Tuomas T. Rusanen

Liikkuvuudenhallinnan haasteita Proxy Mobile IPv6 -verkossa

Tietotekniikan pro gradu -tutkielma

5. joulukuuta 2012

Jyväskylän yliopisto

Tietotekniikan laitos

Tekijä: Tuomas T. Rusanen

Yhteystiedot: tuomas.t.rusanen@gmail.com

Ohjaajat: Timo Hämäläinen ja Jari Kellokoski

Työn nimi: Liikkuvuudenhallinnan haasteita Proxy Mobile IPv6 -verkossa

Title in English: Mobility Management Challenges in the Proxy Mobile IPv6 Network

Työ: Pro gradu -tutkielma

Suuntautumisvaihtoehto: Mobiilijärjestelmät

Sivumäärä: 76+10

Tiivistelmä: Tässä työssä käydään läpi ja vertaillaan keskenään erinäisiä liikkuvuudenhallintaan soveltuvia protokollia ja menetelmiä. Tämän päivän haasteena on luoda edellytykset liikkuvuudenhallintaan tietoverkoissa ilman, että loppukäyttäjän mobiililaitteeseen tarvitsee tehdä muutoksia. Tarkastelussa siis verkkoperustainen liikkuvuudenhallinta, jonka hyvä puoli on (tässä tapauksessa) ettei päätelaitteisiin tarvitse tehdä muutoksia sen ollessa käytännössä mahdotonta. Liian monta laitetta joita ei voi päivittää. Proxy Mobile IPv6 -protokolla on yksi kyseiseen haasteeseen ehdolla oleva ratkaisu. Tässä pro gradu-työssä perehdytään kyseiseen protokollaan ja tarkoituksena on luoda puhtaasti IPv6-protokollaa käyttävä testiympäristö suorituskykymittauksia varten.

Avainsanat: Tietotekniikka, IPv6, Mobile IPv6, Proxy Mobile IPv6, Isäntätunnisteprotokolla, Hierarkinen Mobile IP, Liikkuvuudenhallinta, Verkonliikkuvuusprotokolla, IPsec, horisontaalinen yhteydensiirto

Abstract: This research will be reviewed and compared with each other different protocols and techniques for mobility management. Todays challenge in networking is to create the conditions for mobility management without making changes end users mobile node. Therefore the analysis is the network-based mobility management, which is a good thing (in this case) there is no need to make changes to terminal equipments when it is practically impossible. Too many devices that can not be updated. Proxy Mobile IPv6 protocol is one of those that could provide a solution to that challenge. This master's thesis focus on Proxy Mobile IPv6 protocol and the purpose on building a test bed which is based entrily on IPv6 for performance measurements.

Keywords: Information Technology, IPv6, Mobile IPv6 (Fast Handovers), (Fast handovers for) Proxy Mobile IPv6, Host Identity Protocol, Hierarchical Mobile IPv6, Mobility Management, Network Mobility Protocol, IPsec, horizontal handover

Esipuhe

Opi liikkuvuudenhallintaa Proxy Mobile IPv6 -verkossa.[1]

Jyväskylässä 5. joulukuuta 2012

Tuomas T. Rusanen

[1] Tai tee jotain muuta, eihän se minulle kuulu.

Termiluettelo

AAA	(Authentication, Authorization and Accounting): *AAA-palvelin* (tunnistautuminen, valtuututus ja kirjanpito) kuuluu RADIUS verkkoprotokollan prosesseihin.
APN	(Access Point Name): *Liitäntäpisteen nimi* on mobiiliverkon ja toisen tietoverkon yhdyskäytävän nimi. Koostuu kahdesta osasta, verkon tunnisteesta (Network Identifier) ja operaattorintunnisteesta (Operator Identifier)
BA	(Binding Acknowledgement): *Sidoskuittauksella* kuitataan sidospäivityksen vastaanottaminen.
BC	(Binding Cache): *Sidosvälimuisti* on kotiagentin ja liikennöintikumppanien ylläpitämä lista mobiililaitteiden koti- ja vierasosoitteiden sidoksista.
BU	(Binding Update Message): *Sidospäivitys*, jonka avulla mobiililaite ilmoittaa muille laitteille uudesta vierasosoitteesta (CoA).
BUL	(Binding Update List): Jokainen mobiililaite ylläpitää *sidospäivityslistaa*, joka sisältää jokaisen mobiililaitteen sen hetkisen tai tulevan tekeillä olevan sidoksen.
CN	(Correspondent node): Mobiililaitteen *liikennöintikumppani*, jonka ei välttämättä tarvitse tukea MIPv6-protokollaa ja se voi olla joko liikkuva tai paikallaan. Tukiessaan MIPv6-protokollaa liikennöintikumppani ylläpitää sidosvälimuistia (binding cache), jossa on lista mobiililaitteiden koti- ja vierasosoitteiden sidoksista. Liikennöintikumppani voi olla liikkuva tai
CoA	(Care of Address): Mobiililaitteen vieraassa verkossa saama *vierasosoite*.
Datagram	*Datagrammi* on peruskuljetusyksikkö pakettikytkinverkoissa, jossa toimitus- ja saapumisisaikaa eikä saapumisjärjestystä taata verkkopalvelussa.

FA	(Foreign Agent): *Vierasagentti* on vieraassa verkossa sijaitseva reititin, joka lähettää eteenpäin kotiagentilta toimitetut paketit mobiililaitteelle.
FIMO	(Flow Identification Mobility Option): *Tietovirran liikkuvuuden tunnistamisoptio* sisältyy sidospäivitys- ja sidoskuittausviesteihin. Kyseinen optio mahdollistaa sidospäivityksen vastaanottajan asettaa uusia määritelmiä tietovirran liikenteelle ja reitittää se annettuun osoitteeseen.
FMI	(Flow Mobility Indicator): *Viesti tietovirran liikkeestä*, joka sisältää mobiililaitteen tunnisteen ja tietovirran liikkuvuuden tunnistamisoption (FIMO). Viesti välittää osoitteen, joka on oletuksena, tai tietovirran tiedot sekä liikkuvuuden tyypin toiminnan.
FMIPv6	(Mobile IPv6 Fast Handovers): Protokolla on lisäys Mobile IPv6:een, jossa vieraassa verkossa sijaitseva reititin toimii mobiililaitteelle välityspalvelimena. Yhteydensiirron tapahtuessa aikaisempi reititin käyttää tunnelointia hyväksi reitittääkseen paketit uudessa verkossa sijaitsevalle uudelle reitittimelle.
HA	(Home Agent): *Kotiagentti* on kotiverkossa sijaitseva reititin, jolla on sidosvälimuistissa tiedot mobiililaitteiden koti- ja vierasosoitteiden sidoksista.
HAL	(Home Agent List): *Kotiagenttilista* sisältää tiedot verkossa sijaitsevista kotiagenteista.
HI	(Host Identifier): *Isäntätunniste* pysyy muuttumattomana toisin kuin IP-osoite laitteen vaihtaessa verkkoa.
HIL	(Host Identity Layer): *Isäntätunnistekerros* sijoittuu verkko- ja kuljetuskerroksen väliin.
HIP	(Host Identity Protocol): *Isäntätunnisteprotokolla* käyttää isäntätunnisteita yhteyksien kytkemisessä.

HMIP	(Hierarchical Mobile IP): *Hierarkinen MIPv6* on lisäys MIPv6-protokollalle. HMIPv6 esittelee uuden yksikön, nimeltään *mobiililliitospiste* (MAP), joka toimii paikallisena kotiagenttina mobiililaitteelle.
HN	(Heterogeneous network): *Heterogeeninen verkko* yhdistää tietokoneita ja muita laitteita, joissa on eri käyttöjärjestelmät, verkkoteknologiat ja/tai protokollat.
HoA	(Home Address): Mobiililaitteen *kotiverkon määrittämä ensisijainen IP-osoite*.
IF-ID	(Interface Indentifier): Mobiililaitteen *rajapinnan tunniste*, joka on yksilöllinen jokaisella rajapinnalle.
LMA	(Local Mobility Anchor): PMIPv6-domainissa sijaitseva *mobiililiitos*, johon päivitetään mobiililaitteen sijainnin muutokset, ja joka toimii topologisena liitoskohtana (topological anchor point) mobiililaitteille. Mobiililiitoksella on samat toiminnot kuin MIPv6:ssa määritellyssä kotiagentissa sekä lisäksi uusia toimintoja, jotka tukevat PMIPv6 määrittelyn mukaista protokollaa.
LMAA	(Local Mobility Anchor Adress): *Mobiililiitoksen liitoskohtana toimivan rajapinnan osoite*, joka toimii päätepisteenä kaksisuuntaiselle tunnelille, joka on luotu mobiililiitoksen ja mobiiliyhdyskäytävän välille. Kyseiseen osoitteeseen mobiiliyhdyskäytävä lähettää sidospäivitysviestit.
MAC	(Media Access Control): *MAC* -osoite on verkkosovittimen ethernet-verkossa yksilöivä tunniste. MAC-osoite koostuu kuudesta kaksinumeroisesta heksademisaalisesta luvusta, joista kolme ensimmäistä on valmistajan itselleen varaama etuliite ja kolme jälkimmäistä on juokseva sarjanumero.

