäpisteen niiden lähettämän signaalin voimakkuuden ja laadun perusteella. Tätä varten asemat tarkkailevat jatkuvasti eri liityntäpisteiden lähetteiden ominaisuuksia. Monitorointi voi tapahtua joko yhdellä tai useammalla kanavalla.

2.6 Standardit

IEEE:n 802.11 -työryhmä [18] kehittää jatkuvasti WLAN-standardiaan ja siihen on jo olemassa sekä valmisteilla useita laajennuksia, jotka on eritelty kirjaimin standardin tunnuksen perässä. Suurin osa laajennuksista esittelee uusia kehittyneempiä fyysisen kerroksen ratkaisuja, joiden avulla pyritään entistä suurempiin tiedonsiirtonopeuksiin. Myös uusien fyysisten kerrosten kanssa käytetään yhä alkuperäistä MAC-kerrosta. Lisäksi standardin kehitysversiot tarjoavat ratkaisuja muun muassa tietoturva- ja yhteensopivuusongelmiin. Seuraavassa on esitelty lyhyesti 802.11-standardin olennaisimmat laajennukset.

IEEE 802.11a [19] käsittää fyysisen kerroksen, joka toimii 5 GHz:n UNII-taajuusalueella. Se perustuu OFDM-monikantoaaltotekniikkaan (Orthogonal Frequency Division Multiplexing) ja tarjoaa jopa 54 Mbps tiedonsiirtonopeuden. Järjestelmässä on 52 alikantoaaltoa, joiden modulointiin voidaan käyttää seuraavia tekniikoita: BPSK, QPSK, 16-QAM (Quadrature Amplitude Modulation) ja 64-QAM. Standardi on

suunnattu pääasiassa Yhdysvaltain markkinoille eikä se siten täytä eurooppalaisia vaatimuksia. Euroopan käytössä vaaditaan lisäksi IEEE 802.11h -laajennus [20], joka sisältää muun muassa dynaamisen kanavanvalinnan sekä lähetystehonsäädön.

Tämän hetken käytetyin WLAN-standardi IEEE 802.11b [21] määrittelee myös fyysisen kerroksen, joka perustuu alkuperäisen standardin suorasekvenssi hajaspektriin. 802.11b:n avulla saavutetaan parhaimmillaan 11 Mbps teoreettinen siirtonopeus. Uudet 5.5 ja 11 Mbps palvelunopeudet on toteutettu käyttämällä koodaukseen 11 sirun Barker-koodin sijaan 8 sirun CCK:ta (Complementary Code Keying). Valinnaisesti voidaan käyttää myös PBCC:tä (Packet Binary Convolutional Coding).

IEEE 802.11d -standardi [22] määrittelee tarvittavat laajennukset, jotta 802.11-verkkoja voidaan käyttää alkuperäisten kuuden sääntelyalueen ulkopuolella. Laajennuksen avulla liityntäpisteet voivat lähettää asemille kullakin alueella vaaditut radioparametrit. Lisäksi mekanismi mahdollistaa asemien liikkumisen eri sääntelyalueiden välillä.

Tekeillä olevan 802.11e-standardin tavoitteiksi on asetettu MAC-kerroksen ominaisuuksien kehittäminen esimerkiksi tarjoamalla QoS-tuki. Lisäksi tutkitaan turvallisuuden sekä DCF:n ja PCF:n tehokkuuden parantamista. Muutoksilla pyritään parantamaan 802.11-verkkojen tukea erilaisille reaaliaikaisille palveluille kuten VoIP, videoneuvottelu sekä audio- ja videosuoratoisto.

IEEE 802.11f [23] määrittelee liityntäpisteiden välisen kommunikoinnin, jota tarvitaan asemien liikkuessa laajennetun palveluryhmän alueella peruspalveluryhmästä toiseen. Kuten edellä todettiin, saattoi alkuperäisen standardin avoimuus tällä kohdin aiheuttaa yhteensopivuusongelmia eri laitevalmistajien liityntäpisteiden välillä. 802.11f:n esittelemä jakelujärjestelmässä toimiva liityntäpisteiden välinen protokolla (Inter-Access Point Protocol, IAPP) korjaa nämä puutteet.

802.11g-standardi [24] tarjoaa vielä yhden vaihtoehtoisen fyysisen kerroksen. Se laajentaa edelleen standardin b-versiota tavoitteena yhä parempi suorituskyky. 802.11g toimii 2.4 GHz:n kaistalla ja mahdollistaa suurimmillaan 54 Mbps siirtonopeuden. Alimmat nopeudet 11 Mbps saakka on toteutettu kuten 802.11b-standardissa, joten ne ovat keskenään yhteensopivia. Suuremmilla nopeuksilla käytetään OFDM-tekniikkaa. 802.11a:han verrattuna 802.11g:n kokonaiskapasiteetti on pienempi kapeamman taajuuskaistansa takia. G-version etuna taas on suurempi peittoalue.

Alkuperäisen standardin varsin haavoittuvaksi osoittautuneen tietoturvan takia on alettu kehittää IEEE 802.11i -standardia, joka sisältää kehittyneemmät

tietoturvamekanismit. Se määrittelee sekä salaus- että autentikointimenetelmät. Salaukseen voidaan käyttää kahta vaihtoehtoista protokollaa: TKIP (Temporal Key Integrity Protocol) ja CCMP (Counter mode with Cipher block chaining Message authentication code Protocol). Autentikointi ja salausavaintenhallinta on toteutettu IEEE 802.1X -standardin mukaisesti.

3 Mobile IPv6

Langattomien verkkojen kenties merkittävin lisäarvo tavanomaisiin langallisiin verkkoihin verrattuna on niiden suoma mahdollisuus liikkua – ei vain yhden tukiaseman alueella vaan myös verkosta toiseen – ilman, että tietoliikenneyhteys menetetään. Kuten edellä nähtiin, tarjoaa IEEE 802.11 -standardi kuitenkin vain rajoitetut liikkuvuusominaisuudet. Lisäksi liikuttaessa laajemmissa verkoissa kuten Internetissä aliverkosta toiseen liikkuvuudenhallinta yksinomaan linkkitasolla ei välttämättä ole riittävä ratkaisu vaan on otettava huomioon liikkuvan päätelaitteen vaikutukset myös ylemmillä protokollakerroksilla. Liikkuvuudenhallintaongelmaa täytyy siis käsitellä koko protokollapinon kannalta, jotta yhteys säilytetään aina käyttäjälle näkyvälle sovelluskerrokselle asti.

Tässä luvussa esitellään ensin lyhyesti liikkuvuusongelman syyt IP-verkoissa, minkä jälkeen käydään läpi Mobile IPv6 -protokollaa alkaen sen yleisistä ominaisuuksista ja arkkitehtuurista. Seuraavaksi kuvataan uudet pakettityypit ja muutokset IPv6:een sekä protokollan eri vaiheiden toiminta. Lisäksi tässä luvussa käsitellään protokollan tietoturvaa sekä kehitteillä olevia laajennuksia. Lopuksi suoritetaan vertailu MIPv6:n ja MIPv4:n välillä.

3.1 Liikkuvuusongelmat IP-verkoissa

IP-verkkoprotokollaa hyödyntävissä verkoissa liikkuvuuden toteuttaminen pelkästään linkkitasolla ei takaa verkkotason yläpuolella toimivien tiedonsiirtoprotokollien ja sitä kautta sovellusten katkeamatonta tiedonsiirtoa vaihdettaessa liityntäpistettä aliverkosta toiseen. Tämä johtuu IP-protokollan osoitejärjestelmästä, jossa osoitteella on kahtalainen merkitys. Ensinnäkin IP-osoitetta käytetään laitteiden tunnistamiseen, jotta paketit voidaan lähettää halutulle kohdekoneelle. Toisaalta taas IP-osoitteen verkkotunniste määrittelee aliverkon, johon

osoitetta käyttävä laite kuuluu. Koska reitittimet käyttävät pakettien välityksessä koko IP-osoitteen sijasta osoitteen verkko-osaa, eivät liikkuvan laitteen IP-osoitteeseen lähetetyt paketit enää tavoita sitä laitteen siirryttyä aliverkosta toiseen vaan paketit välitetään laitteen alkuperäiseen aliverkkoon, jossa niille ei kuitenkaan ole vastaanottajaa ja paketit hävitetään. Tällaiseen reitittimien toimintamalliin on päädytty, jotta reititystaulujen kokoa on saatu pienennettyä sekä järjestelmän skaalautuvuutta parannettua. [25]

Jotta liikkuva laite ei menettäisi liikennöintikykyään täysin, tulisi joko

- asettaa laitteelle uusi IP-osoite uuden aliverkon osoiteavaruudesta
- lisätä reitittimien reititystauluihin liikkuvalle laitteelle johtava reitti.

Kumpikaan ratkaisumalli ei kuitenkaan ole käytännössä laajemmassa mittakaavassa varteenotettava vaihtoehto. Jos laitteen osoite muutetaan, menetetään avoinna olevat yhteydet ja ne joudutaan aloittamaan uudelleen, mikä aiheuttaisi pitkän katkoksen liikenteeseen. Lisäksi kone ei ole enää tavoitettavissa sen alkuperäisestä osoitteesta eivätkä muut koneet voi aloittaa liikennöintiä osoitetta vaihtaneen koneen kanssa, koska ne eivät tiedä sen uutta osoitetta. Reitittimien reititystaulujen päivittäminen taas ei ole realistinen vaihtoehto, koska taulujen koko kasvaisi suoraan verrannollisesti liikkuvien koneiden määrään nähden ja myös reititysliikenne kasvaisi vastaavasti. Sinällään pelkkä IP-protokolla ei siis käytännössä tue liikkuvia päätelaitteita.

Edellä esitelty ongelma juontaa juurensa IPv4:n [1] kohdalla sen suunnittelusta, sillä kun nykyisin laajimmin käytössä olevan IP-protokollan nelosversiota kehiteltiin, ei näköpiirissä ollut liikkuvia tietokoneita eikä niiden tuomia lisävaatimuksia verkkotason protokollalle otettu siten lainkaan huomioon protokollan toiminnassa vaan suunnittelussa on keskitytty kiinteiden, paikallaan pysyvien koneiden yhteen liittämiseen mahdollisimman optimaalisesti. Toisaalta myös kuljetustasolla yleisesti käytettävän TCP-protokollan [26] kohdalla on tehty suunnitteluratkaisuja, jotka vaikeuttavat liikkuvuuden toteuttamista. TCP/IP-arkkitehtuurissa ei kerrosrakenne nimittäin ole siinä mielessä täydellinen, että TCP käyttää yhteyksien tunnistamiseen porttien lisäksi myös IP-osoitteita. Tämä on ristiriidassa kerrosrakenteen perusidean kanssa ja aiheuttaa avoimien TCP-yhteyksien katkeamisen, kun osoitetta vaihdetaan.

Myös IPv6:ssa [5] on edellä kuvatut IPv4:n osoitejärjestelmän perusmekanismit säilytetty eikä se siten suoranaisesti tuo ratkaisua liikkuvuusongelmaan, mutta liikkuvuus on kuitenkin huomioitu sen suunnittelussa, mikä antaa paremmat lähtökohdat liikkuvuudenhallinnan toteuttamiselle IPv6-ympäristössä.

3.2 Yleistä Mobile IP:stä

Langattomien verkkotekniikoiden yleistyessä tarve toimivalle liikkuvien laitteiden tuelle kasvoi, joten IETF perusti IP Routing for Wireless/Mobile Hosts -työryhmän, jonka tehtävä oli suunnitella liikkuvuudenhallintamekanismi IPv4:n päälle. Mekanismin oli määrä ratkaista liikkuvuudenhallinnan kaksi perusongelmaa:

- avoimien yhteyksien ylläpito liikuttaessa IP-aliverkosta toiseen
- tavoitettavuuden säilyttäminen liikuttaessa.

Ryhmän työn tuloksena julkaistiin vuonna 1996 ensimmäinen versio Mobile IPv4 -protokollasta [27]. Sen perusidea on, että kullakin liikkuvalla laitteella on samanaikaisesti kaksi osoitetta. Näistä ensimmäinen on kiinteä ja se kuuluu laitteen alkuperäisen ns. kotiverkon osoiteavaruuteen. Tätä osoitetta käyttävät kuljetustason protokollat ja sovellukset. Toinen osoite on väliaikainen ja muuttuu sitä mukaa, kun laite vaihtaa liityntäpistettään. Tätä osoitetta käytetään pakettien välityksessä liikkuvalle laitteelle. Kun laite siirtyy pois kotiverkosta ja saa väliaikaisen osoitteen, se ilmoittaa edellä mainitun osoitteen kotiverkossa olevalle agentille, joka tietää siten aina liikkuvan laitteen sijainnin ja pystyy välittämään sille osoitetut paketit kohteeseensa tunneloinnin avulla.

Nykyisin kehitystyötä tehdään kolmessa IETF:n työryhmässä: Mobility for IPv4 (mip4), Mobility for IPv6 (mip6) ja MIPv6 Signaling and Handoff Optimization (mipshop). Mip4 kehittää edelleen MIPv4-protokollaa, jonka uusin versio löytyy RFC:stä 3344 [4]. Mip6 taas on määritellyt IPv6:lle vastaavan äskettäin RFC-statuksen saaneen liikkuvuudenhallintamekanismin Mobile IPv6 [6], johon keskitymme tässä työssä jatkossa. Mipshop-työryhmä kehittelee menetelmiä, joiden avulla MIPv6-protokollan signaloinnin aiheuttamaa kuormaa voitaisiin vähentää ja toisaalta nopeuttaa yhteydenvaihtoa liityntäpisteiden välillä. Näitä menetelmiä esitellään lyhyesti tämän luvun loppupuolella.

Kun Mobile IPv6:tta lähdettiin suunnittelemaan, asetettiin protokollalle seuraavat vaatimukset [28].

- Liikkuvan laitteen pitää pystyä liikennöimään niin liikkuvien kuin kiinteiden laitteiden kanssa vaihdettuaan Internetin liityntäpistettä IP-aliverkosta toiseen vaihtamatta samalla kuitenkaan IP-osoitetta.
- Liikkuva laite tulee olla aina tavoitettavissa sen kotiosoitteesta riippumatta laitteen sijainnista. Kaikki laitteen kotiosoitteeseen lähetetyt paketit tulee

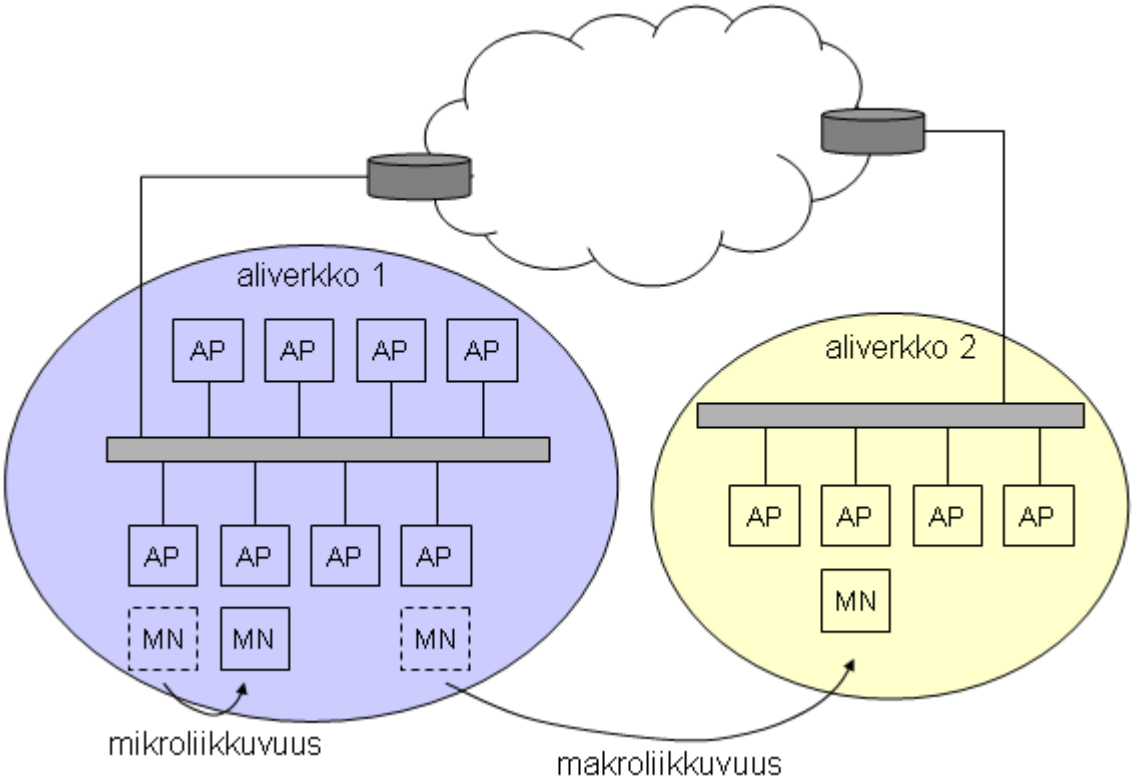
välittää sille. Tavoitettavuus on erityisen tärkeää suoria yhteyksiä hyödyntävien erilaisten vertaissovellusten käytön lisääntyessä.

- Liikkuvuudenhallintamekanismin tulee olla läpinäkyvä ylempien kerrosten kuljetusprotokollille ja sovelluksille. Ylempien kerrosten pitäisi jatkaa normaalia toimintaansa ilman mitään erityisvaatimuksia laitteen liikkuvuudesta ja liityntäpisteen vaihdoista huolimatta.
- Kaikki liikkuvan laitteen sijaintitiedon päivityksiin käytettävät paketit tulee autentikoida. Näin pyritään estämään ns. etäuudelleenohjaushyökkäykset (remote redirection), jossa hyökkääjä kaappaa liikkuvalle laitteelle osoitetun liikenteen yksinkertaisesti antamalla väärää tietoa laitteen sijainnista ja ohjaamalla liikenne siten haluttuun osoitteeseen.
- Liikkuvuudenhallintaan käytettävien signalointiviestien määrä ja koko tulisi olla mahdollisimman pieni, koska liikkuvat laitteet käyttävät usein verkkoon liittymiseen langattomia linkkejä, joiden tiedonsiirtokyky ja virhesuhde eivät ole yhtä hyviä kuin langallisissa verkoissa. Lisäksi liikkuvat laitteet ovat useimmiten akkukäyttöisiä, joten tehonkulutus tulisi minimoida. Protokollan synnyttämän signalointiliikenteen määrä on merkittävä tekijä myös skaalautuvuuden kannalta, sillä tulevaisuudessa on odotettavissa liikkuvien laitteiden määrän kasvavan huomattavasti.

Ottaen huomioon edellä esitetyt vaatimukset sekä Mobile IPv4:stä saadut kokemukset, päädyttiin Mobile IPv6 -protokollan toimintaperiaatteessa pääosiltaan samankaltaiseen ratkaisuun kuin Mobile IPv4:ssä, mutta siinä hyödynnetään IPv6:n tuomia useita uusia ominaisuuksia kuten suurempi osoiteavaruus, laajennusotsikot, automaattinen osoitteen konfigurointi sekä integroitu tietoturva. Liikkuvat päätelaitteet on myös otettu huomioon jo IPv6-protokollaa suunniteltaessa, joten liikkuvuudenhallinta on saatu paremmin yhdistettyä siihen ja MIPv6 kykenee siten tarjoamaan kehittyneempiä ominaisuuksia kuin MIPv4. Protokollaversioiden ominaisuuksia on vertailtu tämän luvun lopussa.