MAG	(Mobile Access Gateway): *Mobiiliyhdyskäytävä* on vastuussa mobiililaitteiden liikkuvuuden havainnoinnista ja hallinnoinnista PMIPv6-domainin sisällä. Mobiiliyhdyskäytävä on vastuussa yhteydensiirron signaloinnista mobiililaitteen puolesta.
MAP	(Mobility Anchor Point): *Mobiililiitospiste* toimii mobiililaitteen paikallisena kotiagenttina. Mobiililaitteen liikkuessa mobiililitospisteen domainin sisällä, mobiililaitteen signalointi tapahtuu mobiililiitospisteen kanssa, jonka oletetaan olevan lähempänä kuin kotiagentti.
MIP	(Mobile IP): *Mobile IP*.
MN	(Mobile Node): *Mobiililaite* kykenee vaihtamaan verkon liitäntäpistettä linkistä toiseen ja silti olla saavutettavissa kotiverkosta saamallaan osoitteella.
MN HNP	(Mobile Node's Home Network Prefix): Mobiililaitteen *kotiverkon etuliite* saadaan mobiililiitokselta jolle se toimii topologisena liitooskohtana.
MNID	(Mobile Node's Indentifier): *Mobiililaitteen tunniste* on yksilöllinen useista rajapinnoista huolimatta.
NA	(Neigbor Advertisement): *Naapurinmainostus*-viesti.
NAR	(New Access Router): Mobiililaitteen siirtyessä vieraasta verkosta toiseen, NAR tarkoittaa uusimmassa vieraassa verkossa sijaitsevaa reititintä.
NE	(Network Entity): *Verkkoyksikkö* esittää laitetta tai yhdyskäytävää, joka määrittää isännän tai ryhmän isäntiä.
NEMO	(Network Mobility Protocol): *Verkon liikkuvuusprotokolla*, jonka ideana on käyttää mobiilireititintä ainoana laitteena, jonka liitäntäpiste internetiin vaihtuu liikkuvassa verkossa. Muut verkon laitteet näkevät verkon normaalina aliverkkona ja käyttävät mobiililireititintä oletusyhdyskäytävänä.
NS	(Neigbor Solicitation): *Naapurinkysely*-viesti.

PAR	(Previous Access Router): Mobiililaitteen siirtyessä vieraasta verkosta toiseen, PAR tarkoittaa *edellisessä vieraassa verkossa sijaitsevaa reititintä*, jonka tehtävä on lähettää mobiililaitteelle osoitetut viestit NAR-reitittimelle yhteydensiirron ajan.
PBA	(Proxy Binding Acknowledgement): *Sidoskuittausta* käytetään kuittaamaan mobiiliyhdyskäytävän lähettämän sidospäivityksen vastaanottaminen.
PBU	(Proxy Binding Update): *Sidospäivitys* on mobiiliyhdyskäytävän lähettämä viesti mobiililaitteen mobiililiitokselle, sitoakseen mobiililaitteen rajapinnoille asetetut osoitteet ja sen nykyisen vierasosoitteen (PCoA).
PDP	(Packet Data Protocol): *Pakettidataprotokolla* on paketinkuljetusprotokolla jota käytetään langattomissa GPRS/HSDPA-verkoissa.
PMIPv6	(Proxy Mobile IPv6): *Proxy Mobile IPv6*.
PCoA	(Proxy Care of Address): Mobiiliyhdyskäytävän ulkorajapinnan määrittämä vierasosoite, joka on mobiililiitoksen ja mobiiliyhdyskäytävän välillä sijaitsevan tunnelin päätepiste. Mobiililiitos käsittelee kyseistä osoitetta *mobiililiitoksen osoitteena* ja rekisteröi sen sidosvälimuistiin kyseiselle mobiililaitteelle.
RA	(Router Advertisement): *Reititinmainostus*-viesti.
RADIUS	(Remote Authentication Dial In User Services): *RADIUS* verkkoprotokolla sallii valtuutetun käyttäjän yhdistää tietoverkkopalvelimelle.
RS	(Router Solicitation): *Reititinkysely*-viesti.
SA	(Security Association): IP-turvallisuusarkkitehtuurissa käytetty konsepti, *suojauskytkentä*, joka toimii pohjana IP-protokollan päälle luotavista tietoturva toimista. Suojauskytkentä on nippu algoritmeja ja parametreja (kuten salausavaimia), joita käytetään hyväksi salatessa ja varmistaessa tiettyä liikennettä yhteen suuntaan.

SAD	(Security Association Database): *Suojauskytkentätietokannassa* sijaitsee suojauskytkentöjen asetukset, kuten pakettien salaamisessa käytettävät prokotollat, salausalgoritmit sekä salausavaimien voimassaoloaika.
SPD	(Security Policy Database): *Turvallisuussäädöstietokannassa* määritellään käytettävät turvallisuussäädäkset kahden järjestelmän välillä.
ULP	(Upper Layer Protocol): *Verkkokerrosta ylemmät kerrokset*.

Kuviot

Taulukot

Sisältö

1 Johdanto

Liikkuva laajakaista on kehittynyt nopeasti uusien tekniikoiden ja palveluiden sekä erilaisten liityntätekniikoiden saralla lähivuosien aikana. Mobiililaitteiden ja käyttäjien nopea kasvu on luonut tarpeen yhteyksien ja palveluiden tehokkaaseen hallintaan, sillä tämän päivän mobiililaitteessa on useita rajapintoja, joilla yhteys internetissä sijaitseviin palveluihin on mahdollista luoda. Kuitenkaan kaikkia laitteiden mahdollistavia palveluita ja tekniikoita ei käytetä tehokkaasti, vaan usein käyttäjän tulee valita käytettävä verkko, ja vain yksi verkko, manuaalisesti.

Liikkuvuus ja palvelut IP-verkossa (LIPA) —hankkeessa kehitetään menetelmiä tieto- ja viestinteknologioiden palveluiden hallintaan aina parhaiten kytketyissä IP-verkoissa (Always Best Connected, ABC). Hankkeen tutkimuskohteet ovat aina parhaan liitynnän tarjoaminen Internet Protocol-pohjaisille (IP) palveluille heterogeenisissä verkoissa, sekä suunnitella ja toteuttaa palveluita, joissa palvelunlaatu ja käyttäjän liikkuvuus on otettu huomioon. Tälläisiä huomioon otettavia asioita ovat muun muassa käyttäjän tunnistaminen, laskutus, tietoturva, käytettävän palvelun sopeuttaminen liityntätavan mukaan sekä älyn lisääminen käyttäjän päätöksen teon tueksi. Tässä pro gradu-työssä syvennytään lähemmin hankkeen tutkimuskohteista liikkuvuudenhallintaan, käyttäjäntunnistamiseen ja tietoturvaan.

1.1 Tutkimusongelma

Nykyajan haasteena on luoda edellytykset liikkuvuudenhallintaan tietoverkoissa ilman, että loppukäyttäjän mobiililaitteeseen tarvitsee tehdä muutoksia. Vaikka IPv6 osoitteiden arkkitehtuuri ja määritelmä on ollut määriteltynä jo vuodesta 1995, sen käyttöönotto ja teknisten toteutusten toteuttaminen verkkolaitteille ja tietoverkoille on vielä kesken, etenkin toimiva IP versio 6 (IPv6) -tuki ohjelmistoille on erittäin puutteellista (Deering ja Hinden 1995) (Hinden ja Deering 1995). Kyseistä haastetta varten on olemassa protokollia, joiden tekniset vaatimusmäärittelyt on tehty mutta lopulliset toteutukset ovat vielä puutteellisia. Proxy Mobile IPv6 (PMIPv6) -protokolla on yksi kyseiseen haasteeseen ehdolla oleva ratkaisu. Tässä tutkimuksessa perehdytään kyseiseen protokollaan ja tarkoituksena on luoda puhtaasti IPv6-

protokollaa käyttävä testiympäristö. Tarkastelussa siis verkkoperustainen liikkuvuudenhallinta, jonka hyvä puoli on (tässä tapauksessa) ettei päätelaitteisiin tarvitse tehdä muutoksia, sen ollessa käytännössä mahdotonta. Liian monta laitetta joita ei voi päivittää. Kuten useimmissa tämän päivän toteutuksissa tietoturva on tärkeä osa liikkuvuudenhallintaa, niin käyttäjän kuin palveluntarjoajankin näkökulmasta. Tutkimuksen tarkoituksena on toteutttaa puhtaasti IPv6- ja PMIPv6-protokollaa käyttävä verkko, jolla voidaan tehokkaasti hallita liikkuvan käyttäjän mobiililaitteen palveluita ja yhteyttä verkkoon.

1.2 Toisten tutkimuksia aihealueelta

Yonsein yliopistossa tehdyssä tutkimuksessa (Kim ja Lee 2009) ehdotettiin kuormantasausjärjestelmää PMIPv6-pohjaisiin langattomiin verkkoihin . Tutkimuksessa tieto kuormituksista kerättiin jokaiselta mobiiliyhdyskäytävältä ja kuormantasaus suoritettiin, kun kuormitus ylitti asetetun kynnysarvon. Mobiililaite lähettää mittausraportin mobiiliyhdyskäytävälle, joka sisältää mobiililaitteen tunnisteen, rajapinnan tunnisteen, uuden liitäntäpisteen tunnisteen ja vastaanotetun signaalin vahvuuden. Jos mobiiliyhdyskäytävä vastaanottaa kuormantasauspyynnön mobiililiitokselta tai sen kuorma ylittää kynnyksen, kuormitettu mobiiliyhdyskäytävä valitsee sopivan mobiililaitteen yhteydensiirrolle (Handover Mobile Node, HMN), joka sijaitsee kahden päällekkäin menevän verkon alueella. Kuormitettu mobiiliyhdyskäytävä saa kuormitustietoa sopivilta ehdokkailta vaihtamalla yhteydensiirron aloitus- (Handover Initiate) ja yhteydensiirronkuittausviestit (Handover Acknowledgement).

Kuormitettu mobiiliyhdyskäytävä päättää sopivan mobiiliyhdyskäytävän valinnasta mobiililaitteen yhteydensiirrolle, vastaanotetun signaalin vahvuuden mobiililaitteen ja liitäntäpisteen välillä sekä mobiiliyhdyskäytävä ehdokkaan kuormituksen perusteella. Tämän jälkeen kuormitettu mobiiliyhdyskäytävä lähettää yhteydensiirtokäskyn (Handover Command) mobiililaitteelle, joka luo vastaanotettuaan yhteydensiirtokäskyn yhteyden kohdeverkkoon. Kohdeverkon mobiiliyhdyskäytävä ilmoittaa sidospäivityksellä mobiililiitokselle mobiililaitteen yhteydensiirrosta kahden rajapinnan välillä. Vastaanotettuaan sidospäivityksen mobiililiitos päivittää sidosvälimuistin viittaukset mobiililaitteen rajapinnantunnisteella, liitäntätavalla ja lähettää sidoskuittauksen, joka sisältää kotiverkon etuliitteen, kohdeverkon mobiiliyhdyskäytävälle. Kyseinen järjestely siirtää mobiililaitteen sidoksen ja vähentää palvelevan mo-

biiliyhdyskäytävän kuormaa ennen kuin se ylikuormittuu. Huomioitavaa on kuitenkin, että jatkuva signalointi sopivia yhdyskäytävä ehdokkaita etsiessä rasittaa verkkoa sekä kuormantasausmenettelyä käyttäessä niin sanottu ping-pong ilmiö voi ilmetä, jos myös kohdemobiiliyhdyskäytävä on ylikuormittumassa.(Kim ja Lee 2009)

Sungkyunkwan yliopistossa tehdyssä tutkimuksessa (Kong, Jang ja Choo 2010) tutkittiin tehokasta mobiiliyhdyskäytävän kuormantasausta PMIPv6-domainissa, vertailukohtana esiintyi aiemmin mainittu Yonsein yliopistossa tehty tutkimus. Tutkimuksen ideana on esittää kuormantasausjärjestelmä, joka tietyin väliajoin vaihtaa mobiiliyhdyskäytävien kuormitustietoja PMIPv6-domainissa. Mobiiliyhdyskäytävien kuormitustietoihin nojaten mobiiliyhdyskäytävät kokoavat ja ylläpitävät listaa kuormantasaukseen soveltuvista mobiiliyhdyskäytävistä. Kyseistä listaa käytetään mobiililaitteen liittymisprosessissa ja kuormantasauksessa, joka tulee käyttöön kun palveleva mobiiliyhdyskäytävä ylittää asetetun kynnysarvon. Kuormantasaus suoritetaan mobiililaitteen yhteydensiirrolla, kuormitetusta mobiiliyhdyskäytävästä toiseen. Valituissa mobiililaitteissa, joilla yhteydensiirto suoritetaan, on useita rajapintoja.

Tieto mobiiliyhdyskäytävien kuormituksesta liitetään sykeviestiin (Heartbeat Message), joka on liikkuvuuden ylätunniste (Mobility Header, protokollan tyyppiä 135) ja sitä lähetetään määritetyin väliajoin (Devarapalli et al. 2010). Koska sykeviestit vaihdetaan kaikkien verkonyksiköiden välillä, niiden jatkaminen mahdollistaa mobiiliyhdyskäytävien kerätä tietoa muista mobiiliyhdyskäytävistä, joista lista kuormantasaukseen soveltuvista mobiliiliyhdyskäytävistä kootaan. Mobiililaitteen yhdistäessä PMIPv6-domainiin, mobiiliyhdyskäytävä havaitsee liittymisen ja valitsee sille vähiten kuormitetun mobiiliyhdyskäytävän jo kootun listan perusteella. Palveleva mobiiliyhdyskäytävä lähettää yhteydensiirtokäskyn, joka sisältää uuden liitäntäpisteen (Access Point, AP) tai langattoman verkon yksillöllisen tunnisteen, joka ei sisällä liitäntäpistettä (Basic Service Set Identification, BSSID) sekä kohde mobiiliyhdyskäytävän tiedot. Tämän jälkeen mobiililaite perustaa uuden siirtokerrosyhteyden kohdemobiiliyhdyskäytävän kanssa, jonka jälkeen kohdemobiiliyhdyskäytävä lähettää sidospäivityksen mobiililiitokselle uudesta mobiililaitteen sidoksesta. Mobiililiitoksen päivitettyä sidosvälimuistin viittaukset se vastaa mobiiliyhdyskäytävälle sidoskuittauksella, joka sisältää mobiililaitteen kotiverkon etuliitteen.(Kong, Jang ja Choo 2010)

Kuormituksentasaustarpeen ilmetessä mobiiliyhdyskäytävä valitsee sopivan mobiililaitteen yhteydensiirrolle, joka vaihtaa liitäntää mobiiliyhdyskäytävästä toiseen. Valitun mobiililaitteen valintaan vaikuttaa senhetkisen siirron nopeus ja liitettävyys muihin mobiiliyhdyskäytäviin. Mobiiliyhdyskäytävä valitsee istuntoa kuormittavan mobiililaitteen muttei kuitenkaan mobiililaitetta, jolla on reaaliaikainen palveluistunto meneillään, jottei reaaliaikainen palvelu häiriinny yhteydensiirron tuottaman viiveen takia. Tieto reaaliaikaisesta palveluistunnosta saadaan tutkimalla mobiililaitteen IPv6 paketin ”Traffic Class” tai ”Flow Label” kenttää. Jos mobiiliyhdyskäytävässä, mobiililaitteen yhteydensiirron jälkeenkin ilmenee vielä kuormantasauksen tarvetta, toistetaan toimenpide kunnes kuormitus alittaa asetetun kynnysarvon. Kyseisessä tapauksessa palvelevan mobiiliyhdyskäytävän kuormantasaus kestää kauan ja sen lisäksi verkon liikenne kasvaa kuormantasauksen signalointiviestin takia. Siksi esitetyssä kuormantasausjärjestelmässä palveleva mobiiliyhdyskäytävä valitsee useampia mobiililaitteita yhteydensiirtoa varten silloin, kun kuormitus ylittää mobiiliyhdyskäytävälle asetetun kynnysarvon. Tällä hetkellä valitut mobiililaitteet tulevat olla kytkeytyneenä samaan mobiiliyhdyskäytävään. (Kong, Jang ja Choo 2010)

Aveiron yliopistossa tehdyssä pro gradu —työssä (Filipe ja Santos 2011) tutkittiin paikallista liikkuvuudenhallinnan implementointia PMIPv6-protokollan avulla. Tutkimuksessa käytettiin AMazING (Advanced Mobile wireless Network playGround[1]) testiympäristöä, joka sijaitsee IT Aveiron katolla. Rakennetun testiympäristön suorituskykyä mitattiin ja saatujen mittaustulosten perusteella tehtiin päätelmät testiympäristössä käytetyn protokollan eduista. Lisäksi esiteltiin ratkaisu avoimen lähdekoodin IEEE 802.21 implementaatioille, mediariippumattomalle liikkuvuuden havainnoille ja saumattomalle yhteydensiirrolle. Testiympäristö koostui 24 verkkosolmusta, jotka oli sijoitettu kiinteästi ja kuvastivat tarpeen mukaan mobiililaitetta tai mobiiliyhdyskäytävää, joilla kaikilla oli oma yksilöllinen IPv6-osoite sekä langattoman verkon tunniste, joka sisältää verkon liitäntäpisteen (Extended Service Set Identification, ESSID). Jäljitelläkseen liikkuvuutta verkossa, verkon liitäntäpisteen vaihto tehtiin yhdistämällä manuaalisesti eri tukiasemiin, joka kuvasti yhteydensiirtoa mobiiliyhdyskäytävään. Mittauksen pääpaino oli tehokkuudessa, erityisesti verkonvaihdon latenssissa, käsittelyn eri vaiheissa ja resurssien käytössä. Tutkimuksessa huomattiin, että mobiililiitos kykenee palvelemaan keskimäärin viittä (5) mobiiliyhdyskäytävää samalla prosessorin käytöllä kuin

[1] http://amazing.atnog.av.it.pt/

palveltaessa yhtä (1) mobiiliyhdyskäytävää. Yhteydensiirtoon kuluva aika oli keskimäärin 4,12 millisekuntia. (Filipe ja Santos 2011)

1.3 Tutkielman rakenne

Pro gradu -tutkielma alkaa johdannolla, jossa tuodaan esille aihetta läheisesti koskevia tutkimuksia sekä tutkimusongelma ja kerrotaan hankkeesta, johon tutkimus liittyy. Seuraavassa luvussa käsitellään liikkuvuudenhallintaa IP-verkoissa sekä erilaisia liikkuvuudenhallintaprotokollia. Tämän jälkeen esitellään ensiksi Mobile IPv6- (MIPv6) ja sen jälkeen PMIPv6-testiympäristö. Ennen lopullista yhteenvetoa tarkastellaan liikkuvuudenhallinnan nykyhetkeä sekä sitä, kuinka se tulevaisuudessa kehittyy.

2 Liikkuvuudenhallinta IP-verkoissa

Tässä luvussa esitellään ensimmäiseksi 3GPP:n EPC:n ydinverkkoarkkitehtuurin kehitysaskeleet siihen, kuinka päädyttiin pakettikytkin arkkitehtuuriin, IPv6-protokollaan palveluiden kuljettamisessa ja mistä Evolved Packet System (EPS) arkkitehtuuri koostuu. Seuraavaksi käydään lyhyesti läpi IPv6-protokollan osoitteiden muodostaminen sekä eri osoitteiden käyttötarkoitukset. Kolmannessa kappaleessa esitellään liikkuvuudenhallintaprotokollista seuraavat:

- Mobile IPv4 (MIPv4)
- Mobile IPv6 (MIPv6)
- Mobile IPv6 Fast Handovers (FMIPv6)
- Hierarchial Mobile IPv6 (HMIPv6)
- Proxy Mobile IPv6 (PMIPv6)
- Fast handovers for Proxy Mobile IPv6 (FPMIPv6)
- Host Identity Protocol (HIP)
- Network Mobility Protocol (NEMO)

  Lisäksi lopussa esitellään Network-Based Mobility Extensions -työryhmä, joka kehittää aktiivisesti verkkopohjaisia liikkuvuuslaajennuksia.

Viimeisessä tämän luvun kappaleessa käydään läpi sitä, mitä MIPv6- ja PMIPv6-protokolliin suositelluista tietoturva menettelyistä tapahtuu ja mitä nissä suojataan.