Mobile IPv6 on ns. makrotason liikkuvuudenhallintaprotokolla, millä tarkoitetaan, että liikkuminen tapahtuu laajan verkon, kuten Internetin, alueella aliverkosta toiseen. Käytännössä tämä näkyy siinä, että MIPv6 soveltuu paremmin tilanteisiin, joissa liikkuva laite vaihtaa verkon liityntäpistettä melko harvoin. Melko harvoin tarkoittaa tässä tapauksessa harvemmin kuin kerran sekunnissa vaikkakin protokolla todennäköisesti selviää myös useammin tapahtuvista yhteydenvaihdoista

[28]. Saman aliverkon sisällä esimerkiksi tukiasemasta toiseen vaihdettaessa taas puhutaan mikrotason liikkuvuudesta, jota hallitaan linkkitason mekanismeilla. Kuten edellä nähtiin, on muun muassa IEEE 802.11 -standardissa määritelty mikrotason liikkuvuudenhallinta. Koska yksittäisen tukiaseman peittoalue on huomattavasti pienempi kuin kokonaisen useiden tukiasemien muodostaman aliverkon, tapahtuu mikrotasolla yhteydenvaihtoja huomattavasti enemmän ja pienemmällä aikavälillä kuin makrotasolla. Liikkuvuuden eri tasot on esitetty kuvassa 18.



Kuva 18. Makro- ja mikroliikkuvuus

Nopeasti liikkuva päätelaite joutuu vaihtamaan liityntäpistettään usein ja uusi sijaintitieto pitää aina lähettää kotiverkon agentille. Tämä kasvattaa signalointiliikenteen määrää ja viivettä, jolloin myös ylemmän tason kuljetusprotokollien suorituskyky heikkenee. Ylimääräinen viive vaikuttaa haitallisesti erityisesti reaaliaikaisten sovellusten kuten esimerkiksi VoIPin laatuun. MIPv6:n yhteydenvaihdon sujuvuuden parantamiseksi on IETF:ssä esitetty monia erilaisia vaihtoehtoja kuten hierarkkinen Mobile IPv6 (Hierarchical Mobile IPv6, HMIPv6) [29] ja nopeat yhteydenvaihdot Mobile IPv6:lle (Fast Handovers for Mobile IPv6, FMIPv6) [30], jotka esitellään lyhyesti tämän luvun loppupuolella Mobile IPv6:n laajennuksia käsittelevässä kappaleessa. Lisäksi on olemassa ns. verkkoalueen sisäiset liikkuvuudenhallintaprotokollat Cellular IP [31] ja HAWAII [32], joita käytetään

Mobile IP:n rinnalla. Ne hallitsevat liikkuvuutta koko Internetin sijaan paikallisesti pienemmällä rajatulla alueella kuten esimerkiksi ISP:n, yrityksen tai kampusalueen verkossa. Näillä ratkaisuilla pyritään tyypillisesti rajoittamaan suurin osa liikkuvuuden hallinnan aiheuttamasta signalointiliikenteestä pienemmälle verkon alueelle, jolloin sijaintitiedon päivitykset tapahtuvat nopeammin ja Internetin kautta kotiverkkoon lähetettävien päivitysviestien määrä vähenee. Edellä mainittuja menetelmiä on vertailtu lukuisissa tutkimuksissa [33, 34, 35, 36].

Myös vaihtoehtoisia tapoja liikkuvuudenhallinnan toteuttamiseksi protokollapinon eri tasoilla on esitetty. Eräässä mallissa [37] ratkaisuksi on ehdotettu, että päätelaitteen sijaintitiedon ylläpitoon käytettäisiin dynaamisia päivityksiä nimipalveluun (Domain Name System, DNS) [38, 39] eli aina kun laite liikkuu ja saa uuden osoitteen, se päivittää osoitteen kotiverkon nimipalvelimen tietokantaan. Näin laite on aina tavoitettavissa sen nimen kautta. DNS:ssä käytetään välimuisteja järjestelmän skaalautuvuuden parantamiseksi ja kyselyiden nopeuttamiseksi. Jotta DNS-välimuisteihin ei jäisi vanhentunutta tietoa liikkuvan laitteen IP-osoitteesta, asetetaan nimipalvelimen liikkuvan laitteen nimeä vastaava tietue sellaiseksi, ettei sitä tallenneta välimuistiin. Tämä aiheuttaa luonnollisesti sen, että nimipalvelimeen lähetettyjen DNS-kyselyiden määrä kasvaa. Jottei TCP-yhteyksiä menetettäisi liikuttaessa, on lisäksi jouduttu laajentamaan TCP-protokollaa ominaisuuksilla, jotka mahdollistavat avoimen yhteyden päätepisteiden IP-osoitteiden vaihtamisen. Arkkitehtuuri ei vaadi muutoksia IP-protokollaan vaan liikkuvuudenhallinta on toteutettu täysin kuljetus- ja sovelluskerroksilla, mistä johtuen liikkuvuus täytyy huomioida erikseen jokaisessa liikkuvan laitteen käyttämässä kuljetusprotokollassa ja sovelluksessa. Liikkuvuustuen kehittäminen yksittäin jokaiseen protokollaan aiheuttaisi huomattavasti ylimääräistä päällekkäistä työtä. Tämän ratkaisun hyvä puoli on, että liikkuvuudenhallinta voidaan toteuttaa kunkin sovelluksen kohdalla sille ominaisten vaatimusten mukaisesti. Esitetyn mekanismin eduksi mainitaan muun muassa nopeat yhteydenvaihdot.

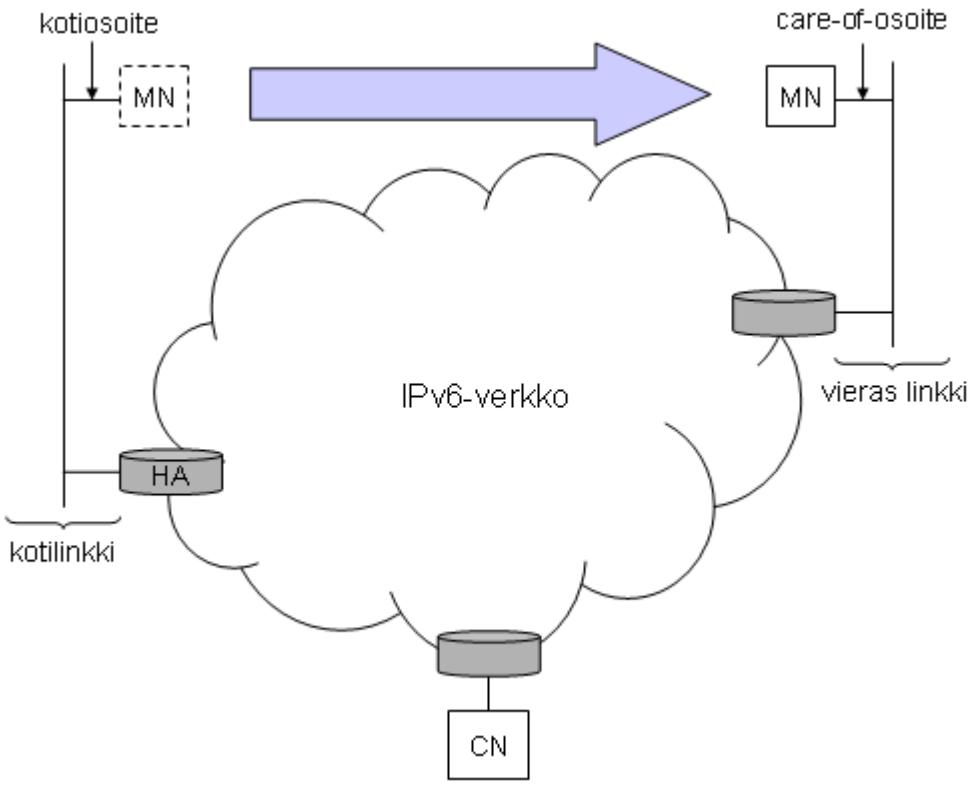
Toisessa ehdotuksessa [40] on esitetty liikkuvuudenhallinnan toteuttamista sovelluskerroksella Session Initiation Protocolin (SIP) [41] avulla. Ratkaisulla pyritään tukemaan Mobile IP:tä paremmin reaaliaikaisia palveluita käyttämällä hyväksi tietoa liikenteen ominaisuuksista ja vaatimuksista. SIP-protokolla tukee henkilöiden liikkuvuutta, mutta vaatii joitakin pieniä muutoksia laitteiden liikkuvuuden mahdollistamiseksi. Myös tämän vaihtoehdon heikkous on sovellusriippuvaisuus. Se ei myöskään pysty ylläpitämään TCP-yhteyksiä liikuttaessa ja artikkelissa ehdotetaankin

SIPin tarjoaman liikkuvuudenhallinnan käyttämistä reaaliaikasovelluksille samalla kun TCP-sovellukset käyttävät Mobile IP:tä. SIPin ja Mobile IP:n rinnakkaiskäytön tehokkuutta on selvitetty myös toisessa tutkimuksessa [42].

Liikkuvuudenhallinnan toteuttamisella verkkotasolla saavutetaan kuitenkin muutamia huomattavia etuja edellä esitettyihin vaihtoehtoisiin malleihin verrattuna. Ensinnäkin, koska verkkokerros on ainoa yhteinen kerros kaikille IP-verkoissa käytetyille sovelluksille, ei tarvita muutoksia erikseen jokaiseen kuljetuskerroksen protokollaan tai sovellukseen. Myös kaikkia uusia ylempien kerrosten protokollia voidaan käyttää liikkuvissa laitteissa ilman erityisvaatimuksia. Toisaalta, koska MIPv6 toimii verkkotasolla, on se riippumaton myös käytetystä linkkikerroksesta. Tämä mahdollistaa erilaisten langallisten ja langattomien linkkikerrosten, kuten Ethernet, WLAN ja GPRS, käyttämisen sekä siirtymisen linkkikerrokselta toiselle ilman, että IP-osoite muuttuisi tai käynnissä olevat yhteydet katkeaisivat. Tällöin voidaan käytettävissä olevista verkoista ja niiden kuormituksesta sekä palvelunlaatuvaatimuksista riippuen valita kulloinkin sopivin tiedonsiirtomedia.

3.3 Arkkitehtuuri

Mobile IPv6:n arkkitehtuurissa on pyritty tekemään mahdollisimman vähän muutoksia olemassa olevaan IP-verkkojen rakenteeseen ja toimintaan, jotta protokollan käyttöönotto ei vaatisi suuria uudistuksia jo käytössä olevaan verkkoon ja sen laitteisiin tai ohjelmistoihin. Vaikkakin on mahdollista lisätä liikkuvuudenhallintaominaisuudet joihinkin reitittimiin liikkuvuuden tukemiseksi, on käytössä olevan verkkolaitteiston suuren määrän vuoksi kuitenkin täysin mahdotonta vaatia muutoksia esimerkiksi kaikkiin reitittimiin pelkästään liikkuvuudenhallinnan vuoksi. Mitä vähemmän muutoksia tarvitaan, sitä nopeammin tekniikka myös otetaan käyttöön. Näin ollen MIPv6:ssa pyritään säilyttämään Internetissä käytetty periaate, jossa äly sijoittuu verkon laidoille. Mobile IPv6:n arkkitehtuuri ja uudet elementit on esitetty kuvassa 19.



Kuva 19. Mobile IPv6 -arkkitehtuuri

Arkkitehtuurin komponentit ovat:

- Liikkuva laite (Mobile Node, MN): IPv6-verkkoa käyttävä laite, esimerkiksi langattoman lähiverkkoliitännän sisältävä kannettava tietokone, joka pystyy vaihtamaan verkon liityntäpistettään linkistä toiseen säilyttäen samalla kuitenkin tavoitettavuuden kotiosoitteensa kautta. Liityntäpisteen vaihtuminen saattaa johtua laitteen fyysisestä liikkumisesta paikasta toiseen tai verkon topologian muutoksesta kuten esimerkiksi reitittimen hajoamisesta.
- Kotiosoite: Liikkuvalle laitteelle määritelty pysyvä IPv6-osoite, jonka kautta laite on aina tavoitettavissa ja jota sovellukset käyttävät. Kotiosoite kuluu kotilinkin osoiteavaruuteen. Liikkuvalla laitteella voi olla myös useita kotiosoitteita, jos esimerkiksi kotilinkille on määritelty useita verkkotunnisteita. Liikkuvan laitteen kotiosoitteeseen lähetetyt paketit reititetään laitteen kotilinkille tavanomaisten IP-reititysmekanismien mukaisesti.
- Kotilinkki: Kotilinkki on linkki, jonka verkkotunniste on sama kuin liikkuvan laitteen kotiosoitteen verkkotunniste. Kun liikkuva laite on liittyneenä verkkoon kotilinkkinsä kautta, ei Mobile IPv6:tta käytetä vaan

liikennöinti tapahtuu normaalisti. Kotiosoitteensa kautta liikkuva laite on aina loogisesti kytketty kotilinkkiinsä.

- Vieras linkki: Mikä tahansa linkki paitsi liikkuvan laitteen kotilinkki.
- Care-of-osoite: Liikkuvalle laitteelle vieraan linkin osoiteavaruudesta määritelty väliaikainen IPv6-osoite, jota käytetään pakettien välittämisessä laitteelle sen sijaitessa vieraalla linkillä. Care-of-osoite hankitaan IPv6:lle määriteltyjen mekanismien mukaisesti joko tilallisella tai tilattomalla automaattisella konfiguroinnilla. Liikkuvalla laitteella voi olla samanaikaisesti useita care-of-osoitteita, joista vain yksi on rekisteröity kotiagentille. Tätä osoitetta kutsutaan ensisijaiseksi care-of-osoitteeksi.
- Kotiagentti (Home Agent, HA): Liikkuvan laitteen kotilinkillä oleva reititin, johon laite rekisteröi senhetkisen care-of-osoitteensa siirryttyään pois kotilinkiltä. Kotiagentti kaappaa rekisteröityneen liikkuvan laitteen kotiosoitteeseen osoitetut paketit kotilinkiltä ja tunneloi ne kapselointia käyttämällä laitteen care-of-osoitteeseen. Kotiagentti voi olla kotilinkin IPv6-verkkoon liittävä reititin kuten kuvassa 19 tai se voi olla erillinen kotilinkillä sijaitseva laite, joka hoitaa ainoastaan liikkuvien laitteiden liikenteen välityksen näiden ollessa poissa kotilinkiltä.
- Vertaislaite (Correspondent Node, CN): Mikä tahansa IPv6-verkkoon kytketty laite, jonka kanssa liikkuva laite kommunikoi. Vertaislaite voi olla joko kiinteä tai liikkuva eikä sen tarvitse välttämättä toteuttaa mitään Mobile IPv6:n toimintoja.

Lisäksi määritellään seuraavat Mobile IPv6:n toiminnan kannalta keskeiset käsitteet ja tietorakenteet:

- Sidos (binding): Sidoksella tarkoitetaan liikkuvan laitteen kotiosoitteen ja care-of-osoitteen assosiaatiota. Sidokseen liittyy aina myös sen jäljellä oleva elinaika. Sidoksen avulla kotiagentti osaa välittää liikkuvalle laitteelle osoitetut paketit sen sijaintipaikkaan.
- Sidosvälimuisti (Binding Cache): Välimuisti, joka sisältää tiedot liikkuvien laitteiden senhetkisistä rekisteröidyistä sidoksista. Sekä kotiagentit että vertaislaitteet ylläpitävät sidosvälimuistia. Sidosvälimuistin tarkkaa toteutusta ei ole määritelty Mobile IPv6:n spesifikaatiossa, mutta sen tulee toteuttaa vaaditut toiminnot.

- Sidospäivityslista (Binding Update List): Jokainen liikkuva laite ylläpitää sidospäivityslistaa, joka sisältää tiedot laitteen muihin koneisiin muodostamista sidoksista. Aina kun laite rekisteröi care-of-osoitteensa johonkin koneeseen lähettämällä sidospäivitysviestin, lisätään siitä tiedot sidospäivityslistaan. Kun sidoksen elinaika loppuu, poistetaan kyseinen tietue listasta. Listan avulla liikkuva laite tietää milloin kukin sidos täytyy virkistää, jottei sen elinaika ehdi kulua umpeen
- Kotiagenttilista: Kotiagentit ylläpitävät kotiagenttilistaa, joka sisältää tiedot muista samalla linkillä olevista kotiagenteista. Listaa tarvitaan dynaamisessa kotiagentin osoitteenetsinnässä (Dynamic Home Agent Address Discovery, DHAAD), jotta kotiagentti voi lähettää tiedot käytettävissä olevista kotiagenteista liikkuvalle laitteelle.

3.4 Pakettityypit

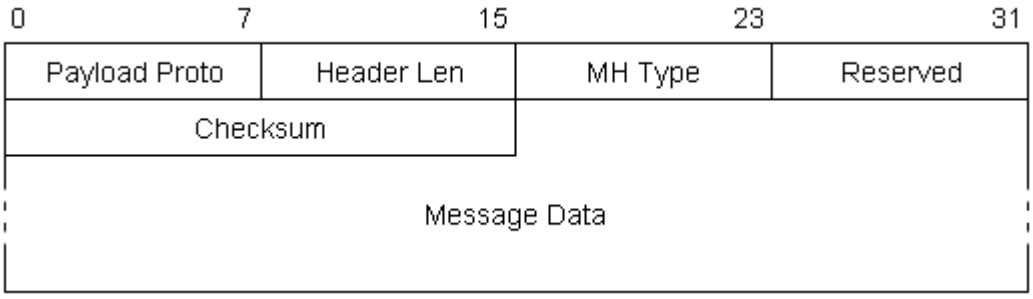
Mobile IPv6 määrittelee uuden IPv6-protokollan käyttämällä liikkuvuusotsikkoa (Mobility Header), jota hyödynnetään suuressa osassa liikkuvuudenhallinnan signalointiviestejä. Lisäksi on tehty joitakin muutoksia ja lisäyksiä jo olemassa oleviin IPv6-protokolliin. Seuraavissa kappaleissa esitellään keskeisimmät uudet pakettityypit.

3.4.1 Liikkuvuusotsikko

Liikkuvuusotsikko on laajennusotsikko, jota liikkuvat laitteet, kotiagentit ja vertaislaitteet käyttävät kaikkeen sidostenhallintaa koskevaan viestintään. Otsikon rakenne on esitetty kuvassa 20 ja se sisältää seuraavat kentät:

- Payload Proto: 8-bittinen kenttä, joka kertoo seuraavana olevan otsikon tyypin. Kenttää tullaan mahdollisesti käyttämään tulevaisuuden laajennuksissa, mutta tässä vaiheessa sen arvo on aina IPPROTO_NONE (59) eli liikkuvuusotsikko on paketin viimeinen otsikko.
- Header Len: määrittelee liikkuvuusotsikon pituuden.
- MH Type: oktetin kokoinen valitsin, joka identifioi liikkuvuudenhallintaviestin tyypin.
- Reserved: varattu mahdollista tulevaa käyttöä varten.
- Checksum: 16-bittinen tarkistussumma, joka lasketaan pseudo-otsikosta ja liikkuvuusotsikosta.

- Message Data: muuttuvan kokoinen kenttä, joka sisältää MH Type -kentän osoittaman liikkuvuudenhallintaviestin datan.



Kuva 20. Liikkuvuusotsikon muoto

Kutakin toimintoa varten on määritelty oma liikkuvuusotsikkoa käyttävä liikkuvuudenhallintaviesti. Viestityypit ovat:

Binding Refresh Request (MH Type = 0)

Vertaislaitteet käyttävät tätä viestiä pyytäessään liikkuvaa laitetta päivittämään sidoksensa. Tämä tapahtuu tyypillisesti, kun sidos on yhä käytössä mutta sen elinikä on loppumassa.