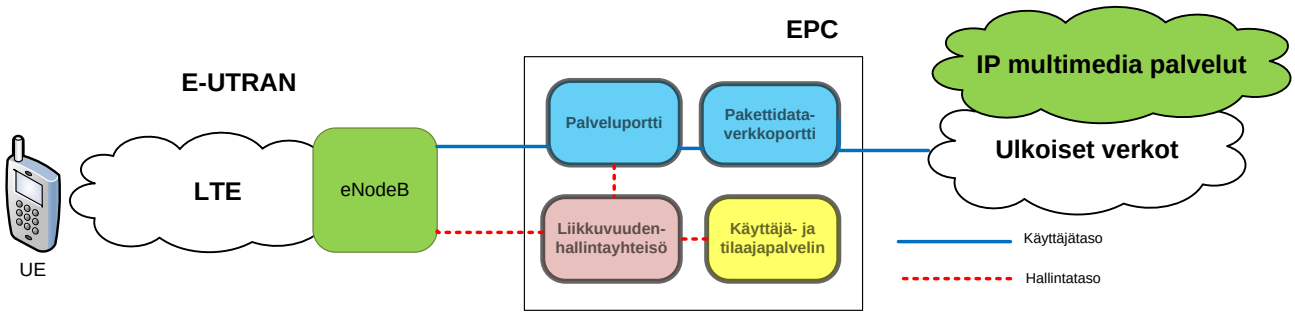
IP-verkot suunniteltiin paikallaan pysyville laitteille, jotka tunnistetaan IP-osoitteen avulla, joka toimi tunnisteen lisäksi myös sijaintina. Reitittimet käyttävät sijaintia hyväksi toimittaessaan datagrammeja. Mobiililaite on verkossa sijaitseva laite tai solmu, joka vaihtaa topologista sijaintiaan tai liitäntäpistettä verkossa. Jotta yhteyden säilyttäminen liikkuessa olisi mahdollista, mobiililaitteen tulee kyetä tarvittaessa vaihtamaan IP-osoite laitteen vaihtaessa verkon liitäntäpistettä. Jotta yhteyden muodostus mobiililaitteeseen olisi mahdollista, verkossa sijaitsevien laitteiden tulee päivittää mobiililaitteen uuden sijainnin osoite. Mobiililaite ei kykene säilyttämään yhteyttä siirtokerroksen eikä ylempien kerroksien sijainnin muuttuessa. Tämä tuottaa ongelmia yhteyksille, kuten puheelle, jotka vaativat jatkuvan yhteyden. Toi-

nen ongelma on verkossa liikkuvien pakettien hävikki sekä yhteydensiirrosta johtuva viive. Näiden ongelmien minimoiminen on erityisen tärkeää käyttömukavuuden kannalta. Tämän päivän verkkolaitteissa on useita eri teknologioiden rajapintoja, joiden avulla yhteyden muodostaminen verkkoon on mahdollista. Laitteessa riippuen se voi käyttää yhteyden muodostamiseen ja sen ylläpitämiseen yhtä tai useampaa rajapintaa. Useiden eri verkkojen ollessa saatavilla yhtäaikaisesti, niin olisi suotavaa yhteyden muodostuvan parhaaseen mahdolliseen, tiettyjen ennalta määrättyjen sääntöjen puitteissa. (Fekete 2012, s. 19)

2.1 Evolved Packet Core

EPC on 3GPP:n ydinverkkoarkkitehtuurin uusin kehitysaskel. Global System for Mobile Communications (GSM) -teknologia käytti piirikytkimiä, jotka olivat suoraan toisiinsa yhteydessä. GSM-teknologiassa kaikki palvelut kuljetettiin piirikytkimien yli puhelinyhteysperiaatteella, poislukien SMS-viestit ja dataliikenne. General Packet Radio Service (GPRS)-teknologia käytti piirikytkimien lisäksi pakettikytkimiä, jonka avulla se kuljetti datan paketeissa ilman piirien apua. GPRS-teknologiassa piirit kuljettivat puheen ja usein myös SMS-viestit. Universal Mobile Telecommunications System (UMTS, 3G) -teknologiassa ydinverkkoarkkitehtuuri on pysynyt samana ja osa verkkoelementeistä on kehittynyt, mutta käsite on pysynyt verrattain samana. IPv6-tuki on tullut 3GPP Release 99:ssä ja IPv6 on spesifioitu ainoaksi tuetuksi IP versioksi alkaen Release 5:st ä.(Firmin 2008) (Arkko et al. 2003)

3G-teknologian kehittämisessä 3GPP yksikkö päätti käyttää Internet Protokollaa (IP) pääprotokollana palveluiden kuljettamisessa. Luovuttiin piirikytkin domainin käytöstä ja päätettiin EPC kehityksen suuntautuvan GRPS/UMTS-teknologioissa käytettyyn pakettikytkinarkkitehturiin. Perinteisten piirien tilalle, joita käytetään puheen ja viestien kuljettamiseen, tulee IP-teknologiaan pohjautuva all-IP ratkaisu, joka yksinkertaisti arkkitehtuuria. EPC arkkitehtuurin ajatus oli käsitellä dataliikennettä tehokkaasti suorituskyvyn ja kustannuksien näkökulmasta. Vain muutama verkkolaite käsittelee liikennettä ja protokollien muutoksia pyritään välttämään. Päätettiin myös erottaa käyttäjätaso (käyttäjien data) sekä hallintataso (signalointi), jotta niiden itsenäinen käsittely olisi mahdollista. Erotuksen ansiosta operaattorit kykenevät suhteuttamaan ja sovittamaan tasojen liikenteen helposti.



Kuvio 1: Yksinkertainen EPS arkkitehtuuri E-UTRAN yhteydellä(Firmin 2008)

Kuvassa 1 näkyy EPS arkkitehtuuri, missä käyttäjä on yhdistetty EPC:n E-UTRAN:n (Long Term Evolution, LTE liitäntäverkko) kautta ja Evolved NodeB (eNodeB) on LTE-lähettimen tukiasema. 3GPP määrittelee tuen useille eri siirtotekniikoille sekä yhteydensiirron näiden välillä. 3GPP:n aikaisemmin määrittelemät verkkoarkkitehtuurit sekä useat muiden määrittelemät teknologiat (esimerkikisi WiMAX, WLAN, CDMA2000) on tuettu käyttäjän yhdistämisessä EPC:n. Operaattorin tehtäväksi jää määrittää, mitkä ei-3GPP:n teknologioista ovat luotettuja ja mitkä eivät. Luotetut teknologiat voivat olla suoraan yhteydessä EPC:n, kun taas ei-luotetut teknologiat yhdistävät EPC:n ePakettidataportin (Evolved Packet Data Gateway, ePDG) verkkoyksikön kautta. ePakettidataportin pääasiallinen tehtävä on luoda turvallinen yhteys käyttäjän laitteen ja ei-luotetun yhteyden yli.(Firmin 2008) Kuvan 1 EPS koostuu neljästä verkkoelementistä:

Käyttäjä- ja tilaajapalvelin (Home Subscriber Server)

on tietokanta, joka sisältää käyttäjään ja tilaajaan liittyviä tietoja. Se myös tuottaa liikkuvuudenhallintaan soveltuvia toimintoja, puhelujen ja istuntojen asetuksia, käyttäjäntunnistautumista sekä pääsynvalvontaa.

Palveluportti (Serving Gateway)

käsittelee käyttäjätasoa, kuten pakettidataverkkoporttikin. Ne kuljettavat IP-dataliikenteen loppukäyttäjän laitteen (User Equipment, UE) ja ulkoisten verkkojen välillä. Palveluportti on yhteyspiste lähettimelle ja EPC:lle, joka reitittää käyttäjän laitteelle saapuvat ja siltä lähtevät IP-paketit. Palveluportti on sisäisen LTE-verkon ja muiden LTE- sekä 3GPP tekniikoiden liitospiste.

Pakettidataverkkoportti (Packet Data Network Gateway)

toimii yhdyspisteenä EPC:n ja ulkoisten verkkojen kanssa. Näitä verkkoja kutsutaan

pakettidataverkoiksi. Pakettidataverkkoportti reitittää saapuvat ja lähtevät paketit pakettidataverkkoon. Se myös muun muassa jakaa IP-osoitteita/IP-verkkomaskeja tai säädöstenhallintaa ja muokkausta. 3GPP määrittää portit erikseen mutta käytännössä ne voivat sijaita samassa laitteessa.

Liikkuvuudenhallintayksikkö (Mobility Management Entity)

käsittelee hallintasoa, joka kattaa liikkuvuuteen ja E-UTRAN:n yhteyden turvallisuuteen liittyvät signaloinnit.

2.2 IP versio 6

IPv6 on IP versio 4 (IPv4) seuraaja. Erot protokollien välillä jakautuvat pääasiassa seuraaviin luokkiin:

Osoitteiden laajennetut ominaisuudet:

IPv6 kasvattaa IP-osoitteen kokoa 32 bitistä 128 bittiin tukeakseen useampia osoitteiden hiearkiatasoja, huomattavasti suuremman määrän verkko-osoitteita ja yksinkertaisempaa osoitteiden muodostamista. Multicast reitityksien skaalautuvuus paranee multicast-osoitteiden tunnisteeseen lisätyllä *Raja (Scope)* -tarkenteella, joka näkyy taulukossa 1. Uuden tyyppinen osoite nimeltään *Anycast* määritellään, jonka avulla lähetetään paketti kenelle vain ryhmään kuuluvista laitteista.

Ylätunnisteen muotoilun yksinkertaistaminen:

Osa IPv4-ylätunnisteiden kentistä on poistettu tai asetettu valinnaiseksi. Tällä tavoin vähennetään äkseen tavallisia paketin käsitellykustannuksia sekä rajoitetaan IPv6-ylätunnisteen kaistan käyttöä.

Paranneltu tuki laajennuksille ja vaihtoehdoille:

Muutos IP-ylätunnisteen koodaukselle, joka mahdollistaa tehokkaamman eteenpäin lähettämisen, lievemmät rajoitukset pituuden määritelylle sekä paremman joustavuuden uusille tulevaisuuden vaihtoehdoille.

Tietovirran merkitseminen:

Mahdollisuus merkitä paketteja tietyistä tietovirroista, joista lähettäjä vaatii erityiskäsittelyä, kuten epätavallista palvelun laatua tai reaaliaikaista palvelua.(Deering ja Hinden 1998) (Postel 1981)

Multicast -osoitteen Raja-tarkenne	
Arvo	**Raja**
1	Solmu-paikallinen (Node-local)
2	Yhteys-paikallinen (Link-local)
8	Organisaation-paikallinen (Organizational-local)
E	Maailmanlaajuinen (Global)

Taulukko 1: Multicast -osoitteen tunnisteen Raja -tarkenteet (MSDN 2010)

Kaikki IPv6-osoitteet määritellään rajapinnoille, ei laitteille. Jokaisella rajapinnalla tulee vähintään olla yksittäinen unicast paikallisoite. IPv6-osoite koostuu kahdeksasta 16 bitin palasesta, jotka ilmoitetaan heksadesimaaleina. Kuvissa 2, 3 ja 4 näkyy unicast-osoitteiden yleiset muodot ja kuvassa 5 näkyy anycast-osoitteen yleinen muoto. IPv6-osoitteet ovat 128 bittisiä rajapintojen tunnisteita, joita on olemassa kolmea eri tyyppiä:

Unicast
: on rajapinnan tunniste. Unicast -osoitteeseen lähetettävä paketti toimitetaan kyseisen osoitteen omistavalle rajapinnalle.

Anycast
: on usein useiden eri laitteiden/solmujen rajapintojen sarja. Anycast-osoitteeseen lähetettävä paketti toimitetaan kyseisen osoitteen lähimmäksi tunnistavalle rajapinnalle (reititysprotokollan mukaisesti mittana etäisyys). Anycast-osoitetta ei saa käyttää IPv6-paketin lähdeosoitteena ja sen saa määrätä vain IPv6-reitittimelle, ei isännälle.

Multicast
: on usein useiden eri laitteiden/solmujen rajapintojen sarja. Multicast-osoitteeseen lähetettävä paketti toimitetaan kaikille kyseiseen osoiteavaruuteen kuuluville rajapinnoille.

IPv6-protokollassa ei ole IPv4-protokollasta tuttuja broadcast-osoitteita, jonka toiminnon multicast-osoitteet korvaavat. Multicast-osoitteen yleinen muoto on esitetty kuvassa 6. IPv6-osoitteiston arkkitehtuuri mahdollistaa useiden unicast-osoitteiden käytön rajapinnoilla. Kyseiset osoitteet voivat olla julkisia, yksittäisiä tai tietyn osoiteavaruuden paikallisosoitteita, jonka paketteja reitittimet eivät reititä silloin, kun lähteenä on paikallisosoite tai määränpäänä osoiteavaruuden ulkopuolella sijaitseva osoite. Kyseiset osoitteet voivat olla suositeltuja

tai vanhentuneita.

n bittiä	m bittiä	128-n-m bittiä
Julkinen reititys osoiteavaruus	Aliverkontunniste	Rajapinnantunniste

Kuvio 2: Julkisen Unicast-osoittteen yleinen muoto

10 bittiä	54 bittiä	64 bittiä
1111111010	0	Rajapinnantunniste

Kuvio 3: Yksittäisen Unicast-osoitteen yleinen muoto

10 bittiä	54 bittiä	64 bittiä
1111111011	Aliverkontunniste	Rajapinnantunniste

Kuvio 4: Tietyn osoiteavaruuden Unicast-osoitteen yleinen muoto

n bittiä	128-n bittiä
Aliverkontunniste	00000000000000

Kuvio 5: Anycast-osoitteen yleinen muoto

8 bittiä	4 bittiä	4 bittiä	112 bittiä
11111111	Asetus 0 0 0 T	Alue	Ryhmätunniste

Asetus koostuu neljästä tilasta:
Ensimmäiset kolme tilaa on varattu ja ne tulee olla asetettu nollaksi.
T=0 ilmaisee pysyvästi määrättyä Multicast-osoitetta, jonka IANA on määrännyt.
T=1 ilmaisee väliaikaisesti määrättyä Multicast-osoitetta

Alueen arvot ovat:
0 varattu
1 rajapinnan paikallisalue
2 yhteyden paikallisalue
3 varattu
4 hallinnon paikallisalue
5 osoitenavaruuden paikallisalue
6 vapaana
7 vapaana
8 organisaation paikallisalue
9 vapaana
A vapaana
B vapaana
C vapaana
C vapaana
D vapaana
E julkinen alue
F varattu
Arvolla rajoitetaan Multicast-ryhmän toiminta-aluetta.

Kuvio 6: Multicast-osoitteen yleinen muoto

Huoli yksityisyydestä on tuonut esille käsitteet julkiset osoitteet ja väliaikaiset osoitteet. Liikkuvuuden arkkitehtuuri esittelee käsitteet kotiosoite (Home Address, HoA) ja vierasosoite (Care of Address, CoA). IPv6-protokollan tuki liittyä verkkoon useamman yhteyden kautta mahdollistaa tilanteeet, joissa mobiililaitteella on useita eri osoitteita. Kyseinen skenaario tuo haasteita IPv6-implementointien toteuttamiseen, koska niissä on usein useita mahdollisia lähde- ja määränpääosoitteita yhteyttä muodostettaessa. Tästä syystä on suositeltavaa käyttää oletusalgoritmeja, jotka ovat yhteisiä eri toteutusten kanssa. Kyseisten algoritmien avulla lähde- ja määränpääosoitteet valitaan, jotta kehittäjät ja ylläpitäjät kykynevät ymmärtämään ja ennakoimaan järjestelmien toimintaa. (Hinden ja Deering 2003) (Draves 2003)

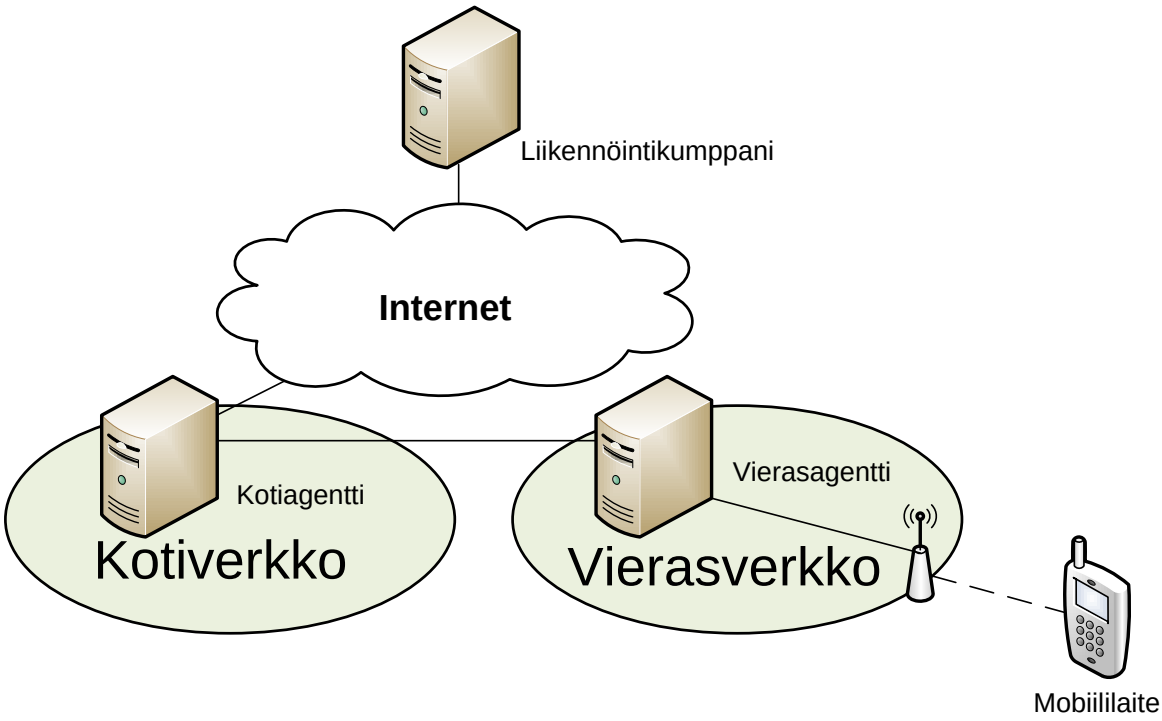
2.3 Liikkuvuudenhallintaprotokollat

Liikkuvuudenhallintaprotokollat pyrkivät mahdollistamaan IP-yhteyden toiminnan sekä ylläpitämään ja päivittämään mobiililaitteen sen hetkistä sijaintia. On olemassa useita keinoja sekä protokollia liikkuvan yhteyden muodostamiseen ja ylläpitoon IP-verkoissa. Mobile IP (MIP) mahdollistaa tiedonsiirron mobiililaitteiden (Mobile Node, MN), kuten kannettavien sekä kännyköiden, välillä. Kyseinen protokolla mahdollistaa mobiililaitteiden siirtymisen vieraaseen verkkoon, jonka jälkeenkin on mahdollista olla yhteydessä mobiililaitteeseen kotiverkosta saadulla osoitteella. MIP-protokolla mahdollistaa mobiililaitteen siirtymisen yhteydestä toiseen ilman, että mobiililaitteen kotiosoite muuttuu. Paketit reititetään mobiililaitteelle kyseistä osoitetta hyväksikäyttäen mobiililaitteen sijaitessa toisessa verkossa. Mobiililaite kykenee myös jatkamaan yhteyttä muihin laitteisiin yhteydensiirron jälkeen. Mobiililaitteen yhteyden muutos ei näy siirtokerroksen eikä ylempien kerrosten protokollille tai sovelluksille. (Mäkelä 2011, s. 31)

2.3.1 Mobile IPv4

MIP-protokollista molemmat, MIPv4 ja MIPv6, toimivat ja perustuvat kotiverkossa sijaitsevan kotiagentin (Home Agent, HA) toimintaan. Kotiagentti on kotiverkossa sijaitseva laite, joka on aina tietoinen mobiiliaitteen senhetkisestä sijainnista. Kotiverkko määrittää ensisijaisen IP-osoitteen, jota mobiililaite käyttää yhteydenpitoon ja joka toimii mobiililaitteen kotiosoitteena. Mobiililaitteen siirtyessä ja yhdistyessä uuteen verkkoon se tarvitsee

tavan yhteydenpitoon kyseisessä verkossa. MIPv4-prokotokolla ottaa käyttöön uuden vierasosoitteen, jonka se saa käyttämällä esimerkiksi Dynamic Host Configuration Protocol:laa (DHCP). Saamallaan osoitteella mobiililaite kykenee kommunikoimaan uudessa verkossa. Kotiosoitteen topologisen sijainnin ollessa mobiililaitteen kotiverkossa, missä myös kotiagentti sijaitsee, mobiililaitteelle kohdistetut paketit reititetään kotiverkkoon ja kotiagentille, joka lähettää ne tunneloimalla mobiililaitteelle.(Mäkelä 2011, s. 31)