Home Test Init (1), Care-of Test Init (2), Home Test (3), Care-of Test (4)

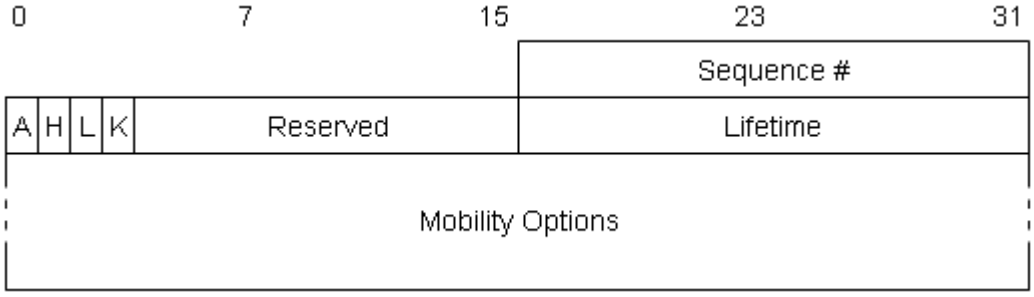
Näitä neljää sanomaa käytetään Return Routability -prosessissa, jonka avulla autentikoidaan vertaislaitteelle lähetettävät sidospäivitykset. Prosessi esitellään myöhemmin tässä luvussa.

Binding Update (5)

Liikkuva laite käyttää sidospäivitysviestiä (kuva 21) ilmoittaakseen kotiagentille tai vertaislaitteelle uuden care-of-osoitteensa. Viesti sisältää seuraavat kentät:

- Acknowledge (A): asettamalla tämän kentän arvoksi yksi, voi liikkuva laite pyytää viestin vastaanottajaa lähettämään kuittausviestin.
- Home Registration (H): kun tämä kenttä on yksi, pyytää liikkuva laite viestin kohdetta toimimaan laitteen kotiagenttina.
- Link-Local Address Compatibility (L): tämä bitti asetetaan ykköseksi, kun liikkuvan laitteen kotiosoitteen ja paikallisen linkkiosoitteen (link-local) liitäntätunnisteet (interface identifier) ovat samat.
- Key Management Mobility Capability (K): määrittelee selviytyykö käytetty avaintenhallintaprotokolla liikkumisesta.
- Reserved: ei käytössä.
- Sequence #: 16-bittinen järjestysnumero.

- Lifetime: sidoksen elinikä, yksi yksikkö neljä sekuntia. Jos kentän arvo on nolla, pitää vastaava tietue poistaa sidosvälimuistista.
- Mobility Options: muuttuvan kokoinen kenttä, joka sisältää mahdolliset liikkuvuusotsikon optiot.

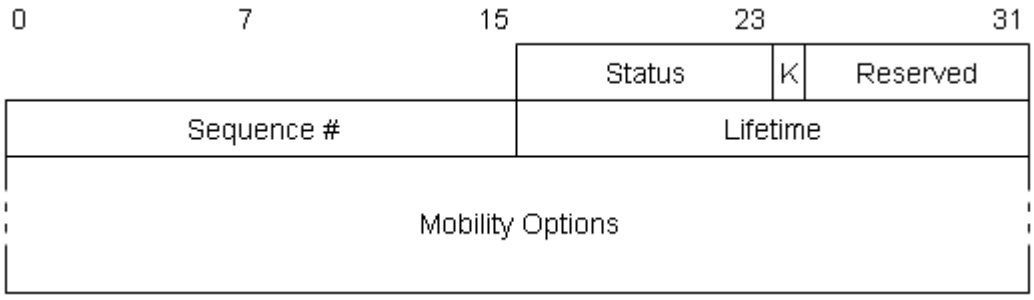


Kuva 21. Sidospäivitysviestin dataosuus

Binding Acknowledgement (6)

Sidoskuittausviestillä (kuva 22) voidaan ilmoittaa liikkuvalle laitteelle sen lähettämän sidospäivitysviestin perille saapumisesta. Kuittaus lähetetään, jos sitä erikseen pyydetään sidospäivitysviestissä, kyseessä on rekisteröinti kotiagentille tai jos sidoksen rekisteröinnissä tapahtui virhe. Sanoma koostuu seuraavista kentistä:

- Key Management Mobility Capability (K): määrittelee selviytyykö käytetty avaintenhallintaprotokolla liikkumisesta.
- Reserved: ei käytössä.
- Status: määrittelee sidospäivityksen tilan. Alle 128 olevat arvot tarkoittavat, että päivitys hyväksyttiin. 128 ja sen yli olevat arvot merkitsevät, että päivitys hylättiin jostain syystä. Tilalle on tällä hetkellä määritelty 14 eri arvoa.
- Sequence #: 16-bittinen järjestysnumero, joka kopioidaan sidospäivitysviestistä.
- Lifetime: sidokselle myönnetty elinikä.
- Mobility Options: muuttuvan kokoinen kenttä, joka sisältää mahdolliset liikkuvuusotsikon optiot.

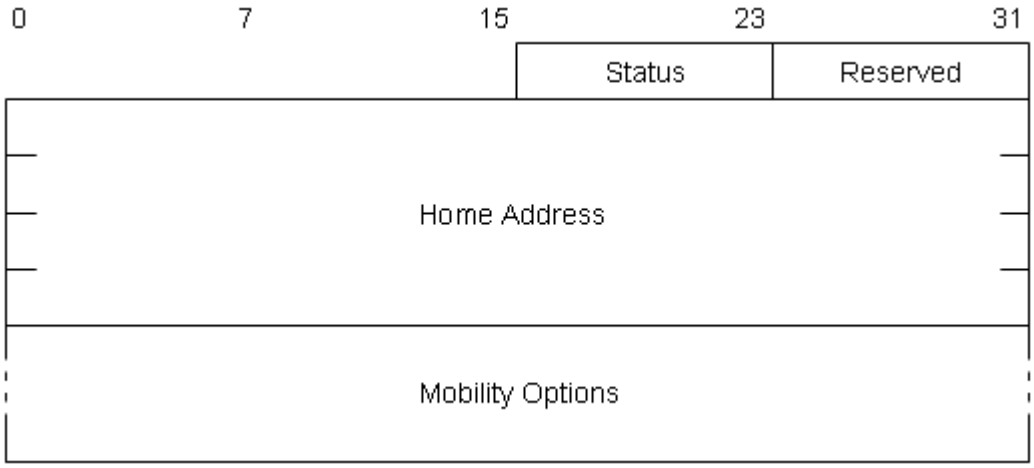


Kuva 22. Sidoskuittausviestin dataosuus

Binding Error (7)

Vertaislaite voi käyttää sidosvirheviestiä kertoakseen liikkuvalle laitteelle liikkuvuudenhallintaan liittyvästä virheestä. Viestin rakenne on esitetty kuvassa 23 ja sen kentät ovat:

- Status: määrittelee virheen syyn. Kentälle on tällä hetkellä olemassa 2 eri arvoa.
- Reserved: ei käytössä.
- Home Address: virheen aiheuttaneen viestin sisältämä kotiosoite.
- Mobility Options: muuttuvan kokoinen kenttä, joka sisältää mahdolliset liikkuvuusotsikon optiot.



Kuva 23. Sidosvirheviestin dataosuus

Edellä esitellyt liikkuvuusotsikkoa käyttävät viestit voivat lisäksi sisältää erilaisia optioita, joita ovat:

Pad1, PadN

Näitä optioita käytetään täytteenä, jotta paketista saadaan määrätyn kokoinen. Pad1 lisää yhden oktetin täytettä ja PadN lisää 2 tai useampia oktetteja.

Binding Refresh Advice

Kotiagentti voi tällä optiolla ilmoittaa sidoskuittausviestissä liikkuvalle laitteelle ajan, jonka jälkeen sen pitäisi lähettää uusi sidospäivityssanoma.

Alternate Care-of Address

Normaalisti sidospäivitysviesteissä care-of-osoite asetetaan IPv6-paketin lähdeosoitteeksi, mutta joissakin tapauksissa tämä ei esimerkiksi tietoturvasyistä ole mahdollista. Tällöin käytetään Alternate Care-of Address -optiota, joka sisältää sidoksen care-of-osoitteen.

Nonce Indices

Tätä optiota käytetään vain yhdessä Binding Authorization Data -option kanssa vertaislaitteelle lähetetyissä sidospäivitysviesteissä. Vertaislaite käyttää option sisältämää tietoa avainten muodostamisessa.

Binding Authorization Data

Sisältää viestin todentamiseen käytettävän kryptografisen datan.

3.4.2 Kotiosoiteoptio

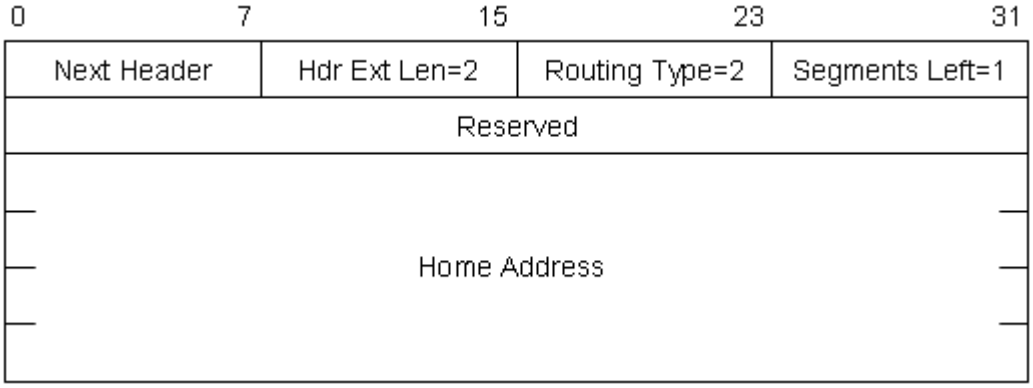
Kotiosoiteoptio on IPv6:n kohdeoptio-laajennusotsikkoon sijoitettava optio, jolla kotiverkosta poissa oleva liikkuva laite ilmoittaa kotiosoitteensa paketin vastaanottajalle. Sitä käytetään sekä sidospäivitysviesteissä että liikkuvan laitteen suoraan vertaislaitteelle lähettämissä datapaketeissa, kun vertaislaitteelle on muodostettu sidos. Optiota tarvitaan, jotta paketin IPv6-otsikon lähdeosoitteeksi voidaan asettaa topologisesti oikea osoite (care-of-osoite). Tällöin vältytään siltä, että ingress-suodatusta käyttävät reitittimet pudottaisivat paketin.

3.4.3 Tyypin 2 reititysotsikko

Tyypin 2 reititysotsikko on Mobile IPv6:n määrittelemä uusi reititysotsikko, jonka avulla vertaislaitteet voivat lähettää paketteja suoraan liikkuvalle laitteelle sen care-of-osoitteeseen. Uutta reititysotsikkoa käytetään ilmaisemaan kohdekoneen kotiosoite ja se eroaa normaalista lähdereitityksen käytetystä tyypin 0 reititysotsikosta siten, että se voi sisältää vain yhden IPv6-osoitteen. Lisäksi määrittelemällä Mobile IPv6:lle oma otsikkotyyppi, voidaan eri otsikoille haluttaessa asettaa erilaiset säännöt palomuureihin. Tyypin 2 reititysotsikko (kuva 24) sisältää seuraavat kentät:

- Next Header: kertoo seuraavan otsikon tyypin.

- Hdr Ext Len: 2.
- Routing Type: 2.
- Segments Left: 1.
- Reserved: varattu tulevaa käyttöä varten.
- Home Address: paketin kohteena olevan liikkuvan laitteen kotiosoite.



Kuva 24. Tyypin 2 reititysotsikko

3.4.4 Uudet ICMPv6-viestit

Mobile IPv6 määrittelee myös neljä uutta ICMPv6-protokollan [43] viestityyppiä, joita käytetään liikkuvan laitteen tarvitsemien kotiagentin osoitteen ja kotiosoitteen automaattisen konfigurointiin laitteen ollessa poissa kotiverkosta. Jos edellä mainitut tiedot jostain syystä muuttuvat tai liikkuva laite ei tiedä niitä, täytyy sen hankkia ajan tasalla olevat tiedot itselleen pystyäkseen toimimaan. Uudet ICMPv6-viestityypit ovat:

ICMP Home Agent Address Discovery Request (Type = 143)

Liikkuva laite lähettää tämän viestin kotiverkkoonsa käynnistääkseen DHAAD-prosessin.

ICMP Home Agent Address Discovery Reply (144)

Kotilinkillä oleva kotiagentti käyttää tätä viestiä vastatessaan liikkuvan laitteen lähettämään DHAAD-pyyntöön. Se sisältää käytettävissä olevien kotiagenttien osoitteet.

ICMP Mobile Prefix Solicitation (145)

Liikkuva laite voi tällä viestillä pyytää kotiagenttia lähettämään kotiverkossa käytössä olevat verkkotunnisteet, joiden avulla se voi muodostaa itselleen kotiosoitteen.

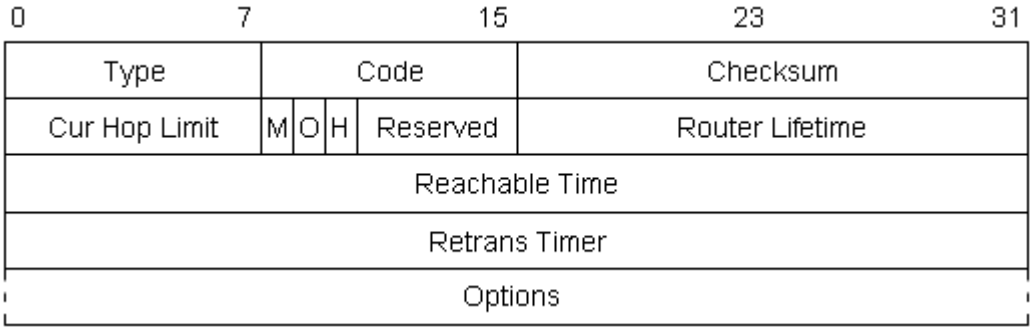
ICMP Mobile Prefix Advertisement (146)

Kotiagentti käyttää tätä viestiä mainostaakseen kotiverkosta poissa oleville liikkuville laitteille kotilinkillä käytössä olevista verkkotunnisteista.

3.4.5 Muutokset IPv6 Neighbor Discovery -protokollaan

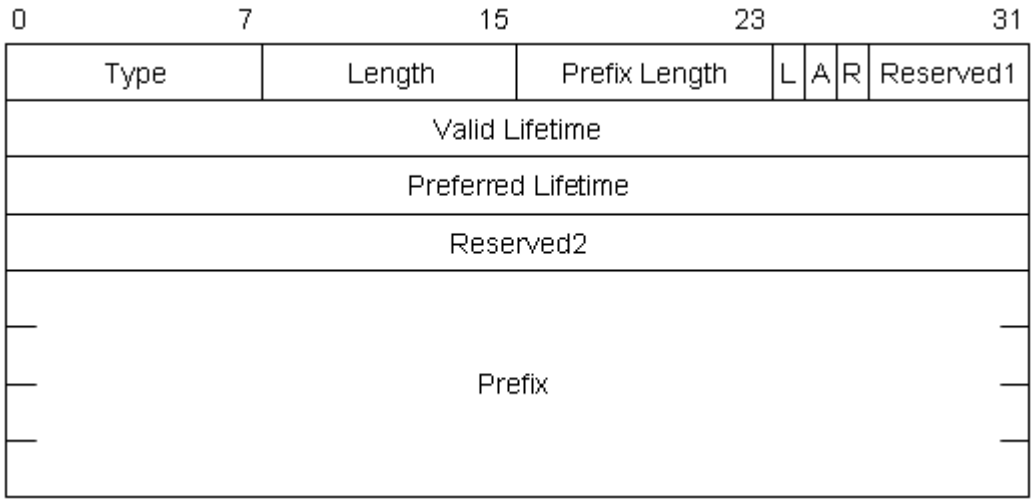
Mobile IPv6 pyrkii hyödyntämään mahdollisimman paljon IPv6:n mukanaan tuomia uusia mekanismeja. Yksi näistä on Neighbor Discovery -protokolla [44], jota käytetään mm. samalla linkillä olevien reitittimien ja muiden naapurikoneiden etsimiseen sekä laitteiden linkkikerroksen osoitteiden selvittämiseen. Lisäksi se ylläpitää tietoa linkin laitteiden saavutettavuudesta. MIPv6:n toimintoja varten protokollaan ja sen paketteihin on tehty joitakin muutoksia.

Ensinnäkin reitittimien mainosviestiin (kuva 25) on lisätty yhden bitin kenttä (H), joka ilmaisee toimiiko mainoksen lähettänyt reititin kotiagenttina. Samalla luonnollisesti tulevaan käyttöön varattu Reserved-kenttä lyheni yhdellä bitillä.



Kuva 25. Reitittimen mainosviesti

Myös verkkotunnisteoptiota on laajennettu, jotta reitittimet voivat paikallisen linkkiosoitteen lisäksi mainostaa myös globaalia IPv6-osoitettaan. Tätä varten optioon (kuva 26) lisättiin yhden bitin lippu (R), joka ilmaisee, että optio sisältääkin verkkotunnisteen sijaan reitittimen globaalin osoitteen. Kotiagentin lähettämien reitittimen mainosviestien tulee sisältää vähintään yksi verkkotunnisteoptio, jossa R-bitti on päällä. Kumpaakin näistä lisäyksistä tarvitaan DHAAD-mekanismissa.



Kuva 26. Verkkotunnisteoptio

Edellisten muutosten lisäksi Mobile IPv6 määrittelee kaksi kokonaan uutta Neighbor Discovery -protokollan optiota:

Advertisement Interval

Kotiagentti voi tällä optiolla ilmoittaa reitittimen mainosviestissä aikavälin, jolla se lähettää mainoksia.

Home Agent Information

Tällä optiolla kotiagentti voi puolestaan mainostaa toimintaansa liittyviä ominaisuuksia kuten elinaikaa.

3.5 Toiminta

Seuraavissa kappaleissa käydään läpi Mobile IPv6 -protokollan varsinaista toimintaa eri tilanteissa. Protokollan keskeisimpiä toimintoja ovat liikkumisen seuranta, sidosten rekisteröinti ja hallinta sekä pakettien reititys liikkuvan laitteen ja vertaislaitteen välillä. Lisäksi standardissa on määritelty kaksi mekanismia, joilla voidaan hoitaa liikkuvan laitteen tarvitsemien tietojen automaattinen konfigurointi.

3.5.1 Liikkumisen seuranta

Jotta liikkuva laite pystyy suorittamaan vaadittavat toimenpiteet siirryttyään pois kotilinkiltä, tulee sen voida havaita siirtyminen linkiltä toiselle. Mobile IPv6:ssa tämä liikkumisen havaitseminen perustuu Neighbor Discovery -protokollaan ja erityisesti sen Router Discovery ja Neighbor Unreachability Detection -toimintoihin. MIPv6:ssa määritelty menetelmä on tarkoitettu yleiseksi liikkumisen seurantamekanismiksi eikä sitä ole optimoitu nopeita yhteydenvaihtoja tai tiettyä linkkikerrosta varten.

Perusmenetelmää voidaan tehostaa käyttämällä lisäksi muita mekanismeja, jotka hyödyntävät esimerkiksi linkkikerrokselta saatavia tietoja. Näitä laajennuksia ei kuitenkaan ole määritelty Mobile IPv6:ssa.

Kaikki IPv6-reitittimet ilmoittavat olemassaolostaan lähettämällä säännöllisin väliajoin Neighbor Discovery -protokollaan kuuluvia Router Advertisement -viestejä. Liikkuva laite määrittelee vastaanottamiensa Router Advertisement -viestien perusteella oletusreitittimensä. Samalla selviää myös onko laite kotilinkillä vai vieraalla linkillä. Neighbor Unreachability Detection -mekanismin avulla liikkuva laite taas huomaa, jos sen käyttämä oletusreitin ei ole enää tavoitettavissa. Se voi tarkoittaa että laite on siirtynyt linkiltä toiselle tai että kyseinen reititin on esimerkiksi vikaantunut. Tällöin liikkuvan laitteen tulee joka tapauksessa etsiä itselleen uusi oletusreititin Router Discovery -mekanismilla. Jos uusi oletusreititin sijaitsee eri linkillä kuin edellinen oletusreititin, on yhteydenvaihto verkkokerroksella tapahtunut ja liikkuvan laitteen pitää ilmoittaa uusi sijaintinsa kotiagentille.