Kuvio 7: MIPv4 Topologia

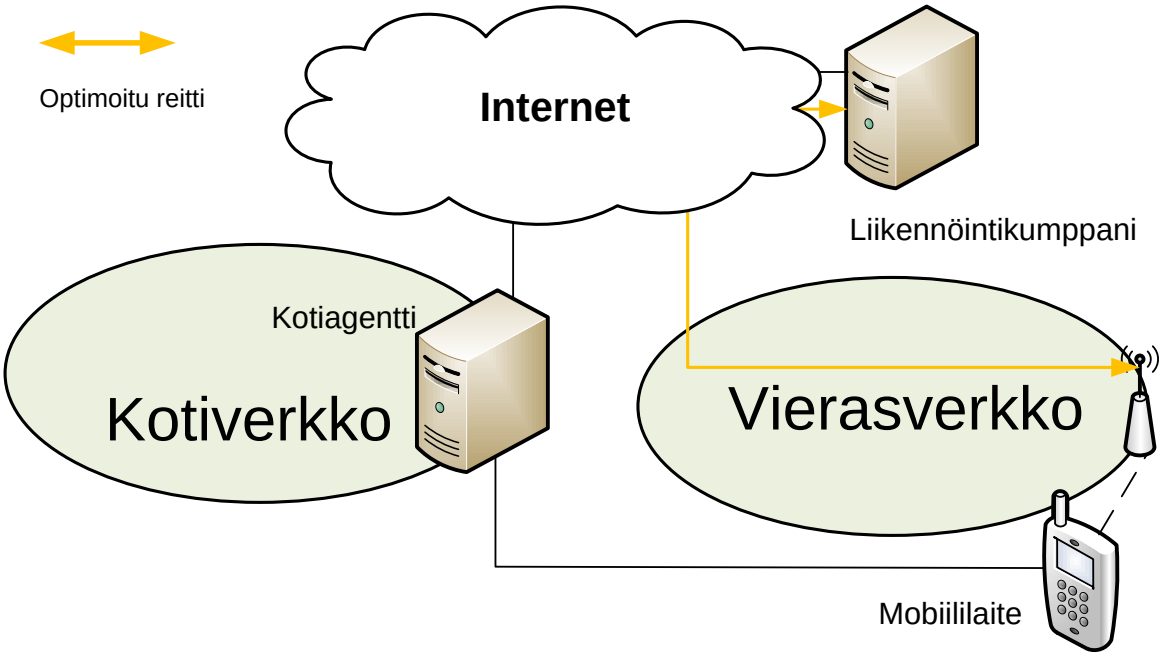
Vieraassa verkossa saattaa myös olla vierasagentteja (Foreign Agent, FA), jotka toimivat porttina mobiililaitteelle. Kuvassa 7 näkyy skenaario MIPv4-topologiasta, jossa mobiililaite on kytkeytynyt vierasverkkoon. Kyseisiä laitteita käytettäessä ei ole tarvetta varata uusia vierasosoitteita jokaiselle mobiililaitteelle, näin mahdollistaen vieraan verkon vapaana olevien IP-osoitteiden mahdollisimman suuren määrän. Kuitenkin vierasagenttia käyttämällä voidaan joutua tilanteeseen, jota kutsutaan kolmoisreititykseksi (Triangular routing). Tämä tapahtuu sen johdosta, että mobiililaite kykenee lähettämään ulosmenevät paketit muille laitteille suoraan käyttämällä vierasagenttia ja samalla vastaanottamaan paketteja kotiagentilta sekä vierasagentilta. Kyseisiä erilaisia reitityspolkuja ulosmenevälle ja sisääntulevalle lii-

kenteelle voidaan välttää käyttämällä käänteistä tunnelointimenetelmää (Reverse tunneling mechanism), jossa kaikki paketit menevät suoraan kotiagentin kautta. (Mäkelä 2011, s. 31)

2.3.2 Mobile IPv6

MIPv6-protokolla hyötyy IPv6:n tuomista hyödyistä sekä MIPv4:sta saaduista kokemuksista. MIPv6 käyttää kotiagenttia ja sijainti päivitetään aina sidospäivitystä (Binding Update, BU) käyttämällä johon kotiagentti vastaa sidoskuittauksella (Binding Acknowledgement, BA). Mobiililaite voi saada vieraaseen verkkoon liittyessä uuden vierasosoitteen käyttämällä IPv6:n lähimmäisen laitteen havannointi- ja osoitteen automaattista konfigurointimekanismia (Neighbor discovery and the address auto-configuration mechanism) eikä se siten tarvitse minkäänlaista tukea vieraan verkon reitittimiltä. MIPv6 ei käytä vierasagentteja, kuten kuvasta 8 ilmenee, jotka toimisivat porttina mobiililaitteelle, jolloin kolmoisreititysongelma ratkeaa käyttämällä reitin optimointimekanismia. Kyseisellä mekanismilla mobiililaite kykenee rekisteröimään nykyisen vierasosoitteen suoraan muiden laitteiden kanssa, mikä mahdollistaa suoran IP-yhteyden kahden laitteen välillä ilman reititystä kotiverkossa sijaitsevan kotiagentin kautta. (Mäkelä 2011, s. 32) (Draves 2003) (A et al. 2005) Samantapainen reitinoptimointimekanismi on mahdollista myös MIPv4:ssa mutta toisin kuin MIPv4:ssa, kyseessä ei ole laajennus protokollaan vaan se on olennainen osa MIPv6:sta. MIPv6 kykenee myös käyttämään reititykseen IPv6:n ylätunnisteita tunneloinnin sijaan, mikä nopeuttaa pakettien lähettämistä.

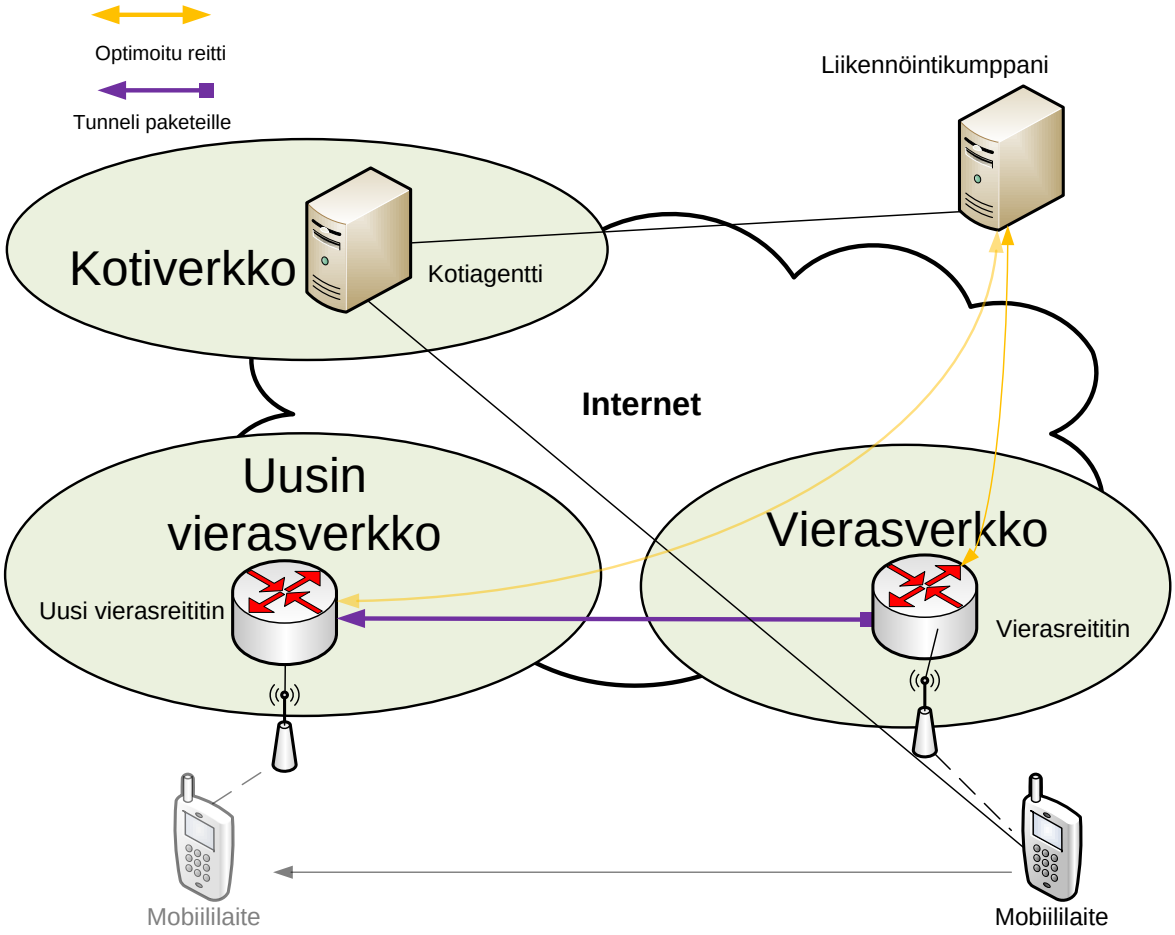
Tukeakseen laitteita, jotka käyttävät IPv4 protokollaa, kehitettiin kaksoispinotuki (Dual stack support). MIPv6:ssa on tuki useammille kotiagenteille ja rajoitettu tuki kotiverkon uudelleenkonfigurointiin. Kyseisissä tapauksissa mobiililaite ei välttämättä tiedä oman kotiagentin IP-osoitetta ja jopa kotiverkon peite voi muuttua ajan saatossa. Mekanismi (Dynamic home agent address discovery, DHAAD) sallii mobiililaitteen dynaamisesti havaita kotiagentin IP-osoitteen liitoksessa silloinkin, kun mobiililaite on poissa kotiverkosta. Mobiililaitteet kykenevät oppimaan uutta tietoa kotiverkon etuliitteiden havainnointimekanismilla (mobile prefix discovery). (Mäkelä 2011, s. 33) (Perkins, Johnson ja Arkko 2011)



Kuvio 8: MIPv6 Topologia

2.3.3 Mobile IPv6 Fast Handovers

FMIPv6-protokollassa reititin, joka sijaitsee vieraassa verkossa, voi toimia mobiililaitteelle välityspalvelimena. Yhteydensiirron tapahtuessa aikaisempi reititin (Previous Access Router, PAR) toimii välityspalvelimena mobiililaitteelle ja käyttää tunnelointia reitittääkseen paketit uudelle reitittimelle (New Access Router, NAR), joka sijaitsee uudessa vieraassa verkossa. FMIPv6-protokolla vähentää yhteydensiirron viivettä MIPv6:ssa sallimalla mobiililaitteen lähettää paketteja heti havaitessaan uuden aliverkon linkin sekä sallii sen vastaanottaa paketteja heti, kun sen kytkeytyminen on havaittu uudessa reitittimessä (Koodli 2009). Kuvassa 9 näkyy miten kahden eri vieraan verkon reittimet luovat tunnelin niiden välille ja optimoivat reitin mobiililaitteelta liikennöintikumppanille. Nopean yhteydensiirron etuna on tuki tiedon reitittämiselle uuteen vieraaseen verkkoon ennen kuin yhteys katkeaa yhteydensiirron takia. Tämä luonnollisesti vähentää pakettien hävikkiä ja edesauttaa sitä, että mobiililaite voi ylläpitää korkeampaa palvelutasoa (Quality of Service level).(Mäkelä 2011, s. 33) (Koodli 2005)

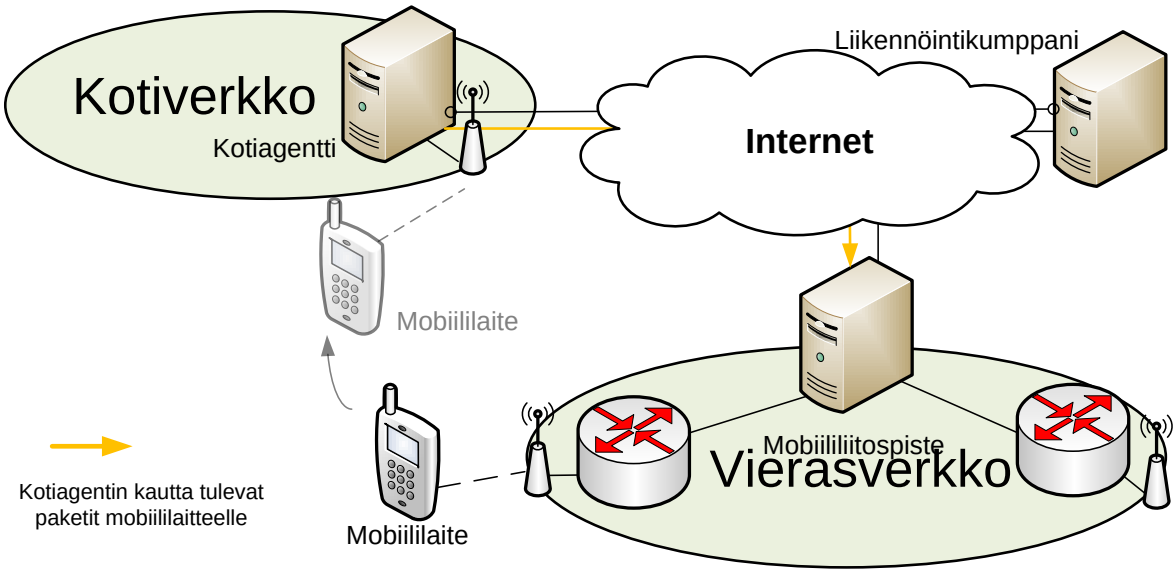


Kuvio 9: FMIPv6 Topologia

2.3.4 Hierarchial Mobile IPv6

HMIPv6-protokolla on lisäys MIPv6-protokollalle. HMIPv6 esittelee uuden yksikön nimeltään mobiililliitospiste (Mobile Anchor Point, MAP), joka toimii paikallisena kotiagenttina mobiililaitteelle. Mobiililaitteen liikkuessa mobiililiitospisteen domainin sisällä, tarvittava signalointi mobiililaitteelta tapahtuu ensimmäisen mobiililiitospisteen kanssa, jonka oletetaan olevan lähempänä kuin itse kotiagentti. Näin tehden signalointiin kuluva aika pienenee ja mobiililiitospiste edesauttaa MIPv6-protokollaa saavuttamaan saumattoman liikkuvuuden. Mobiililiitospiste kykenee vastaanottamaan kaiken mobiililaitteelle suunnatun liikenteen kotiagentilta lähettäen ne eteenpäin mobiililaitteelle. Reitinoptimointi on tuettu ja se voidaan toteuttaa kahdella eri tavalla. Mobiililaite voi optimoida reitin joko suoraan kotiagentin tai mobiililiitoksen kanssa. Jälkimmäisessä tapauksessa liikenteen ei tarvitse mennä kotiagentin

kautta. (Mäkelä 2011, s. 33) (Soliman et al. 2008) Kuvassa 10 näkyy reititystapaukset mobiililaitteelta mobiililiitospisteen kautta liikennöintikumppanille, kun mobiililaite sijaitsee mobiililiitospisteen domainissa. Mobiililaitteen siirtyessä pois mobiililiitospisteen domainista se luo yhteyden kotiverkossa sijaitsevan kotiagentin kautta.

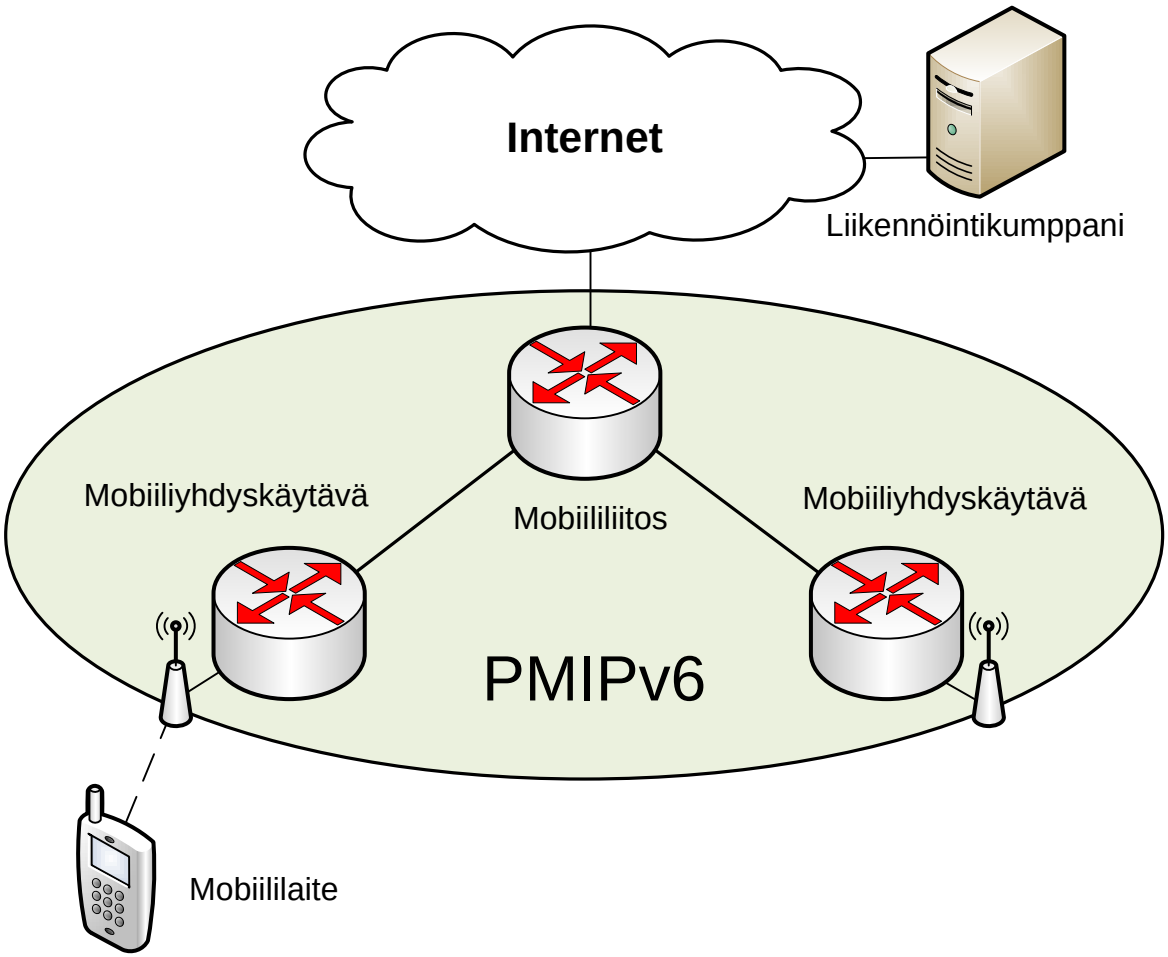


Kuvio 10: HMIPv6 Topologia

2.3.5 Proxy Mobile IPv6

PMIPv6-protokolla on kehitetty tuottamaan tietoverkkoon perustuvaa tukea liikkuvuudelle, joka pyrkii minimoimaan signaloinnin mobiililaitteen ja kotiverkon välillä. Pääajatus on, että verkkoyksiköt (network entities) seuraavat mobiililaitteen liikettä ja aloittavat tarvittavat toimenpiteet yhteydensiirtoa varten ilman, että mobiililaitteen verkkokerroksen signalointiin tarvitsee puuttua. PMIPv6 esittää uuden yksikön nimeltään mobiiliyhdyskäytävä (Mobile Access Gateway, MAG), joka havaitsee ja hallinnoi mobiililaitteen liikkuvuutta PMIPv6-domainin alueella. Mobiiliyhdyskäytävä on vastuussa yhteydensiirrosta mobiililaitteen puolesta ja se päivittää mobiililaitteen sijainnin tiedot mobiililiitokseen (Local Mobility Anchor, LMA), joka toimii topologisena liitoskohtana mobiililaitteelle (vertaa MIPv6 kotiagentti). Tietovirrat mobiililaitteelle ja mobiililaitteelta kulkevat mobiililiitoksen kautta, joka reitittää paketit mobiililaitteelle mobiiliyhdyskäytävän kautta, kuten kuvassa 11. Mobiililiitoksella on samat tehtävät kuin kotiagentilla MIPv6:ssa. PMIPv6-domainissa voi olla useita liitos-