Jotta liikkumisen seuranta toimisi paremmin, on Mobile IPv6:ssa määritelty Neighbor Discovery -protokollan parametreihin muutoksia, jotka mahdollistavat Router Advertisement -viestien lähettämisen normaalia tiheämmin. Lisäksi reitittimet voivat käyttää mainoksissa Advertisement Interval -optiota, joka kertoo linkin koneille kuinka usein kyseinen reititin lähettää mainoksia. Liikkuva laite voi käyttää tätä tietoa hyväksi selvittäessään oletusreitittimensä tavoitettavuutta.

3.5.2 Sidosten hallinta ja pakettien reititys

Liikkuvan laitteen ollessa kotiverkossaan pakettien reititys tapahtuu normaalien IPv6-mekanismien mukaisesti. Laitteen vieraillessa vieraassa verkossa on olemassa kaksi vaihtoehtoista tapaa välittää paketteja vertaislaitteen ja liikkuvan laitteen välillä: käänteistunnelointi (Reverse Tunneling) ja reitinoptimointi (Route Optimization). Käänteistunnelointi on Mobile IPv6:n perusmenetelmä ja se perustuu liikkuvan laitteen ja kotiagentin välille muodostettavaan kaksisuuntaiseen tunneliin. Reitinoptimointi taas on tehokkaampi tapa, jossa hyödynnetään edellä esiteltyjä uusia IPv6-laajennusotsikoita. Jotta näitä reititysmahdollisuuksia voidaan käyttää, täytyy liikkuvan laitteen suorittaa sidosten hallintaa. Tällä tarkoitetaan sidosten luomista, virkistämistä ja kotiverkkoon palattaessa poistamista.

Kun laite huomaa siirtyneensä pois kotiverkosta vieraaseen verkkoon ja saaneensa uuden oletusreitittimen, se muodostaa itselleen care-of-osoitteen joko

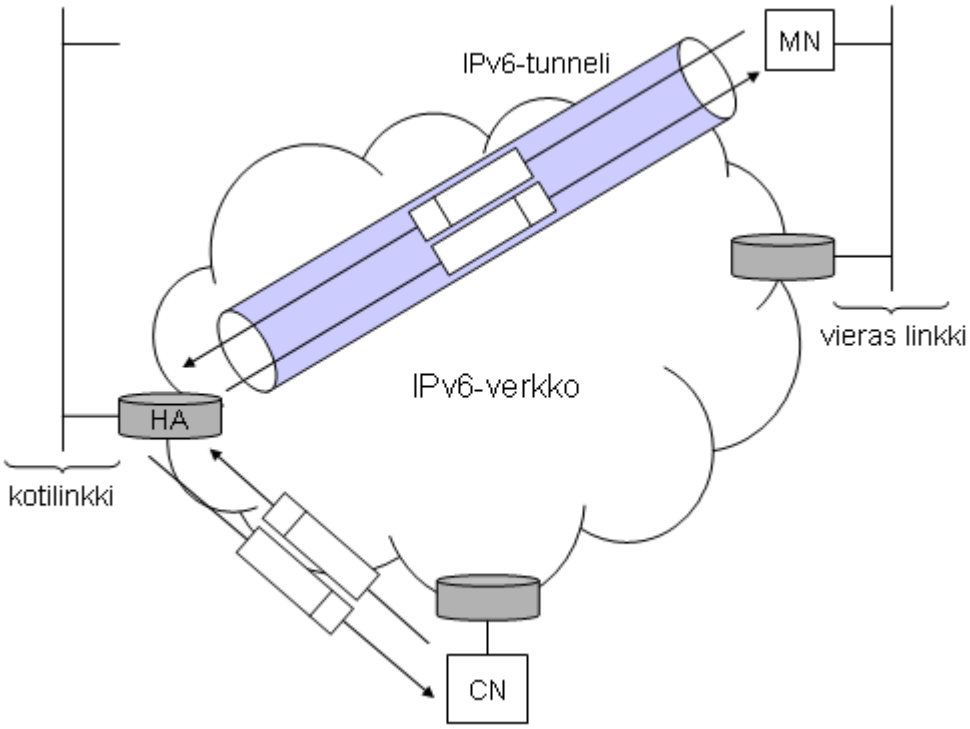
tilattomalla [45] tai tilallisella osoitteen automaattisella konfiguroinnilla (esimerkiksi DHCPv6 [46]). Hankittuaan kelvollisen care-of-osoitteen liikkuva laite lähettää kotiagentille sidospäivitysviestin, jolla se rekisteröi uuden sidoksen. Viesti sisältää kotiosoiteoption sekä Alternate Care-of Address -option, jotka määrittelevät vastaavasti sidoksen kotiosoitteen ja care-of-osoitteen. Aina sidospäivitysviestiä lähetettäessä viestin tiedot tallennetaan myös sidospäivityslistaan. Mikäli viesti läpäisee tarkistukset, kotiagentti lisää sidoksen sidosvälimuistiinsa ja vastaa viestiin sidospäivityskuittauksella, jonka mukaisesti liikkuva laite päivittää vastaavan tietueen sidospäivityslistassaan. Listan perusteella laite tietää virkistää sidoksensa ajoissa ennen sen elinajan loppumista.

Käänteistunneloinnissa liikkuvan laitteen ja kotiagentin välille muodostetaan kaksisuuntainen IPv6-tunneli [47]. Jotta kotiagentti pystyy välittämään liikkuvalle laitteelle lähetyt paketit tunnelin kautta perille, pitää sen kaapata liikkuvan laitteen kotiosoitteeseen osoitetut paketit itselleen. Kaappaus tapahtuu proxy Neighbor Discovery -menetelmällä, jossa kotiagentti lähettää ryhmälähetyksenä laitteen kotilinkin koneille Neighbor Discovery -protokollan Neighbor Advertisement -viestin, joka liittää liikkuvan laitteen kotiosoitteen kotiagentin linkkikerroksen osoitteeseen. Tämän jälkeen kaikki liikkuvan laitteen kotiosoitteeseen lähetetyt paketit ohjautuvat kotiagentille, joka lähettää ne tunnelia pitkin care-of-osoitteeseen. Liikkuva laite purkaa tunnelissa käytetyn kapseloinnin ja antaa näin saadun alkuperäisen kotiosoitteeseensa osoitetun paketin edelleen ylemmälle protokollakerrokselle.

Kun liikkuva laite puolestaan lähettää vertaislaitteelle paketin, reititetään myös se kotiagentin kautta käyttämällä tunnelia toiseen suuntaan. Kotiagentti purkaa kapseloinnin ja välittää paketin edelleen vertaislaitteelle. Vertaislaitteen näkökulmasta näyttää siis siltä kuin liikkuva laite olisi tavallinen kiinteä laite. Käyttämällä tunnelia myös tähän suuntaan vältytään ingress-suodatuksen aiheuttamilta ongelmilta, joita syntyisi, jos liikkuva laite yrittäisi lähettää paketit suoraan vertaislaitteelle käyttäen lähdeosoitteena kotiosoitettaan. Käänteistunneloinnin pakettien reititys on esitetty kuvassa 27.

Lyhytaikaisessa yhteydettömässä viestinnässä kuten esimerkiksi DNS-kyselyissä liikkuva laite voi hyödyntää myös normaaleja IPv6-mekanismeja käyttämällä care-of-osoitettaan lähdeosoitteena. Tällöin menetys ei ole suuri, jos transaktio ei jostain syystä onnistu, koska uudelleenyritys ei aiheuta merkittävää lisäkuormaa. Jos taas avattavaa

yhteyttä halutaan käyttää myös mahdollisten yhteydenvaihtojen jälkeen tai sen kestosta ei ole tietoa, on käytettävä Mobile IPv6:n tarjoamia mekanismeja.



Kuva 27. Pakettien välitys käänteistunneloinnilla

Edellä esitetty pakettien reititys kotiagentin kautta muodostaa liikkuvan laitteen ja vertaislaitteen välille epäedullisen reitin, joka heikentää selvästi laitteiden välisen tiedonsiirtoyhteyden suorituskykyä. Tämän vuoksi Mobile IPv6:lle on määritelty myös vaihtoehtoinen mekanismi eli reitinoptimointi, jota voidaan käyttää lisänä käänteistunneloinnin rinnalla. Reitinoptimoinnissa on kyse nimen mukaisesti liikkuvan laitteen ja vertaislaitteen välisen reitin optimoinnista ja liikennöinti laitteiden välillä tapahtuu suoraan eikä kotiagentin kautta. Menetelmä vaatii kuitenkin vertaislaitteelta joidenkin Mobile IPv6 -toimintojen kuten sidosvälimuistin ylläpidon ja liikkuvuudenhallintaviestien käsittelyn toteuttamista. Tästä johtuen sitä ei voida hyödyntää kaikkien IPv6-verkon laitteiden kanssa kuten epäsuoraa reititystä käyttävää käänteistunnelointia. Uuden vertaislaitteen kanssa muodostetun yhteyden alkuvaiheessa käytetään aina käänteistunnelointia, josta voidaan siirtyä reitinoptimointiin. Jos reitinoptimoinnin käyttö ei jostain syystä onnistu, palautuu pakettien reititys käänteistunneloinnin mukaiseksi.

Kun liikkuva laite huomaa vastaanottavansa paketteja tunnelin kautta, se voi yrittää käyttää reitinoptimointia kyseisen vertaislaitteen kanssa. Tämä tapahtuu lähettämällä vertaislaitteelle sidospäivitysviesti vastaavasti kuin kotiagentille. Viestin

muoto poikkeaa kotiagentille lähetettävistä sidospäivitysviesteistä siten, että se ei sisällä Alternate Care-of Address -optiota vaan Binding Authorization Data ja Nonce Indices -optiot, joita käytetään viestin todentamisessa. Care-of-osoite asetetaan tällöin IPv6-otsikon lähdeosoitteeksi. Jos vertaislaite tukee reitinoptimointia ja sidospäivitysviesti läpäisee tarkistukset, se lisää sidoksen sidosvälimuistiinsa ja lähettää pyydettäessä kuittauksen. Tämän jälkeen vertaislaite voi lähettää paketit suoraan liikkuvalle laitteelle käyttämällä paketissa tyypin 2 reititysotsikkoa, johon sijoitetaan liikkuvan laitteen kotiosoite. Paketin kohdeosoitteeksi asetetaan care-of-osoite, jonne paketti ohjautuu normaalin IPv6-reityksen mukaisesti. Liikkuvan laitteen vastaanottaessa paketin se huomaa reititysotsikon ja korvaa kohdeosoitteen reititysotsikon sisältämällä kotiosoitteella ennen paketin siirtämistä ylemmälle protokollakerrokselle.

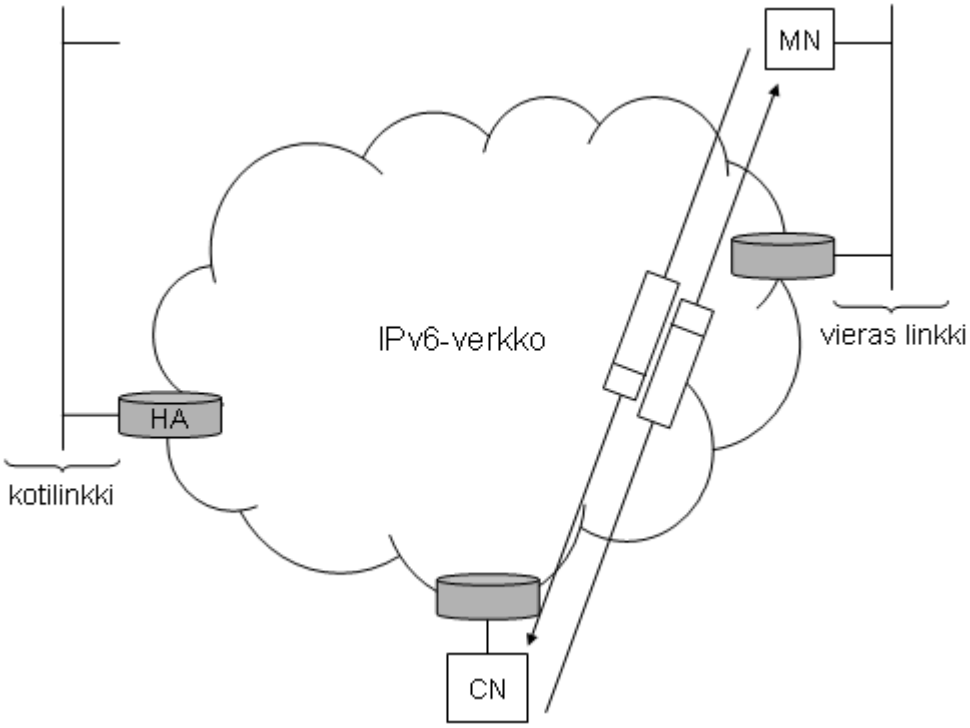
Vastaavasti liikkuvan laitteen lähettäessä vertaislaitteelle paketteja se lisää pakettiin kotiosoiteoption, joka sisältää laitteen kotiosoitteen. Paketin lähdeosoitteeksi asetetaan care-of-osoite ja kohdeosoitteeksi vertaislaitteen osoite. Näin paketti kulkee suoraan vertaislaitteelle, joka korvaa paketin lähdeosoitteen kotiosoiteoption osoitteella ennen paketin välitystä ylemmälle kerrokselle.

Tällä menetelmällä paketit kulkevat suoraan laitteiden välillä (kuva 28) ja ylemmän kerroksen protokollien näkökulmasta näyttää kuitenkin siltä kuin liikkuva laite olisi koko ajan kiinteästi kotiverkossaan. Käyttämällä laitteiden välisessä liikenteessä erillisiä laajennusotsikoita tunneloinnin sijasta saadaan pakettien otsikoista lisäksi pienempiä ja näin vältytään neljännen IPv6-osoitteen aiheuttamalta ylimääräiseltä kuormalta.

Vaikka reitinoptimointi vaatii jonkin verran jonkin verran lisätoimintoja vertaislaitteilta ja lisää signalointiviestien määrää, ovat sillä saavutetut edut suorituskyvyssä huomattavasti merkittävämpiä:

- kotiverkko kuormittuu paljon vähemmän, koska liikkuvien laitteiden liikenne ei kulje sen kautta
- kotiagentin prosessointikuorma vähenee, jolloin se voi palvella useampia liikkuvia laitteita vähemmillä resursseilla
- koko Internetin kuormitus on pienempi, millä on merkitystä etenkin liikkuvien laitteiden määrän kasvaessa tulevaisuudessa
- liikkuvan laitteen ja vertaislaitteen välisen liikenteen viive ja jitter pienenee, koska reitti on lyhyempi ja sisältää vähemmän mahdollisia ruuhkapisteitä

- parempi sietokyky verkon osittumiselle ja ruuhkautumiselle



Kuva 28. Pakettien välitys reitinoptimoinnilla

Ennen sidoksen elinajan loppumista vertaislaite voi lähettää liikkuvalle laitteelle pyynnön virkistää sidos, jos se katsoo, että sidos on edelleen aktiivisessa käytössä eli laitteiden välillä on vielä esimerkiksi avoimia TCP-yhteyksiä. Liikkuvan laitteen vastaanottaessa pyynnön, se voi virkistää sidoksen lähettämällä sidospäivitysviestin pyynnön lähettäneelle laitteelle. Näin vältytään palaamasta heikomman suorituskyvyn tarjoavaan käänteistunnelointiin.

Aina liikkuvan laitteen siirtyessä uudelle vieraalle linkille, se etsii uuden oletusreitittimen, muodostaa uuden care-of-osoitteen ja rekisteröi sidoksen kotiagentille sekä mahdollisille vertaislaitteille, joiden kanssa on käytössä reitinoptimointi. Laitteet, joille sidospäivitysviesti pitää lähettää, selviää sidospäivityslistasta.

Liikkuvan laitteen palattua kotiverkkoon se lähettää kotiagentille ja sidospäivityslistalla oleville vertaislaitteille sidospäivitysviestin, joka poistaa laitteen sidoksen sidosvälimuisteista. Tämä tapahtuu asettamalla viestin sisältämä sidoksen elinaika nollaksi ja care-of-osoite kotiosoitteeksi. Vastaanotettuaan kuittauksen kotiagentilta, laitteen on vielä lähetettävä ryhmälähetyksenä kotilinkille Neighbor Advertisement -sanoma, joka liittää laitteen kotiosoitteen sen linkkikerroksen osoitteeseen. Tämän jälkeen kotiagentti lopettaa pakettien kaappaamisen ja reititys palaa jälleen normaaliksi eikä Mobile IPv6:n toimintoja enää käytetä.

3.5.3 Liikkuvan laitteen automaattinen konfigurointi

Käyttääkseen hyväksi Mobile IPv6:n toimintoja pitää liikkuvan laitteen tietää kotiagenttinsa osoite. Se voidaan joko konfiguroida käsin pysyvästi laitteen muistiin tai käyttää dynaamista kotiagentin osoitteenetsintää (DHAAD) laitteen siirryttyä vieraaseen verkkoon. DHAAD:tä varten on määritelty kaksi ICMPv6-protokollan viestityyppiä, jotka esiteltiin edellä. Lähettämällä ICMP Home Agent Address Discovery Request -viestin kotilinkin kotiagenttien anycast-osoitteeseen, liikkuva laite voi pyytää jotakin kotilinkillä olevaa kotiagenttia lähettämään sille listan käytettävissä olevien kotiagenttien osoitteista. Anycast-osoitteen muodostamiseen liikkuva laite tarvitsee kotilinkin verkkotunnisteen. Kotiagentit keräävät koko ajan kotiagenttilistaansa tietoja samalla linkillä toimivista kotiagenteista seuraamalla reitittimien lähettämiä mainosviestejä. Jos linkillä on useita kotiagentteja, voidaan niiden välillä suorittaa kuormanjakoa asettamalla kotiagenteille eri preferenssiarvot, joita voidaan muuttaa dynaamisesti kuormituksen muuttuessa. Kun jokin kotilinkin kotiagenteista vastaanottaa liikkuvan laitteen lähettämän pyynnön, se muodostaa listan kotiagenttien osoitteista suosituimmuusjärjestyksessä ja lähettää sen liikkuvalle laitteelle ICMP Home Agent Address Discovery Reply -viestillä. Liikkuva laite valitsee listasta ensimmäisen kotiagentin ja yrittää lähettää sidospäivitysviestinsä sille. Jos rekisteröinti ei onnistu, kokeillaan seuraavaa osoitetta.

Kotiagentin osoitteen lisäksi liikkuvan laitteen pitää luonnollisesti tietää oma kotiosoitteensa. Koska kotiosoite on riippuvainen kotilinkin verkkotunnisteesta ja on voimassa vain määrätyn ajan, tulee liikkuvan laitteen olla tietoinen mahdollisista muutoksista sen kotilinkillä käytettäviin verkkotunnisteisiin. Normaalisti IPv6:ssa käytetään Neighbor Discovery -protokollaa näiden muutosten seuraamiseen, mutta sitä ei voida käyttää kun laite on poissa kotilinkiltä. Jos esimerkiksi liikkuvan laitteen kotiosoitteessaan käyttämä verkkotunniste muuttuu jostain syystä, täytyy sen saada tästä tieto ja päivittää vastaavasti kotiosoitteensa sekä mahdolliset rekisteröidyt sidoksensa. Tämän tiedon ylläpitoa varten Mobile IPv6:ssa on määritelty ICMP Mobile Prefix Solicitation ja ICMP Mobile Prefix Advertisement -viestit, joilla liikkuva laite voi pyytää ja vastaavasti kotiagentti mainostaa tietoja kotilinkin verkkotunnisteista. Kotiagentin lähettämä mainos voi sisältää yhden tai useampia verkkotunnisteoptioita.

3.6 Tietoturva

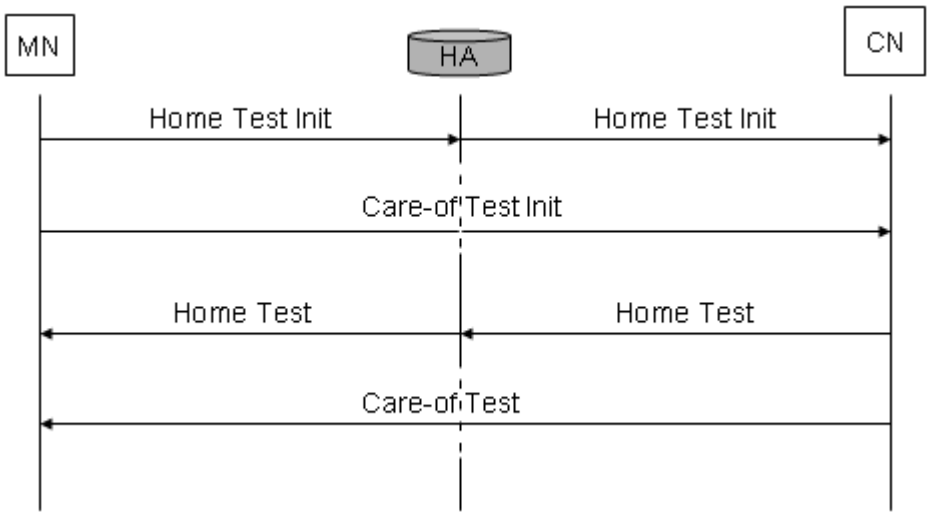
Jotta vältyttäisiin mahdollisilta hyökkäyksiltä Mobile IPv6 -protokollan toimintaa kohtaan, täytyy liikkuvuudenhallintaan käytettävät signalointiviestit pystyä autentikoimaan. Jos näin ei tehdä, on hyökkääjän helppoa suorittaa esimerkiksi etäuudelleenohjaushyökkäys, mikä tarkoittaa, että liikkuvan laitteen liikenne ohjataan haluttuun osoitteeseen. Tällöin hyökkääjä voi lukea ja muokata liikkuvalle laitteelle osoitettuja paketteja halutulla tavalla ilman, että liikkuva laite tai vertaislaite edes välttämättä huomaa sitä. Lisäksi on olemassa monia muita hyökkäysmalleja kuten erilaiset palvelunestohyökkäykset. Edellä mainituista syistä johtuen liikkuvuudenhallintamekanismien tärkeimpiä vaatimuksia ovat riittävän turvatason takaavat ja toimiviksi osoitetut tieturvaominaisuudet. Mobile IPv6 käyttää kahta menetelmää viestien todentamisessa. Liikkuvan laitteen ja kotiagentin välisessä viestinnässä hyödynnetään standardoitua IP Security -protokollaa (IPsec) [48], kun taas liikkuvan laitteen ja vertaislaitteen välillä käytetään erityisesti MIPv6:tta varten suunniteltua Return Routability -mekanismia. Mobile IPv6:n tietoturvan suunnitteluperiaatteena on ollut, että tietoturvan tasoa ei heikennetä siitä, mitä se olisi jos laite olisi kiinteästi kotiverkossaan.

Oletusarvoisesti signalointiviestien suojaamiseen liikkuvan laitteen ja kotiagentin välillä käytetään IPsecin Encapsulating Security Payload -otsikkoa (ESP) [49] kuljetusmoodissa, mutta myös Authentication Header -otsikkoa (AH) [50] voidaan vaihtoehtoisesti käyttää. Salausavaimet voidaan määritellä joko manuaalisesti tai käyttää jotakin automaattista avaintenhallintaprotokollaa (esimerkiksi IKE [51]). Sidospäivitysviestien ja kuittausten lisäksi verkkotunnistetietojen ylläpitoon liittyvät ICMPv6-viestit pitää suojata vastaavasti IPsecillä. Haluttaessa IPseciä voidaan käyttää myös kotiagentin ja liikkuvan laitteen välisessä tunnelissa kulkevien datapakettien todentamiseen. IPsecin käytön yksityiskohtia Mobile IPv6:n kanssa käydään läpi RFC:ssä 3776 [52].

Return Routability -mekanismilla varmistetaan, että liikkuva laite on tavoitettavissa sekä kotiosoitteensa että care-of-osoitteensa kautta. Lisäksi sen avulla muodostetaan sidostenhallinta-avain, jota käytetään signaloinnin todentamisessa. Return Routability suoritetaan aina ennen kuin liikkuva laite voi lähettää uudelle vertaislaitteelle sidospäivitysviestin. Liikkuva laite aloittaa prosessin lähettämällä Home Test Init ja Care-of Test Init -viestit vertaislaitteelle. Näistä ensimmäinen lähetetään

kotiagentin kautta käyttämällä tunnelia kuten mikä tahansa datapaketti. Jälkimmäinen sanoma taas lähetetään suoraan vertaislaitteelle käyttämällä lähdeosoitteena care-of-osoitetta. Vertaislaitteen vastaanottaessa viestit se muodostaa salausavaimen rakentamiseen tarvittavat kaksi polettia (Home Keygen Token ja Care-of Keygen Token) ja lähettää nämä vastaavasti Home Test ja Care-of Test -viesteillä liikkuvalle laitteelle. Viestienvaihto on esitetty kuvassa 29. Liikkuvan laitteen ja kotiagentin välillä kulkevat Home Test Init ja Home Test -viestit suojataan IPsecillä.

Kun koko viestintä on käyty läpi ja liikkuva laite on muodostanut vastaanottamiensa polettien avulla sidostenhallinta-avaimen, se voi viimein lähettää sidospäivitysviestinsä vertaislaitteelle ja suojata viestin avaimellisella tiivistysfunktiolla. Viestin todentamiseen käytettävä tiiviste sijoitetaan Binding Authorization Data -optioon. Vertaislaite käyttää viestin sisältämän Nonce Indices -option tietoja hyväksi muodostaakseen liikkuvan laitteen käyttämän avaimen, jolla se todentaa viestin. Aina kun liikkuvan laitteen kotisoite tai care-of-osoite muuttuu, joudutaan Return Routability suorittamaan uudelleen. Avaimella on myös määrätty elinikä, jonka jälkeen se on uusittava. Return Routability -mekanismin suunnitteluperusteita ja toimintaperiaatteita on kirjattu IETF:n luonnokseen [53].



Kuva 29. Return Routability -mekanismin viestintä

Reitinoptimointiin liittyy myös yksityisyyttä koskeva ongelma, sillä sen käyttö paljastaa yhteyden toiselle osapuolelle liikkuvan laitteen topologisen sijainnin, jonka perusteella voidaan päätellä myös laitteen käyttäjän fyysinen sijainti tietyllä tarkkuudella. Tämä saattaa joissain tapauksissa olla käyttäjän kannalta ei-toivottu ominaisuus.

Edellä esitettyjen suositeltujen tietoturvamekanismien lisäksi IETF:ssä on ehdotettu myös vaihtoehtoisia tapoja signalointiviestien todentamiseen. Return Routabilityn sijaan on esitetty käytettäväksi ennalta jaettuja avaimia liikkuvan laitteen ja vertaislaitteen välisten viestien autentikointiin [54]. Viestien suojaus tapahtuisi samalla tavalla kuin edellä esitettiin, mutta Return Routability -mekanismin mukaista viestintää ei suoriteta, koska molemmilla laitteilla on jo tarvittavat avaimet. Lisäksi sidospäivitysviesteissä ei käytettäisi Nonce Indices -optiota. Tällä vältyttäisiin neljän sanoman vaihtamiselta ja näin nopeutettaisiin reitinoptimoinnin käyttöönottoa. Toinen ehdotus [55] taas esittää kevyempää ja yksinkertaisempaa vaihtoehtoa IPsecin rinnalle liikkuvan laitteen ja kotiagentin välisten sidospäivitysviestien ja kuittausten suojaamiseen. Tämä toteutettaisiin jaetulla tietoturva-assosiaatiolla ja uusilla liikkuvuusotsikon optioilla. Nämä menetelmät ovat kuitenkin vasta luonnosvaiheessa ja kehitystyö niiden osalta jatkuu.

3.7 Tulevat laajennukset

Mobile IPv6:lle on jo suunniteltu joitakin laajennuksia, joilla protokollan toimintaa voitaisiin tulevaisuudessa tehostaa. On esimerkiksi esitetty, että myös hyötykuormaa voitaisiin lähettää samoissa paketeissa sidosten hallintaan käytettyjen signalointiviestien kanssa ns. reppuselässä (piggybacking). Tämä on mahdollista, koska liikkuvuusotsikko on määritelty IPv6-laajennusotsikoksi, jota voi seurata hyötykuorma. Tällä tavalla lähetettävien IPv6-otsikoiden määrää saataisiin hieman vähennettyä. Ennen menetelmän käyttöönottoa täytyy kuitenkin ratkaista joitakin sen käyttöön liittyviä ongelmia kuten esimerkiksi yhteistoiminta IPsecin kanssa. Tulevat laajennukset saattavat mahdollista myös ns. kolmioreitityksen, jota käytetään Mobile IPv4:ssä. Lisäksi ollaan tutkimassa mahdollisuutta muodostaa kotiosoite dynaamisesti ilman, että jokaista osoitetta varten tarvittaisiin oma ennalta sovittu tietoturva-assosiaatio.

Kuten tämän luvun alkupuolella todettiin, on IETF:n mipshop-työryhmä kehittämässä kahta erilaista menetelmää, joilla Mobile IPv6:n yhteydenvaihtoja voidaan optimoida. Yhteydenvaihtoon kuluva aika saattaa olla hyvinkin huomattava. Se muodostuu karkeasti seuraavista osista: linkkikerroksen yhteydenvaihto, liikkumisen havaitseminen verkkokerroksella, uuden oletusreitittimen etsiminen, care-of-osoitteen konfigurointi ja kotiagentin sekä vertaislaitteiden sidosten päivittäminen. Koska useimmat linkkikerroksen tekniikat IEEE 802.11 mukaan lukien eivät salli, että laite on yhtäaikaisesti liittyneenä kahteen eri aliverkkoon, menetetään kaikki yhteydenvaihdon

aikana vanhaan care-of-osoitteeseen lähetetyt ja matkalla olleet paketit siitä lähtien kun vanhalta linkiltä irtaudutaan kunnes koko yhteydenvaihto ja Mobile IPv6:n rekisteröinnit on suoritettu, minkä jälkeen paketteja voidaan jälleen lähettää ja vastaanottaa. Mipshopin ehdottamat laajennukset yhteydenvaihtojen suorituskyvyn parantamiseksi ovat:

- Hierarkkinen Mobile IPv6 [29] on mekanismi, jolla pyritään vähentämään Mobile IPv6:n signaloinnin aiheuttamaa kuormaa ja nopeuttamaan sidospäivityksiä. Sen toiminta perustuu liikkuvuudenankkurointipisteisiin (Mobility Anchor Point, MAP), jotka ovat vierailtavissa verkoissa sijaitsevia reitittimiä. MAP toimii hieman kuten paikallinen kotiagentti, joka mahdollistaa liikkuvuudenhallinnan paikallisesti MAPin verkkoalueella. Liikkuva laite suorittaa uudelle verkkoalueelle siirryttyään sidoksen rekisteröinnin myös MAPille oman kotiagenttinsa lisäksi. Niin kauan kuin liikkuva laite sijaitsee saman MAPin verkkoalueella, ei sen tarvitse liikkuessaan lähettää sidospäivitysviestejä kuin MAPille. Näin Internetin kautta kotiagentille ja vertaislaitteille lähetettävien signalointiviestien määrä vähenee ja sidospäivitykset nopeutuvat, koska MAP on lähempänä liikkuvaa laitetta kuin kotiagentti.
- Nopeat yhteydenvaihdot Mobile IPv6:lle (FMIPv6) [30] pyrkii nimensä mukaisesti lyhentämään yhteydenvaihtoon kuluvaa aikaa ja vähentämään yhteydenvaihdoista johtuvaa pakettihävikkiä. Tämä on toteutettu konfiguroimalla uuden linkin tiedot kuten verkkotunniste ennakkoon laitteen vielä ollessa vanhalla linkillä. Lisäksi FMIPv6:n avulla on mahdollista ohjata vanhaan care-of-osoitteeseen lähetetyt paketit uuteen care-of-osoitteeseen yhteydenvaihdon ollessa käynnissä. Myös menetelmän toteuttamista erityisesti IEEE 802.11 -verkoissa on selvitetty mipshop-työryhmässä [56].

Näitä laajennuksia voidaan käyttää joko yhdessä tai erikseen.

3.8 Erot Mobile IPv4:ään

Mobile IPv6:n suunnittelussa on pystytty hyödyntämään Mobile IPv4:stä saatuja kokemuksia sekä IPv6:n tuomia uusia toimintoja. Täten MIPv6:n toimintaa on kyetty kehittämään pidemmälle ja se tarjoaakin useita parannuksia verrattuna Mobile IPv4:ään.

Seuraavassa on lueteltu näiden IP-protokollan eri versioille tarkoitettujen liikkuvuudenhallintamekanismien välisiä eroja:

- Koska Mobile IP:tä hyödyntävät liikkuvat laitteet käyttävät kaksi IP-osoitetta, tarjoaa IPv6 suuremman osoiteavaruutensa takia paremmat toimintaedellytykset.
- MIPv6:ssa ei tarvita erityisiä liikkuvuutta tukevia laitteita vierailtavaan verkkoon kuten MIPv4:n vierasagentti. Myöskään DHCP-palvelimia ei tarvita, jos käytetään tilatonta osoitteen automaattista konfigurointia.
- MIPv6:ssa reitinoptimointi on osa perusprotokollaa kun taas Mobile IPv4:ssä reittioptimointi on erillinen laajennus, joka on jäänyt luonnosvaiheeseen.
- Reitinoptimointia voidaan Mobile IPv6:ssa käyttää turvallisesti vaikka ennalta ei olisikaan muodostettu tietoturva-assosiaatioita laitteiden välille eikä se aseta vertaislaitteen toiminnoille suuria lisävaatimuksia, mikä mahdollistaa reitinoptimoinnin käytön mahdollisimman monen vertaislaitteen kanssa.
- Liikkuvan laitteen ollessa poissa kotiverkosta suurin osa datapaketeista lähetetään MIPv6:ssa käyttämällä uusia IPv6-laajennusotsikoita eikä tunnelointia ja näin saadaan pienennettyä otsikoiden kokoa verrattuna Mobile IPv4:ään.
- MIPv6:ssa ingress-suodatus ei ole este protokollan toiminnalle, mutta MIPv4:ssä se saattaa aiheuttaa ongelmia.
- Mobile IPv6 ei ole riippuvainen mistään tietystä linkkikerroksesta, koska se hyödyntää IPv6 Neighbor Discoveryä IPv4:n ARPin sijaan.
- IPv6:n anycast-lähetyksiä hyödyntävä DHAAD palauttaa liikkuvalle laitteelle vain yhden vastauksen, kun Mobile IPv4:ssä käytetty suunnattu yleislähetys palauttaa vastauspaketin jokaiselta kotiverkon kotiagentilta. Lisäksi nykyisen suosituksen mukaan reitittimet eivät välitä suunnattuja yleislähetyksiä [57].

4 Simulaatiot

Työn simulaatio-osuudessa selvitettiin ensin edellä esitettyjen IEEE 802.11 ja Mobile IPv6 -tekniikoiden simulointimahdollisuuksia ns-2 [7] verkkosimulaattorilla. Koska simulaattorin perusversio ei sisältänyt kaikkia tarvittavia simulaatiomalleja, jouduttiin siihen tekemään joitakin laajennuksia ja muutoksia. Tämän jälkeen muodostettiin muutamia simulaatioskenaarioita, joilla tutkittiin tässä työssä käsiteltyjen teknologioiden toimintaa ja ominaisuuksia.

Tässä luvussa esitellään ensin käytetty simulaatioympäristö ja simulaattoriksi valittu ns-2 sekä sen ominaisuudet. Myös ns-2:n käyttöä kuvataan lyhyesti. Seuraavaksi kerrotaan simulaattorin vaatimista laajennuksista ja muutoksista, joita simulaatiomalliin tehtiin. Lopuksi esitellään suoritetut simulaatiot ja niiden tulokset.

4.1 Simulointiympäristö

Ns-2 toimii Unix ja Linux ympäristöissä sekä myös Windowsissa Cygwin-emulaattorin avulla [58]. Tässä työssä suoritetut simulaatiot ajettiin tavallisella PC-tietokoneella, jonka käyttöjärjestelmänä toimi Debian GNU/Linux sarge [59] Linux-ytimen versiolla 2.4.28. Simulaattoriksi valittiin ns-2, koska se on yleisesti käytetty lukuisissa verkkotekniikkaa käsittelevissä tutkimuksissa ja julkaisuissa. Ns-2:n suuren suosion eräs merkittävimmistä tekijöistä lienee se, että ohjelma on ilmainen. Sen eduksi kaupallisiin vaihtoehtoihin verrattuna voidaan lukea myös vapaasti saatavissa oleva lähdekoodi, mikä mahdollistaa simulaattorin toiminnan muokkaamisen halutulla tavalla. Muita vastaavia simulaattoreita ovat esimerkiksi OPNET Modeler [60], GloMoSim [61] ja OMNeT++ [62], joista ensin mainittu on kaupallinen tuote ja kaksi jälkimmäistä ovat ilmaisia akateemisessa käytössä.

4.1.1 Ns-2

Ns-2 on diskreetti tapahtumapohjainen verkkosimulaattori, joka tarjoaa mahdollisuuden useiden eri verkkotekniikoiden ja protokollien simulointiin. Tapahtumasimulaattorin toiminta perustuu skeduleriin ja skedulointilistaan, joka sisältää kaikki simulaation tapahtumat kronologisessa järjestyksessä sekä niiden keston. Simulaatioajon aikana skeduleri käy listaa läpi ja suorittaa tapahtumien mukaiset toiminnot tuottaen tarvittaessa uusia tapahtumia listalle. Ns-2 pohjautuu REAL-simulaattoriin [63] ja sen kehittämistä on rahoittanut Yhdysvaltain puolustusministeriön alainen DARPA erilaisten projektien kautta. Se on toteutettu kahdella ohjelmointikielellä: C++ ja OTcl (MIT Object Tool Command Language) [64]. Simulaattorin alemman tason toiminnot kuten tapahtumien ja pakettien käsittelyn hoitava ydin on tehty C++-kielellä sen tehokkuuden takia. Ylemmän tason toimintoihin sekä simulaatioskenaarioiden kuvaukseen ja hallintaan käytetään joustavampaa OTcl-kieltä, joka on oliopohjainen versio Tcl-skriptikielestä.

Avoimen lähdekoodin projektina ns-2 ja sen lähdekoodi on saatavana vapaasti Internetistä. Avoimuutensa ja modulaarisuutensa takia ns-2 on laajennettavissa ja siihen löytyykin Internetistä useita käyttäjien ja tutkijoiden tekemiä laajennuksia. Kahden kielen toteutus tosin hankaloittaa ja monimutkaistaa laajennusten toteuttamista, koska on hallittava molemmat kielet ja eri kielillä toteutettujen osien välinen rajapinta on määriteltävä tarkasti. Myös mahdollisien ohjelmavirheiden etsiminen ja korjaaminen hankaloituu kaksikielisen toteutuksen takia.

Avoimilla projekteilla on myös omat heikot puolensa. Simulaattorin sisältämien simulaatiomallien ja sitä kautta sen antamien tuloksien todenmukaisuudesta ei esimerkiksi anneta minkäänlaisia takuita. Eräs suurimmista ongelmista on heikosti ylläpidetty dokumentaatio [65], joka ei ole kaikilta osiltaan aivan täydellinen ja kaikista simulaatiomallien ominaisuuksista tai käytöstä ei ole olemassa tarkkoja kuvauksia. Tämän takia jouduttiin tässä työssä käytettävien simulaatiomallien toteutusta ja konfigurointia selvittämään lukuisilla erilaisilla testisimulaatioilla sekä simulaattorin lähdekoodia lukemalla. Dokumentaation vajanaisuutta ja käyttäjätuen puutetta voidaankin pitää tällaisen avoimen projektin heikoimpana puolena.

Pyrittäessä parhaaseen mahdolliseen tulokseen pitäisi tarvittavat simulaatiomallit suunnitella ja rakentaa uudelleen alusta alkaen ja hyödyntää ns-2:sta vain sen ydintoiminnot. Tällöin voitaisiin varmistua mallin sopivuudesta juuri omiin

käyttötarkoituksiin. Erilaisia protokollia ja tekniikoita mallintavien simulaatiomallien rakentaminen alusta lähtien on kuitenkin varsin mittava projekti eikä siihen tässä työssä ollut mahdollisuuksia, joten päädyttiin selvittämään millaisia olemassa olevia simulaatiomalleja ns-2:lle on olemassa ja soveltamaan ja muokkaamaan niitä mahdollisuuksien mukaan.

Simulointi ns-2:lla tapahtuu siten, että suoritettavat simulaatioskenaariot kuvataan ensin OTcl-kielellä tiedostoon, joka määrittelee muun muassa simuloitavan verkon elementit ja topologian, mobiililaitteiden liikkumisen sekä verkossa kulkevan liikenteen. Tämän jälkeen tiedostot ajetaan simulaattorilla. Simulaatioajon tuloksena saadaan ns. trace-tiedosto, joka esittää kronologisessa järjestyksessä kaikki simulaation aikana tapahtuneet tapahtumat kuten pakettien lähetykset ja vastaanotot sekä mobiililaitteiden liikkumisen. Langallisen ja langattoman verkon solmujen eroista johtuen myös niiden trace-tiedoissa käytetyt formaatit ovat erilaiset. Lisäksi langattomasta trace-formaatista on olemassa kaksi vaihtoehtoista versiota. Tämä hankaloittaa tiedostojen lukemista ja prosessointia. Sopivia työkaluja (esimerkiksi awk, Perl ja gnuplot) sekä niille rakennettuja skriptejä hyödyntäen voidaan trace-tiedostojen perusteella laskea erilaisia simulaatioverkon sekä käytettyjen protokollien suorituskykyä kuvaavia ominaisuuksia. Itse ns-2:n mukana minkäänlaisia simulaatioiden analysointityökaluja ei tule.

Simulaatioita voidaan visualisoida simulointiajon jälkeen ns-2:n mukana tulevalla Network Animatorilla (Nam), joka ei kuitenkaan vielä tue täydellisesti sekä kiinteitä että langattomia yhteyksiä samanaikaisesti sisältäviä simulaatioita. Tällä hetkellä ohjelmaa voi käyttää vain lähinnä solmujen liikkumisen ja liikenteen havainnollistamiseen. Keskeneräisyydestä johtuen Namista ei ole juurikaan hyötyä eikä sitä käytetä tämän työn simulaatioissa.

Alun perin ns-2 suunniteltiin kiinteiden lankaverkkojen simulointiin, mutta siihen on myöhemmin lisätty langattomien verkkojen simulointiin tarvittavia simulaatiomalleja. Langattomien lähiverkkojen malli on syntynyt osana Monarch-projektia [66] ja se sisältää IEEE 802.11 -standardin mukaisen MAC-kerroksen, josta on tosin toteutettu vain DCF-pääsymekanismi. Myös RTS/CTS-menetelmä sisältyy malliin. Fyysisen kerroksen kolmesta vaihtoehdosta on mallinnettu DSSS, jonka tarjoamista siirtonopeuksista tässä työssä käytetään nopeutta 2 Mbps. 802.11-standardin palveluista on toteutettu vain kehysten välittämiseen tarvittavat palvelut ja esimerkiksi assosiointi- ja autentikointipalveluita ei mallissa ole. Simulaatiomalli on tarkoitettu ad

hoc -verkoissa käytettyjen reititysprotokollien simulointiin eikä se siten tue myöskään infrastruktuuri-arkkitehtuuria.

Tämän työn simulaatioissa käytetty ns-2:n radiokanavamalli on hyvin yksinkertainen: lähietäisyyksillä käytetään Friisin vapaan tilan mallia pelkällä suoralla signaalilla ja pitemmillä etäisyyksillä kaksitie-etenemistä, jossa otetaan huomioon sekä suoraan kulkeva että maan kautta heijastuva signaali. Käytännössä siis vastaanotetun signaalin voimakkuuteen vaikuttaa vain lähettimen ja vastaanottimen välinen etäisyys. Tämän työn simulaatioissa WLAN-asemien kantamaksi asetettiin 100 metriä. Koska käytetyt antennit säteilevät tasaisesti joka suuntaan, pystyvät kaikki liityntäpisteestä 100 metrin säteellä olevat asemat liikennöimään liityntäpisteen kanssa.

Simulaattorin langattomia yhteyksiä käyttävät liikkuvat laitteet eivät osaa vaihtaa automaattisesti kanavalta toiselle, minkä takia kaikki simulaatioiden asemat on asetettava käyttämään yhtä ja samaa kanavaa. Kun lisäksi assosiointipalvelut puuttuvat, voi kahden eri liityntäpisteen peittoalueella oleva asema viestiä kummankin liityntäpisteen kanssa samanaikaisesti. Koska tällainen toiminta ei ole 802.11-standardin mukaista, estettiin se sijoittamalla liityntäpisteet simulaatioissa niin, etteivät niiden peittoalueet leikkaa toisiaan.

Ns-2:n perusjakeluversio sisältää vain Sun Microsystemsin kehittämän Mobile IPv4:n simulaatiomallin, joten Mobile IPv6 -simulaatioita varten ns-2:een joudutaan tekemään muutoksia.

4.1.2 MobiWan

MobiWan [67] on Thierry Ernstin Motorolalle tekemä ns-2:n laajennus, jonka avulla voidaan tutkia liikkuvuutta alueverkoissa (Wide Area Network, WAN). MobiWanin liikkuvuudenhallinta on toteutettu Mobile IPv6 -protokollalla ja sen simulaatiomallia hyödynnetään tässä työssä. MIPv6-mallin lisäksi MobiWan sisältää IPv6-laajennuksen sekä työkaluja, joilla voidaan luoda ja konfiguroida laajoja simulaatioverkkoja. Näitä työkaluja ei kuitenkaan käytetty tässä työssä. MobiWanin sisältämät IPv6- ja MIPv6-mallit on tarkoitettu lähinnä liikkuvuudenhallinnan perustoiminnan simulointiin eivätkä siten mallinna protokollien kaikkia ominaisuuksia. Mallista on jätetty pois esimerkiksi IPv6 Neighbor Discovery, IPsec sekä MIPv6:sta liikkuvan laitteen automaattiseen konfigurointiin liittyvät toiminnot ja Return Routability -mekanismi. Liikkumisen seurantaa varten on toteutettu reitittimien mainosviestit, joiden lisäksi liikkuvat laitteet voivat lähettää reititinkyselyitä uutta

oletusreititintä etsiessään. Kuten edellä todettiin, tukee ns-2 vain ad hoc -verkkoarkkitehtuuria. Tämän vuoksi MobiWan sisältää myös ominaisuuden, jolla ad hoc -reititys voidaan kiertää. MobiWan toimii ainoastaan ns-2:n versiossa 2.1b6, joten sitä käytettiin kaikissa simulaatioissa.

4.1.3 Muutokset simulaatiomalliin

Koska MobiWanin Mobile IPv6 -simulaatiomalli perustuu vanhaan protokollan luonnokseen vuodelta 2000, tehtiin malliin muutoksia, joiden jälkeen sen toiminta vastaa paremmin nykyistä Mobile IPv6 -spesifikaatiota. Lisäksi mallin toimintoja kehitettiin edelleen ja siihen lisättiin joitakin uusia ominaisuuksia. Olennaisimmat muutokset on esitelty seuraavassa:

- Malliin lisättiin käänteistunnelointitoiminnallisuus, jota käytetään pakettien reititykseen oletusarvoisesti. Alkuperäisessä MobiWanissa perusmenetelmänä oli kolmioreititys.
- Mobile IPv6:n signalointiin käyttämien sidospäivitys- ja sidoskuittausviestien koot päivitettiin.
- Ns-2:n mobiililaitteen mallin kiinteä osa on IPv4:n ARP-protokolla, mutta koska IPv6:ssa sitä ei käytetä, poistettiin se käytöstä.
- Sidospäivitysviesti lähetetään vertaislaitteelle heti, kun huomataan pakettien kulkevan tunnelin kautta. Alkuperäisessä mallissa lähetys tapahtui heikoimmassa tapauksessa vasta 10 sekunnin päästä, mikä ei ole Mobile IPv6:n määritelmän mukaista ja heikentää tiedonsiirron suorituskykyä.
- Liikkumisen seurantaa muutettiin siten, että uuden reitittimen mainoksen vastaanottaessaan liikkuva laite ei välittömästi suorita yhteydenvaihtoa vaan tekee sen vasta, kun se huomaa yhteyden oletusreitittimensä katkenneen. Tätä menettelyä suositellaan RFC:ssä 3775, koska siten vältytään tarpeettomilta yhteydenvaihdoilta. Toisaalta tämä saattaa hidastaa yhteydenvaihtoja ja pidentää katkoksia.
- Kotiosoiteoptio lisätään liikkuvan laitteen lähettämiin datapaketteihin laitteen ollessa vieraassa verkossa, jos reitinoptimointi on käytössä.
- Liityntäpisteet alkavat lähettämään reitinmainoksia heti simulaation alusta alkaen eikä vasta saatuaan ensimmäisen mainospyynnön.

- Mobile IPv6 -parametrit asetettiin seuraavasti: sidoksen elinaika 8 sekuntia ja päivitysväli 4 sekuntia. Oletusarvoisesti sekä elinaika että päivitysväli olivat samat, mikä aiheutti sidoksen vanhenemisen ennen kuin liikkuva laite ehti virkistää sen.

Edellisten lisäksi simulaattoriin tehtiin muutamia pienempiä muutoksia, jotka eivät vaikuta suoranaisesti protokollien toimintaan.

4.2 Simulaatioskenaariot

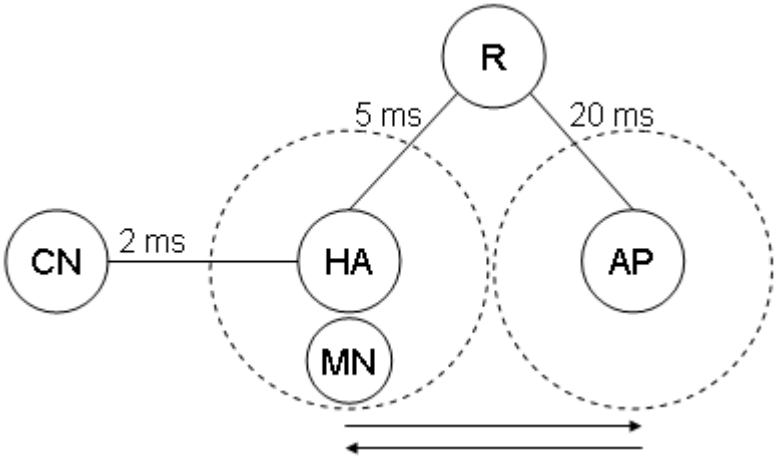
Simulaatioilla saavutettuihin tuloksiin on aina syytä suhtautua kriittisesti, koska niiden todenmukaisuus riippuu täysin käytetyn simulaatiomallin tarkkuudesta ja simulaattorin toteutuksesta. Seuraavia simulaatiotuloksia analysoitaessa on otettava huomioon, että simulaattorin antamat tulokset ovat todellisuuteen verrattuna melko optimistisia. Tämä johtuu pääasiassa siitä, että käytetyt simulaatiomallit ovat yksinkertaistettuja versioita IEEE 802.11 ja Mobile IPv6 -tekniikoiden määrittelyistä. Olennaisimpia puutteita ovat 802.11-standardin mukaiset hallintapalvelut, realistisempi radiokanavamalli, IPv6 Neighbor Discovery -protokolla ja jotkin MIPv6:n toiminnot kuten tietoturvamekanismit.

4.2.1 Reitinoptimointi

Ensimmäisessä simulaatiossa tutkittiin reitinoptimoinnilla saavutettavaa hyötyä verrattuna käänteistunnelointiin. Asiaa tutkittiin kahdessa eri tapauksessa: vertaislaitteen ollessa lähellä kotiagenttia ja vertaislaitteen ollessa lähellä vierasta verkkoa, jonne liikkuva laite siirtyy. Nämä kaksi tilannetta ovat ääritapauksia käänteistunneloinnin kannalta. Paras tilanne käänteistunnelointia käytettäessä on, kun vertaislaite on lähellä kotiverkkoa, koska tällöin paketit eivät tee ylimääräistä lenkkiä vaikka ne kulkevatkin kotiagentin kautta. Heikoin tilanne käänteistunneloinnin kannalta syntyy, jos vertaislaite on samassa verkossa, jonne liikkuva laite on siirtynyt. Tällöin liikenteen kiertäessä edestakaisen lenkin kotiagentin kautta viive kasvaa ja sitä kautta tiedonsiirron suorituskyky heikkenee.

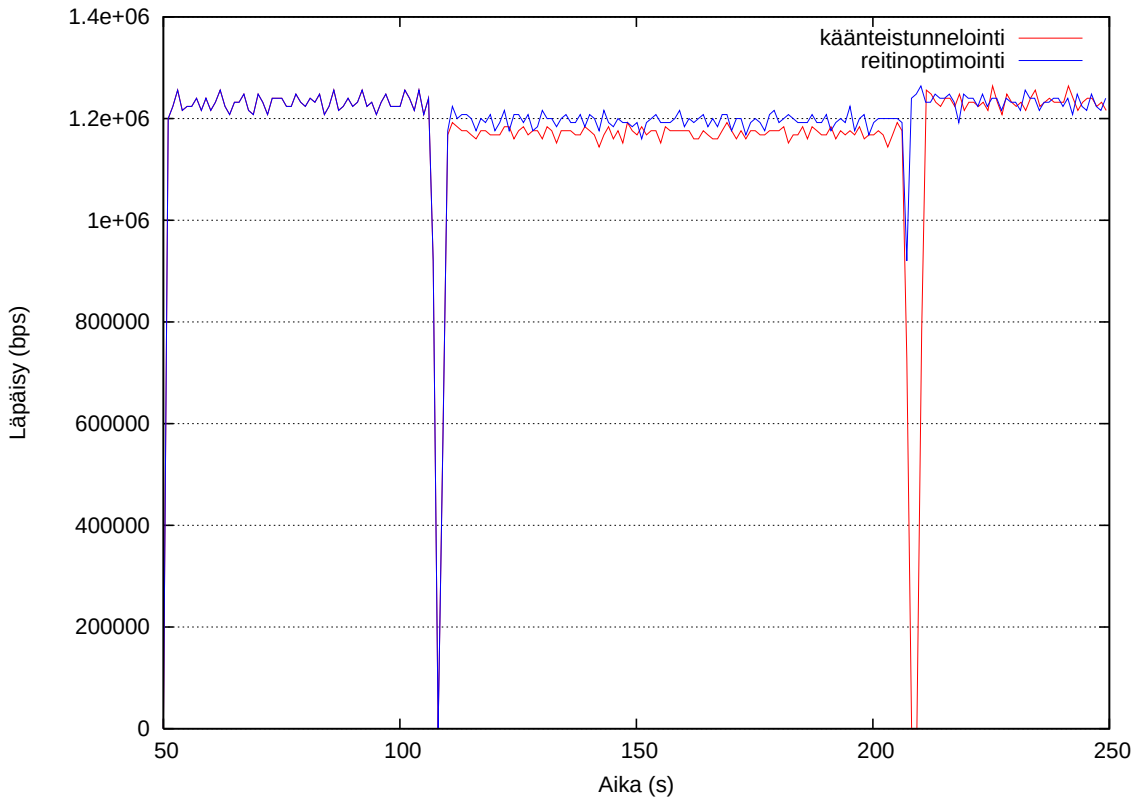
Ensin simuloitiin parasta tilannetta kuvan 30 kaltaisessa verkossa. Se sisältää kaksi WLAN-liityntäpistettä (AP), joista toinen toimii samalla kotiagenttina (HA). Kaikki ns-2:n liityntäpisteet sisältävät myös reitittimen ja ne toimivat siten alueellaan olevien liikkuvien laitteiden oletusreitittiminä. Liityntäpisteet on yhdistetty toisiinsa 5

Mbps linkeillä sekä reitittimellä (R). Vertaislaite (CN) on liitetty vastaavasti linkillä suoraan kotiagenttiin. Kaikkien linkkien viiveet on esitetty kuvassa. Simulaation alussa Liikkuva laite (MN) on kotiverkossaan ja lähtee ajassa 100 sekuntia liikkumaan kohti AP:tä nopeudella 14 m/s eli noin 50 km/h. Saavuttuaan perille MN on hetken paikoillaan, minkä jälkeen se palaa takaisin kotiverkkoonsa. MN alkaa ajassa 50 sekuntia ladata tiedostoa FTP:llä vertaislaitteelta. Simulaatiot ajettiin ensin käänteistunneloinnilla ja sitten reitinoptimointia käyttäen.



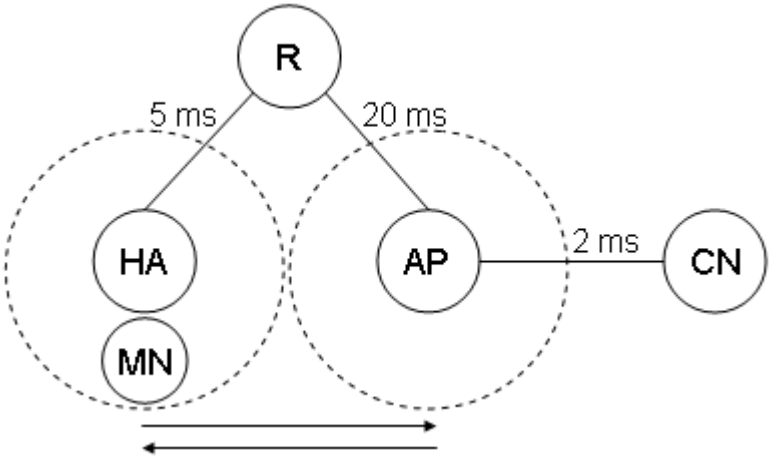
Kuva 30. Käänteistunneloinnin kannalta paras tilanne

Tiedonsiirron suorituskykyä mitattiin liikkuvan laitteen lataaman tiedoston siirtonopeudella. Kuvassa 31 on esitetty saavutetut nopeudet sekä käänteistunneloinnilla että reitinoptimoinnilla. Kuvaajista nähdään ensinnäkin selvästi kuinka liityntäpisteen vaihto aiheuttaa lyhyen katkoksen tiedonsiirtoon noin 107 ja 207 sekunnin kohdalla. Tässä tilanteessa siirtonopeudet liikkuvan laitteen ollessa vieraassa verkossa eivät juuri eroa eri reititysmenetelmien välillä. Tämä johtuu siitä, että paketit kulkevat molemmissa tapauksissa samaa reittiä. Pieni etu reitinoptimoinnin hyväksi syntyy IP-otsikoiden koossa olevan eron takia.



Kuva 31. Läpäisynopeudet parhaassa tilanteessa

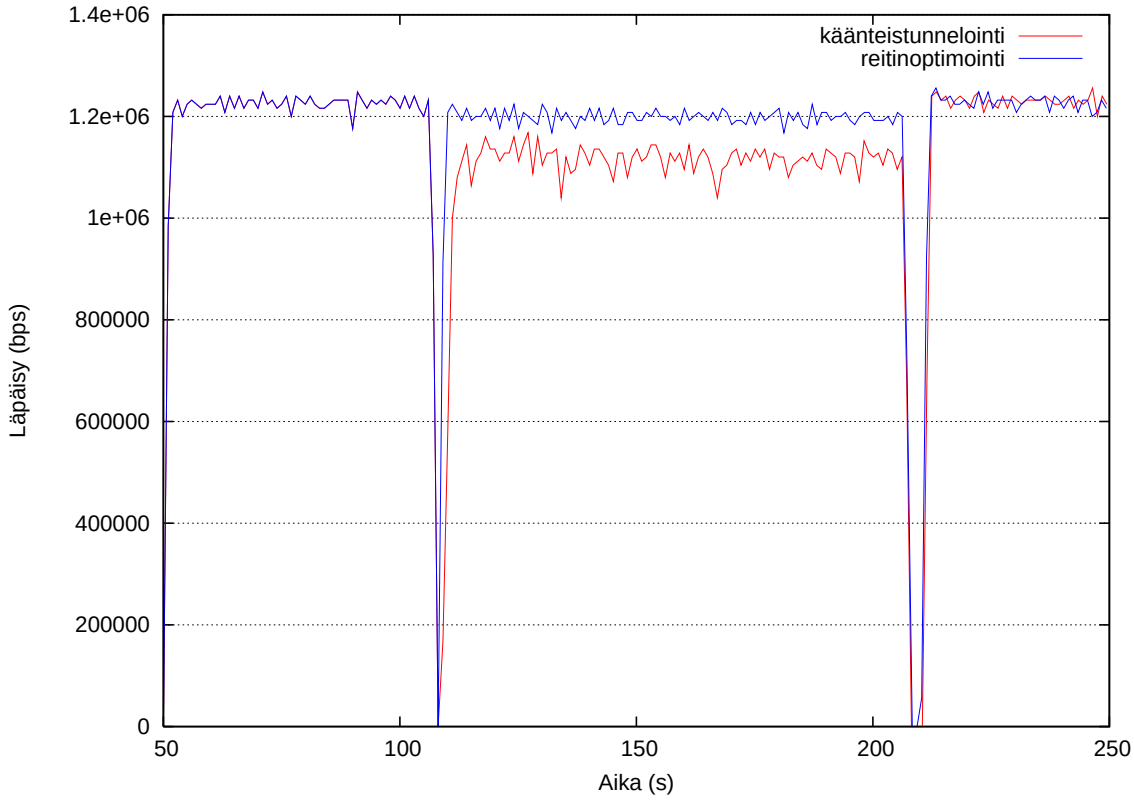
Seuraavaksi simuloitiin käänteistunneloinnin kannalta huonointa tilannetta (kuva 32), jossa ainoa muutos edelliseen skenaarioon on vertaislaitteen sijainti verkossa. Nyt vertaislaite on liitetty suoraan vierailtavan verkon liityntäpisteeseen.



Kuva 32. Käänteistunneloinnin kannalta huonoin tilanne

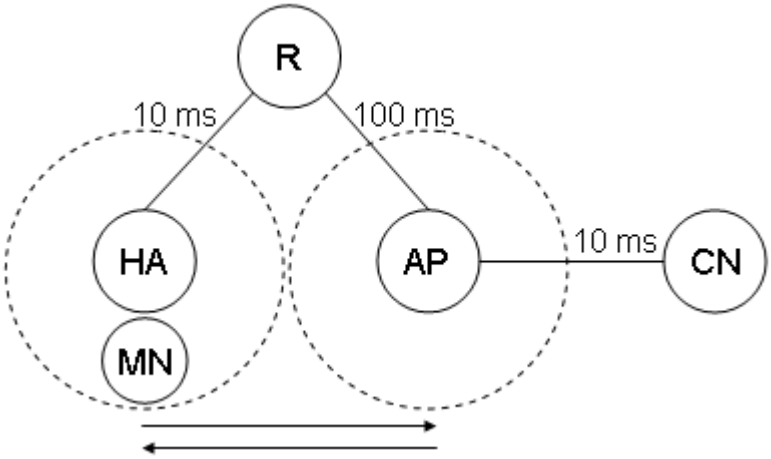
Kuvassa 33 on esitetty tässä tilanteessa mitatut siirtonopeudet. Nyt etu reitinoptimoinnin hyväksi on jo varsin huomattava. Sinä aikana kun liikkuva laite on vieraassa verkossa, saavutetaan reitinoptimoinnilla keskimäärin 100 kbps suurempi läpäisy. Tämä merkitsee noin 9 % etua verrattuna käänteistunnelointiin. Ero johtuu

pääasiassa siitä, että käänteistunnelointia käytettäessä paketit kulkevat aina kotiagentin kautta ja tekevät siten ylimääräisen lenkin, joka kasvattaa pakettien kulkuaikaa vertaislaitteelta liikkuvalle laitteelle ja päinvastoin. Lisäksi reitinoptimointi hyötyy pienemmistä IP-otsikoista kuten edellisessä tapauksessa.



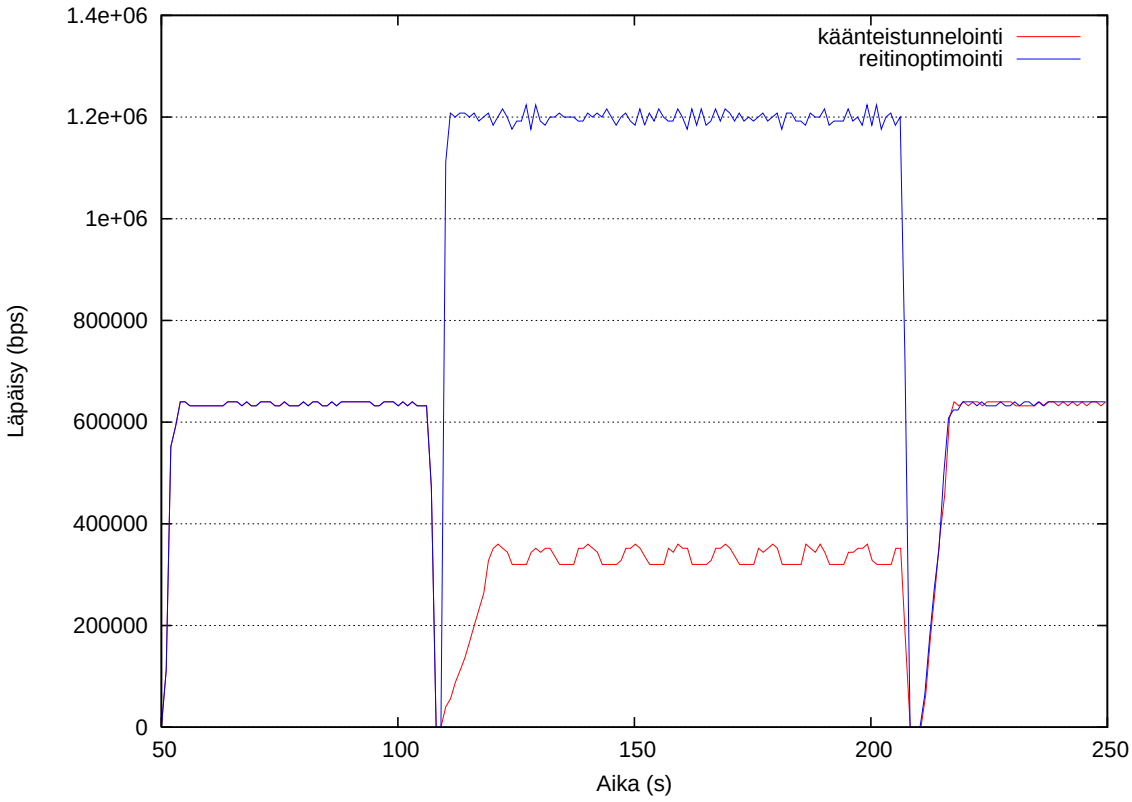
Kuva 33. Läpäisynopeudet huonoimmassa tilanteessa

Jos ajatellaan tapausta, jossa vierailtava verkko on kaukana liikkuvan laitteen kotiverkosta tai esimerkiksi erittäin ruuhkaisen linkin takana, muodostuvat lankalinkkien viiveet edellisiä skenaarioita suuremmiksi. Tällaista tapausta simuloitiin kuvan 33 mukaisessa verkossa, jossa etenkin käänteistunneloinnin kannalta merkittävä kotiagentin ja vieraan verkon liityntäpisteen välinen viive on huomattavasti edellisiä tilanteita suurempi.



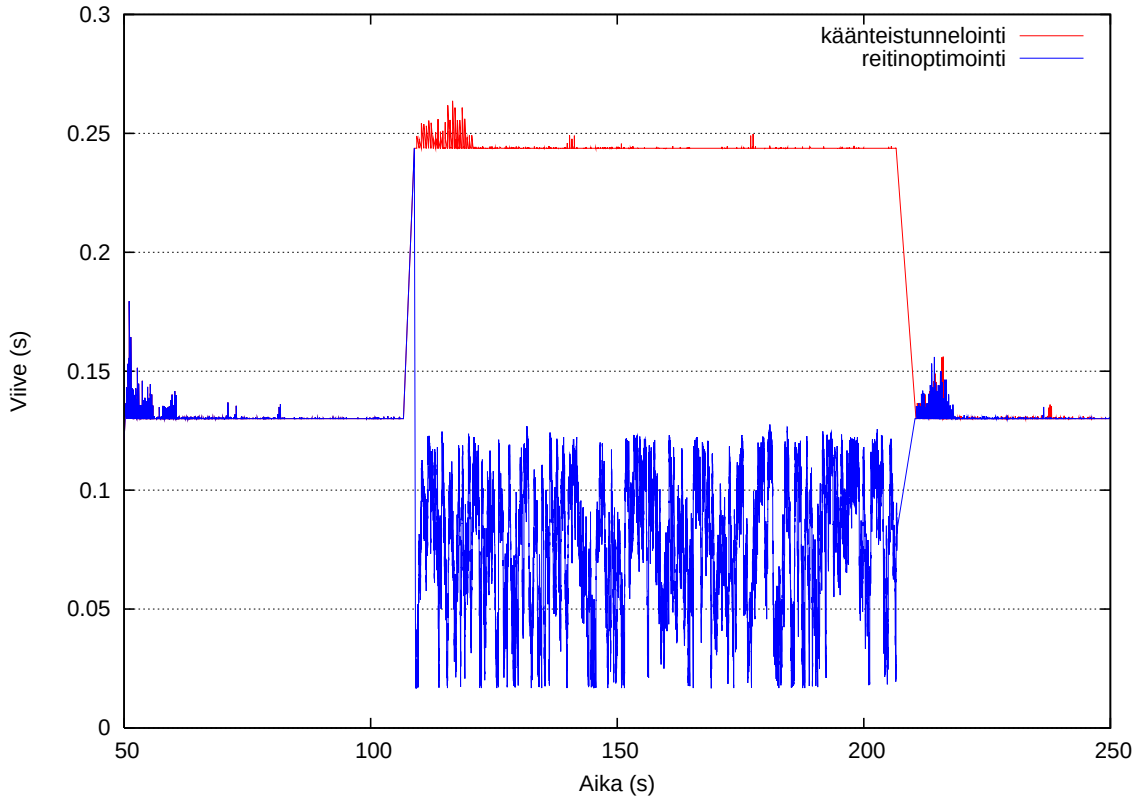
Kuva 34. Muutetut linkkien viiveet

Suuremman viiveen vaikutus voidaan havaita selvästi kuvassa 35 esitetyistä siirtonopeuksista. Käänteistunneloinnilla saavutettu läpäisy vieraassa verkossa on vain noin puolet siitä mitä se on laitteen ollessa omassa verkossaan. Reitinoptimoinnilla taas tapahtuu päinvastainen ilmiö ja siirtonopeus lähes kaksinkertaistuu siirryttäessä vieraaseen verkkoon. Siirtonopeudesta riippuvaisilla sovelluksilla reitinoptimointi tuottaa siis huomattavasti paremman tuloksen.



Kuva 35. Läpäisynopeudet suuremmilla viiveillä

Tutkittaessa TCP-datapakettien kulkuaikaviiveitä (kuva 36) nähdään, mikä aiheuttaa erot eri reititysmenetelmien välille. Käänteistunneloinnilla pakettien kierrättäminen kotiagentin kautta kasvattaa viivettä odotetusti noin 110 ms kun taas reitinoptimoinnilla viive pienenee siirryttäessä vieraaseen verkkoon. Suuri viiveen vaihtelu reitinoptimoinnilla johtuu siitä, että WLAN-yhteys ei pysty välittämään paketteja AP:lta liikkuvalle laitteelle riittävän nopeasti ja ne joutuvat odottamaan AP:n jonossa lähetysvuoroaan.

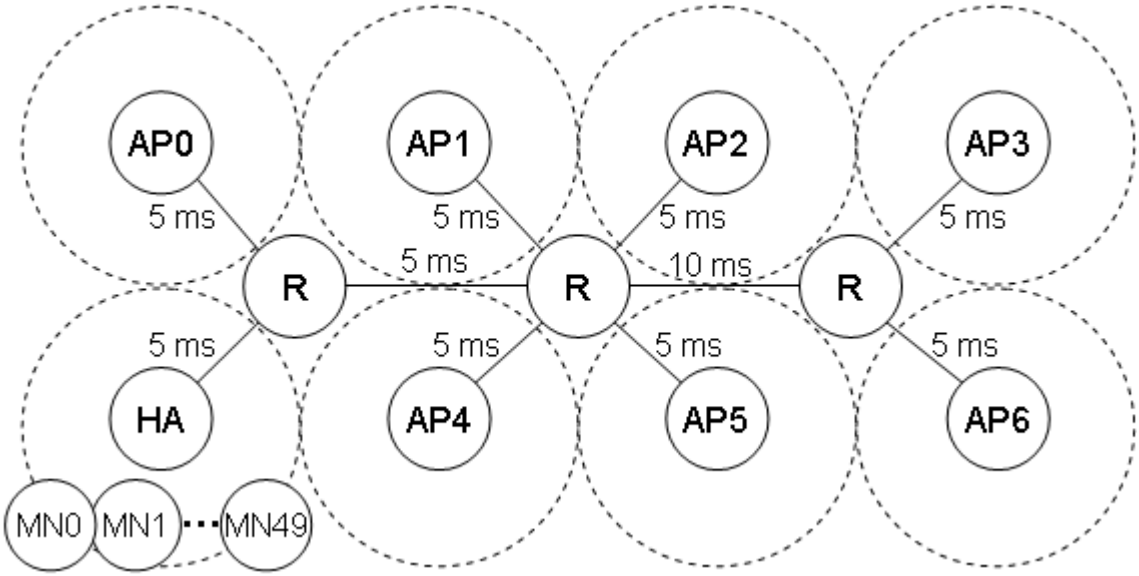


Kuva 36. Pakettien kulkuaikaviiveet

4.2.2 Signalointiliikenne

Toisessa simulaatiossa selvitettiin Mobile IPv6 -protokollan aiheuttaman signalointiliikenteen määrää. Tämä tehtiin simuloimalla kuvan 37 kaltaista verkkoa, jossa on kahdeksan reitittimillä ja 5 Mbps lankalinkeillä toisiinsa liitettyä liityntäpistettä. Yksi liityntäpiste toimii samalla kaikkien liikkuvien laitteiden kotiagenttina. Verkon alueella liikkuu 50 mobiililaitetta, jotka lähettävät kotiagentille sidospäivitysviestejä. Päivitysviestin lähetys tapahtuu, kun liikkuva laite vaihtaa liityntäpistettä tai edellisestä lähetyksestä on kulunut päivitysvälin (4 sekuntia) pituinen aika. Kotiagentti vastaa viesteihin sidoskuittausviesteillä. Muuta liikennettä verkossa ei samanaikaisesti ole.

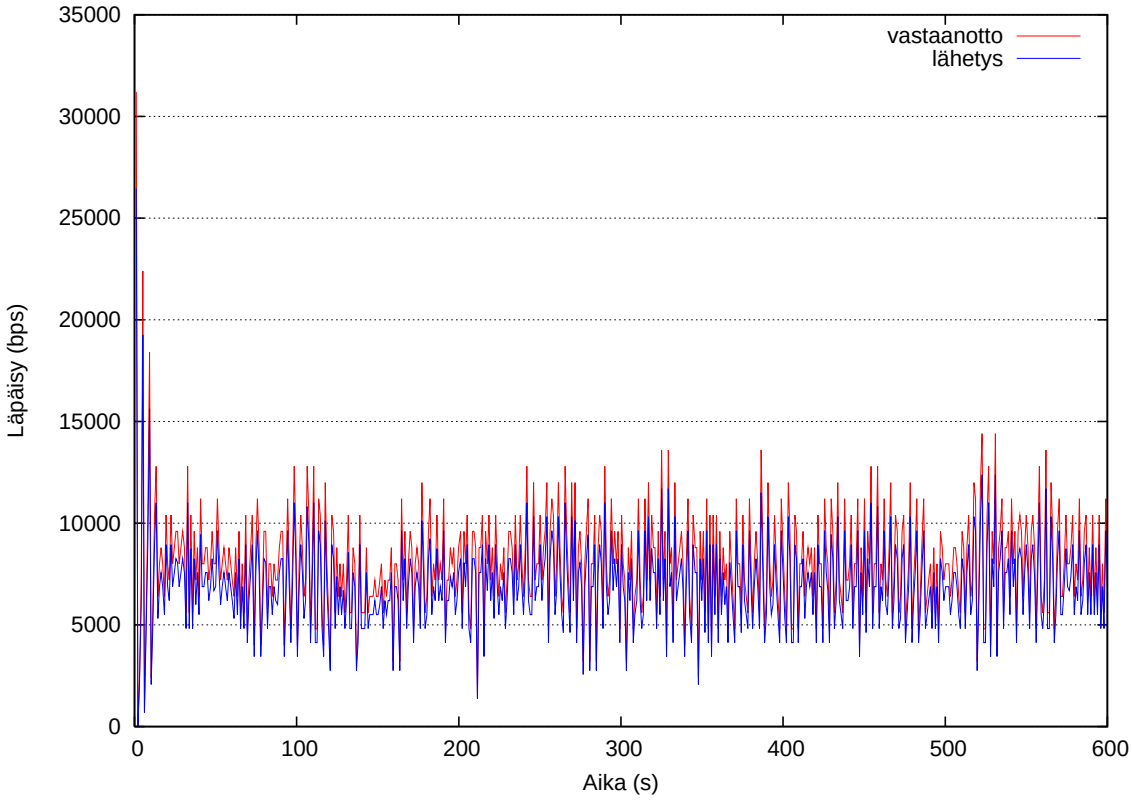
Liikkuvien laitteiden liikkumismalli on luotu ns-2:een kuuluvalla setdest-työkalulla, joka muodostaa annettujen parametrien perusteella satunnaisen liikkumisskenaarion. Setdest perustuu ns. satunnaisen kohdepisteen malliin, jossa kullekin liikkuvalle laitteelle valitaan satunnaisesti verkon alueelta kohdepiste ja nopeus, jolla laite alkaa liikkua kohti pistettä. Kun kohde on saavutettu, laite on tietyn ajan paikallaan, minkä jälkeen valitaan taas uusi kohdepiste ja nopeus. Parametreilla voidaan määritellä muun muassa simuloitavan alueen koko, laitteiden lukumäärä, suurin nopeus ja keskimääräinen aika, jonka laitteet ovat paikoillaan siirtymisien välissä. Tässä suurimmaksi nopeudeksi valittiin 23 m/s eli noin 83 km/h ja keskimääräiseksi pysähtymisajaksi 2 sekuntia.



Kuva 37. Signalointiliikenteen mittauksessa käytetty verkkotopologia

Kuvassa 38 on esitetty signaloinnin aiheuttama liikenne kotiagentilla. Vastaanotettu liikenne muodostuu sidospäivitysviesteistä ja lähetetty liikenne kuittauksista. Alun piikki johtuu siitä, että kaikki liikkuvat laitteet pyrkivät rekisteröitymään heti simulaation alettua lähes samanaikaisesti. Tämän jälkeen liikenne tasoittuu ja on keskimäärin 8 kbps kotiagentin suuntaan ja noin 7 kbps kotiagentilta poispäin. Ero eri suuntien liikennemäärissä selittyy sanomien kokoerolla. Liikenteen määrään vaikuttavia tekijöitä ovat esimerkiksi liikkuvien laitteiden nopeus ja sitä kautta yhteydenvaihtojen tiheys sekä Mobile IPv6 -parametrit kuten sidosten elinaika. Mobile IPv6:n kokonaissignalointiliikenteen määrää arvioitaessa on myös huomioitava, että tässä esitetty liikenne sisältää vain sidospäivitys- ja sidoskuittausviestit, joiden lisäksi tulee esimerkiksi mahdollinen IPsecin tietoturva-assosiaatioiden muodostamiseen

tarvittava viestintä. Lisäksi reitinoptimointia käytettäessä vastaava signalointiliikenne muodostuu vertaislaitteelle. Tosin kaikki liikkuvat laitteet eivät todennäköisesti ole yhteydessä samanaikaisesti samaan vertaislaitteeseen, jolloin liikenne hajautuu useille linkeille ja vertaislaitteille.



Kuva 38. Signalointiliikenteen läpäisy kotiagentilla

5 Yhteenveto

Tämän diplomityön tavoitteena oli tutkia liikkuvien päätelaitteiden käyttöön liittyviä ongelmia langattomia lähiverkkoja liityntätekniikkana hyödyntävissä verkoissa. Työn aluksi tutustuttiin langattomiin lähiverkkotekniikoihin ja erityisesti tämän hetken suosituimpaan vaihtoehtoon IEEE 802.11 -standardiin. Sen tarjoamat liikkuvuusominaisuudet todettiin kuitenkin varsin rajallisiksi, sillä ne mahdollistavat vain saman aliverkon sisällä tapahtuvat yhteydenvaihdot, minkä vuoksi laajemmissa useita aliverkkoja käsittävissä verkoissa liikuttaessa tarvitaan tuki liikkuvuudelle joltakin ylemmältä protokollakerrokselta.

IP-protokollan ja tarkemmin sen osoitejärjestelmän suunnitteluratkaisuista johtuen IP-osoite joudutaan käytännössä aina uusimaan vaihdettaessa verkon liityntäpistettä aliverkosta toiseen. Kun lisäksi kuljetuskerroksella toimivat protokollat käyttävät IP-osoitteita yhteyksien tunnistamiseen, menetetään tässä tapauksessa kaikki avoimet tiedonsiirtoyhteydet ja ne joudutaan muodostamaan uudelleen. Yhteyksien katkeamisen lisäksi uusi osoite aiheuttaa sen, että laite ei ole enää tavoitettavissa sen alkuperäisen osoitteen kautta.

Mobile IPv6 on IPv6-protokollan laajennus, joka lisää tuen liikkuville laitteille verkkokerrokselle. Se ratkaisee liikkuvuuden kaksi perusongelmaa: avoimet yhteydet ylläpidetään sekä tavoitettavuus säilytetään aliverkosta toiseen siirryttäessä. MIPv6:n toiminta perustuu liikkuville laitteille määriteltäviin kahteen osoitteeseen, joista kotiosoitetta käytetään laitteen tunnistamiseen ja care-of-osoitetta pakettien reitittämiseen laitteelle. Liikkuvat laitteet rekisteröivät näiden osoitteiden muodostaman sidoksen sekä kotiagentille että mahdollisesti laitteen kanssa liikennöiville vertaislaitteille. Näin ne pystyvät joko tunnelointia tai IPv6:n laajennusotsikoita hyödyntäen välittämään liikkuvan laitteen kotiosoitteeseen osoitetun liikenteen perille riippumatta laitteen sijainnista. Verkkokerroksen yläpuolella toimiviin

liikkuvuudenhallintamalleihin kuten SIPiin verrattuna MIPv6 tarjoaa läpinäkyvän ratkaisun, joka on riippumaton niin sovelluksista kuin käytetystä linkkikerroksesta. Mobile IPv4:ään verrattuna MIPv6 puolestaan tarjoaa kehittyneempiä toimintoja kuten esimerkiksi standardoitu tietoturvamekanismi ja reitinoptimointi.

Tällä hetkellä Mobile IPv6:n heikkous on etenkin reaaliaikaisia palveluita käytettäessä hitaat yhteydenvaihdot, jotka saattavat eräässä tutkimuksessa suoritettujen mittausten mukaan heikoimmassa tapauksessa kestää jopa useita sekunteja [68]. Yhteydenvaihdon aikana liikkuva laite ei pysty vastaanottamaan eikä lähettämään datapaketteja, mikä aiheuttaa vastaavasti hetkellisen katkoksen tiedonsiirtoon. IETF:ssä on kuitenkin jo ehdotettu muutamia ratkaisumalleja, joilla yhteydenvaihtojen sujuvuutta voidaan parantaa sekä samalla rajoittaa signalointiliikennettä.

Työn simulaatio-osuudessa tutkittiin ns-2 verkkosimulaattorin ominaisuuksia sekä erityisesti IEEE 802.11 ja Mobile IPv6 -tekniikoiden simulointia. Ns-2:n toteutus avoimen lähdekoodin projektina osoittautui sekä eduksi että haitaksi. Toisaalta se mahdollistaa ohjelman ja sen simulaatiomallien toiminnan muuttamisen ja laajentamisen. Toisaalta taas ohjelman dokumentaatio ja yleisesti käyttäjätuki jättää parantamisen varaa. Rajallisen dokumentaation, varsin monimutkaisen rakenteen ja graafisen käyttöliittymän puuttumisen johdosta ns-2:n oppimiskäyrä on melko jyrkkä. Myös simulaatioiden kuvaamiseen ja analysointiin tarvittavien työkalujen puuttuminen heikentää ohjelman käytettävyyttä.

Monet ns-2:n simulaatiomallit on kehitetty erilaisissa tutkimusprojekteissa niiden tarpeiden mukaisesti eivätkä ne välttämättä mallinna protokollien kaikkia toimintoja. Yksinkertaistetut mallit tulee huomioida simulaatioskenaarioita suunniteltaessa ja tuloksia arvioitaessa. Tässä työssä käytettyjen mallien olennaisimpia puutteita ovat 802.11-standardin mukaiset hallintapalvelut, Neighbor Discovery -protokolla sekä jotkin MIPv6:n toiminnot.

Mobile IPv6:n simulointia varten tarvittavan MobiWan-laajennuksen lisäämisen sekä siihen tehtyjen muutosten jälkeen muodostettiin kaksi simulaatioskenaariota, joista ensimmäisessä tutkittiin reitinoptimoinnilla saavutettavia etuja ja toisessa signalointiliikenteen määrää. Tuloksista nähtiin, että reitinoptimoinnilla saavutettavaan etuun vaikuttaa vertaislaitteen sijainti sekä toisaalta liikkuvan laitteen ja vertaislaitteen etäisyys kotiagenttiin. Joissakin tapauksissa reitinoptimoinnilla ylletään moninkertaiseen siirtonopeuteen käänteistunnelointiin verrattuna. Tästä on huomattava etu etenkin siirtonopeudesta riippuvaisilla sovelluksilla. Koska runkoverkon kapasiteetti

oli simulaatioissa yli kaksinkertainen langattoman verkon kapasiteettiin verrattuna, ei se muodostanut pullonkaulaa liikenteelle. Jos verkossa olisi myös muuta liikennettä, joka ruuhkauttaisi runkoverkon, olisi reitinoptimoinnista mahdollisesti vielä enemmän etua. MIPv6:n aiheuttaman signalointiliikenteen määrää puolestaan voidaan pitää varsin kohtuullisena eikä sen pitäisi muodostua ongelmaksi esimerkiksi IEEE 802.11 -standardin mukaisissa verkoissa. Lisäksi Mobile IPv6:n parametreilla liikenteeseen voidaan jossain määrin vaikuttaa.

Tällä hetkellä IPv6:n ja sitä kautta myös Mobile IPv6:n käyttöönotto operaattoreiden ja yritysten verkoissa on hyvin vähäistä, mutta tulevaisuudessa se tulee mitä todennäköismimmin olemaan välttämätöntä Internetiä käyttävien mobiililaitteiden määrän jatkuvasti kasvaessa.

Lähteet

[1] Jon Postel, toim.: Internet Protocol, RFC 791, syyskuu 1981, http://www.ietf.org/rfc/rfc0791.txt [3.6.2004]

[2] R. Droms: Dynamic Host Configuration Protocol, RFC 1541, lokakuu 1993, http://www.ietf.org/rfc/rfc1541.txt [4.6.2004]

[3] The Internet Engineering Task Force, http://www.ietf.org/ [4.6.2004]

[4] C. Perkins, toim.: IP Mobility Support for IPv4, RFC 3344, elokuu 2002, http://www.ietf.org/rfc/rfc3344.txt [4.6.2004]

[5] S. Deering, R. Hinden: Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, joulukuu 1998, http://www.ietf.org/rfc/rfc2460.txt [7.10.2004]

[6] D. Johnson, C. Perkins, J. Arkko: Mobility Support in IPv6, RFC 3775, kesäkuu 2004, http://www.ietf.org/rfc/rfc3775.txt [7.10.2004]

[7] S. McCanne, S. Floyd: ns Network Simulator, http://www.isi.edu/nsnam/ns/ [1.6.2004]

[8] Institute of Electrical and Electronics Engineers, http://www.ieee.org/ [4.6.2004]

[9] IEEE Std 802.11, 1999 Edition, Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, http://standards.ieee.org/getieee802/802.11.html [1.6.2004]

[10] IEEE Std 802.3, 2000 Edition, Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications

[11] ISO/IEC 7498-1:1994, Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model

[12] HiperLAN2, http://www.hiperlan2.com/ [13.7.2004]

[13] HomeRF Specification, Revision 2.01, 2002, http://www.palowireless.com/homerf/homerfspec.asp [13.7.2004]

[14] Bluetooth, http://www.bluetooth.com/ [13.7.2004]

[15] European Telecommunications Standards Institute, http://www.etsi.org/ [13.7.2004]

[16] Jochen H. Schiller: Mobile Communications, Second Edition, Addison-Wesley 2003

[17] Marko Ahvenainen: Langattomien lähiverkkojen turvallisuus, 2003, http://keskus.hut.fi/julkaisut/tyot/diplomityot/977/Ahvenainen.pdf [6.12.2004]

[18] IEEE 802.11 - The Working Group for WLAN Standards, http://grouper.ieee.org/groups/802/11/ [13.7.2004]

[19] IEEE Std 802.11a-1999, Supplement to IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – High-speed Physical Layer in the 5 GHz Band, http://standards.ieee.org/getieee802/802.11.html [14.7.2004]

[20] IEEE Std 802.11h-2003, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 5: Spectrum and Transmit Power Management Extensions in the 5 GHz band in Europe, http://standards.ieee.org/getieee802/802.11.html [14.7.2004]

[21] IEEE Std 802.11b-1999, Supplement to IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band, http://standards.ieee.org/getieee802/802.11.html [14.7.2004]

[22] IEEE Std 802.11d-2001, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN

Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 3: Specification for operation in additional regulatory domains, http://standards.ieee.org/getieee802/802.11.html [14.7.2004]

[23] IEEE Std 802.11f-2003, IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation, http://standards.ieee.org/getieee802/802.11.html [14.7.2004]

[24] IEEE Std 802.11g-2003, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, http://standards.ieee.org/getieee802/802.11.html [14.7.2004]

[25] Y. Rekhter, T. Li: An Architecture for IP Address Allocation with CIDR, RFC 1518, syyskuu 1993, http://www.ietf.org/rfc/rfc1518.txt [6.12.2004]

[26] Jon Postel, toim.: Transmission Control Protocol, RFC 793, syyskuu 1981, http://www.ietf.org/rfc/rfc793.txt [12.10.2004]

[27] C. Perkins, toim.: IP Mobility Support, RFC 2002, lokakuu 1996, http://www.ietf.org/rfc/rfc2002.txt [6.10.2004]

[28] Charles E. Perkins, David B. Johnson: Mobility Support in IPv6, Proceedings of the 2nd annual ACM/IEEE international conference on Mobile computing and networking, marraskuu 1996

[29] H. Soliman, C. Castelluccia, K. El Malki, L. Bellier: Hierarchical Mobile IPv6 mobility management (HMIPv6), Internet Draft, lokakuu 2004, http://www.ietf.org/internet-drafts/draft-ietf-mipshop-hmipv6-03.txt [16.11.2004]

[30] Rajeev Koodli, toim.: Fast Handovers for Mobile IPv6, Internet Draft, lokakuu 2004, http://www.ietf.org/internet-drafts/draft-ietf-mipshop-fast-mipv6-03.txt [16.11.2004]

[31] A. T. Campbell, J. Gomez, S. Kim, A. G. Valkó, C-Y. Wan, Z. R. Turányi: Design, Implementation, and Evaluation of Cellular IP, IEEE Personal Communications 7(4), elokuu 2000

[32] R. Ramjee, K. Varadhan, L. Salgarelli, S. R. Thuel, S-Y. Wang, T. La Porta: HAWAII: A Domain-Based Approach for Supporting Mobility in Wide-Area

Wireless Networks, IEEE/ACM Transactions on Networking 10(3), kesäkuu 2002

[33] X. Pérez-Costa, M. Torrent-Moreno, H. Hartenstein: A Performance Comparison of Mobile IPv6, Hierarchical Mobile IPv6, Fast Handovers for Mobile IPv6 and their Combination, ACM SIGMOBILE Mobile Computing and Communications Review 7(4), lokakuu 2003

[34] Y. Gwon, J. Kempf, A. Yegin: Scalability and Robustness Analysis of Mobile IPv6, Fast Mobile IPv6, Hierarchical Mobile IPv6, and Hybrid IPv6 Mobility Protocols Using a Large-scale Simulation, 2004 IEEE International Conference on Communications, kesäkuu 2004

[35] A. T. Campbell, J. Gomez, S. Kim, C-Y. Wan, Z. R. Turányi, A. G. Valkó: Comparison of IP Micromobility Protocols, IEEE Wireless Communications 9(1), helmikuu 2002

[36] P. Reinbold, O. Bonaventure: A Comparison of IP mobility protocols, Technical Report Infonet-2001-07, kesäkuu 2001

[37] A. C. Snoeren, H. Balakrishnan: An End-to-End Approach to Host Mobility, Proceedings of the 6th annual international conference on Mobile computing and networking, elokuu 2000

[38] P. Vixie, S. Thomson, Y. Rekhter, J. Bound: Dynamic Updates in the Domain Name System (DNS UPDATE), RFC 2136, huhtikuu 1997, http://www.ietf.org/rfc/rfc2136.txt [20.10.2004]

[39] B. Wellington: Secure Domain Name System (DNS) Dynamic Update, RFC 3007, marraskuu 2000, http://www.ietf.org/rfc/rfc3007.txt [20.10.2004]

[40] Elin Wedlund, Henning Schulzrinne: Mobility Support using SIP, Proceedings of the 2nd ACM international workshop on Wireless mobile multimedia, elokuu 1999

[41] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler: SIP: Session Initiation Protocol, RFC 3261, kesäkuu 2002, http://www.ietf.org/rfc/rfc3261.txt [20.10.2004]

[42] J-W. Jung, R. Mudumbai, D. Montgomery, H-K. Kahng: Performance Evaluation of Two Layered Mobility Management using Mobile IP and Session Initiation Protocol, IEEE Global Telecommunications Conference vol. 3, joulukuu 2003

[43] A. Conta, S. Deering: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6), RFC 2463, joulukuu 1998, http://www.ietf.org/rfc/rfc2463.txt [29.10.2004]

[44] T. Narten, E. Nordmark, W. Simpson: Neighbor Discovery for IP Version 6 (IPv6), RFC 2461, joulukuu 1998, http://www.ietf.org/rfc/rfc2461.txt [31.10.2004]

[45] S. Thomson, T. Narten: IPv6 Stateless Address Autoconfiguration, RFC 2462, joulukuu 1998, http://www.ietf.org/rfc/rfc2462.txt [5.11.2004]

[46] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney: Dynamic Host Configuration Protocol for IPv6 (DHCPv6), RFC 3315, kesäkuu 2003, http://www.ietf.org/rfc/rfc3315.txt [5.11.2004]

[47] A. Conta, S. Deering: Generic Packet Tunneling in IPv6, RFC 2473, joulukuu 1998, http://www.ietf.org/rfc/rfc2473.txt [5.11.2004]

[48] S. Kent, R. Atkinson: Security Architecture for the Internet Protocol, RFC 2401, marraskuu 1998, http://www.ietf.org/rfc/rfc2401.txt [15.11.2004]

[49] S. Kent, R. Atkinson: IP Encapsulating Security Payload (ESP), RFC 2406, marraskuu 1998, http://www.ietf.org/rfc/rfc2406.txt [16.11.2004]

[50] S. Kent, R. Atkinson: IP Authentication Header, RFC 2402, marraskuu 1998, http://www.ietf.org/rfc/rfc2402.txt [16.11.2004]

[51] D. Harkins, D. Carrel: The Internet Key Exchange (IKE), RFC 2409, marraskuu 1998, http://www.ietf.org/rfc/rfc2409.txt [16.11.2004]

[52] J. Arkko, V. Devarapalli, F. Dupont: Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents, RFC 3776, kesäkuu 2004, http://www.ietf.org/rfc/rfc3776.txt [16.11.2004]

[53] P. Nikander, J. Arkko, T. Aura, G. Montenegro, E. Nordmark: Mobile IP version 6 Route Optimization Security Design Background, Internet Draft, lokakuu 2004, http://www.ietf.org/internet-drafts/draft-ietf-mip6-ro-sec-02.txt [16.11.2004]

[54] Charles E. Perkins: Precomputable Binding Management Key Kbm for Mobile IPv6, Internet Draft, lokakuu 2004, http://www.ietf.org/internet-drafts/draft-ietf-mip6-precfgkbm-01.txt [16.11.2004]

[55] A. Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury: Authentication Protocol for Mobile IPv6, Internet Draft, heinäkuu 2004,

http://www.ietf.org/internet-drafts/draft-ietf-mip6-auth-protocol-00.txt [16.11.2004]

[56] P. McCann: Mobile IPv6 Fast Handovers for 802.11 Networks, Internet Draft, lokakuu 2004, http://www.ietf.org/internet-drafts/draft-ietf-mipshop-80211fh-03.txt [17.11.2004]

[57] S. Denie: Changing the Default for Directed Broadcasts in Routers, RFC 2644, elokuu 1999, http://www.ietf.org/rfc/rfc2644.txt [23.11.2004]

[58] Nicolas Christin: ns-2 on Cygwin, http://www.sims.berkeley.edu/~christin/ns-cygwin.shtml [25.11.2004]

[59] Debian, http://www.debian.org/ [24.11.2004]

[60] OPNET Modeler, http://www.opnet.com/products/modeler/ [24.11.2004]

[61] GloMoSim, http://pcl.cs.ucla.edu/projects/glomosim/ [24.11.2004]

[62] OMNeT++, http://www.omnetpp.org/ [24.11.2004]

[63] S. Keshav: REAL 5.0 Overview, http://www.cs.cornell.edu/skeshav/real/overview.html [24.11.2004]

[64] OTcl - MIT Object Tcl, ftp://ftp.tns.lcs.mit.edu/pub/otcl/README.html [24.11.2004]

[65] Kevin Fall, Kannan Varadhan, VINT Project: The ns manual

[66] Rice Monarch Project Extensions to ns-2, http://www.monarch.cs.rice.edu/cmu-ns.html [25.11.2004]

[67] MobiWan: NS-2 extensions to study mobility in Wide-Area IPv6 Networks, http://www.inrialpes.fr/planete/mobiwan/ [29.11.2004]

[68] Nicolas Montavont, Thomas Noël: Analysis and Evaluation of Mobile IPv6 Handovers over Wireless LAN, Mobile Networks and Applications 8(6), joulukuu 2003