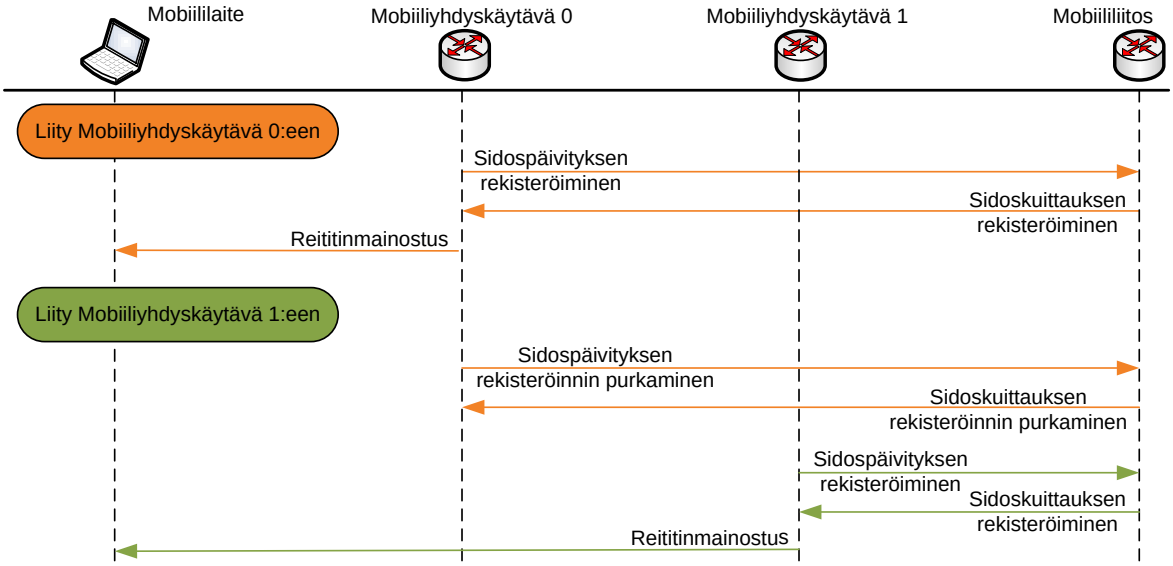
kohtia, jotka ovat vastuussa eri mobiililaiteryhmistä. PMIPv6 tukee IPv4-, IPv6- ja kaksoispinoprotokollia (dual stack IPv4/IPv6) sekä siinä on tuki verkolle, joka on liittynyt verkkoon useamman yhteyden avulla (multihoming). (Mäkelä 2011, s. 34)



Kuvio 11: PMIPv6 Topologia

Kuvassa 12 näkyy PMIPv6-verkon signaloinnin toiminta yksinkertaistettuna (vertaa kuvaan 20). Mobiililaitteen yhdistäessä mobiiliyhdyskäytävään lähettäen samalla mobiililaitteen tunnisteen, kyseinen mobiiliyhdyskäytävä ilmoittaa mobiililiitokselle uudesta sidospäivityksestä (Proxy Binding Update, PBU). Mobiililiitos vastaa sidoskuittauksella (Proxy Binding Acknowledgement, PBA) rekisteröinnin onnistumisesta, jos mobiililaitteen tunniste löytyy mobiililiitoksen tietokannasta, jonka jälkeen mobiiliyhdyskäytävä mainostaa mobiililiitokselta saatua kotiverkon etuliitettä mobiililaitteelle. Mobiililaitteen liikkuessa PMIPv6-domainin alueella ja lähestyttäessä toista mobiiliyhdyskäytävää, aloitetaan liikkuvuudenhallinta purkamalla aikaisempi sidospäivitys vanhan mobiiliyhdyskäytävän ja mobiililiitoksen välillä. Tä-

män jälkeen luodaan aikaisempaan tapaan uusi sidospäivitys samalle mobiililiitokselle sekä mainostetaan uuden mobiiliyhdyskäytävän toimesta kotiverkon etuliitettä mobiililaitteelle.



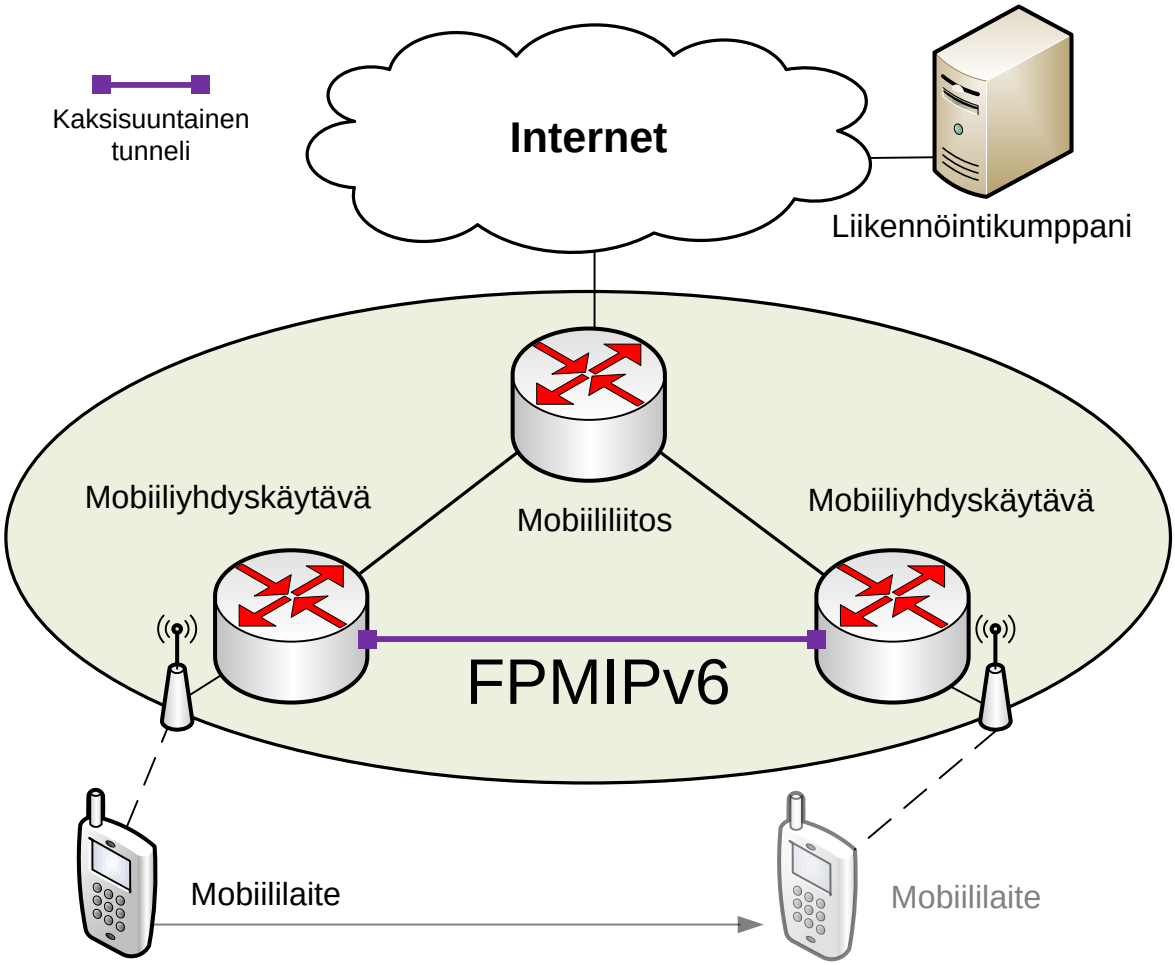
Kuvio 12: PMIPv6 signalointi

2.3.6 Fast handovers for Proxy Mobile IPv6

FPMIPv6 mahdollistaa FMIPv6-protokollan tuen PMIPv6-operaatioille minimoidakseen yhteydensiirron viivettä, pakettien hävikkiä sekä lisätäkseen verkon käyttäjien sisältöä PMIPv6-yhteydensiirtoon. FPMIPv6 käyttää PMIPv6-protokollasta tuttuja yksiköitä ja mobiililiitosta, joka on topologinen liitäntäpiste mobiililaitteen kotiverkon etuliitteille. Lisäksi mobiiliyhdyskäytäviä, jotka toimivat mobiililaitteen reitittiminä suorittaen liikkuvuudenhallinta menettelyt sen puolesta. Siinä tapauksessa, jos mobiiliyhdyskäytäviä kyetään informoimaan ajallaan mobiililaitteen liittymisestä ja/tai irrotautumisesta, on mahdollista optimoida yhteydensiirronmenettely, joka sisältää yhteyden muodostamisen uuteen linkkiin ja signaloinnin mobiiliyhdyskäytävien välillä.

Jotta yhteydensiirron tehokkuutta voitaisiin vielä enemmän parantaa, Internet Engineerin Task Force:n (IETF) dokumentaatio määrittelee kaksisuuntaisen tunnelin aikaisemmin käytetyn mobiiliyhdyskäytävän ja uuden mobiiliyhdyskäytävän välille kuten kuvassa 13. Kaksisuuntaiseen tunneliin lähetetään mobiililaitteelle tarkoitetut paketit. Mahdollistaakseen uuden mobiiliyhdyskäytävän lähettävän sidospäivitys-, yhteydensiirron aloitus- ja yhteyden-

siirronkuittausviestit, jotka on määritelty FMIPv6-standardissa (Koodli 2009), viestejä laajennetaan sisällön siirtämiseen vanhalta mobiiliyhdyskäytävältä, johon sisältyy parametrit, kuten mobiililaitteen verkkotunnus (Network Access Identifier, NAI), kotiverkon etuliite ja IPv4-kotiosoite. Koska mobiililaite ei ole suoranaisesti tekemisissä IP-liikkuvuusprotokollan operaatioiden kanssa, siitä seuraa ettei mobiililaite ole myöskään tekemisissä nopean yhteydensiirtomenetelmän kanssa. Tästä syystä FMIPv6-protokollassa määritetyt viestit, jotka sisältävät mobiililaitteen, eivät ole PMIPv6 toteutuksessa käytössä.(Yukota et al. 2010)

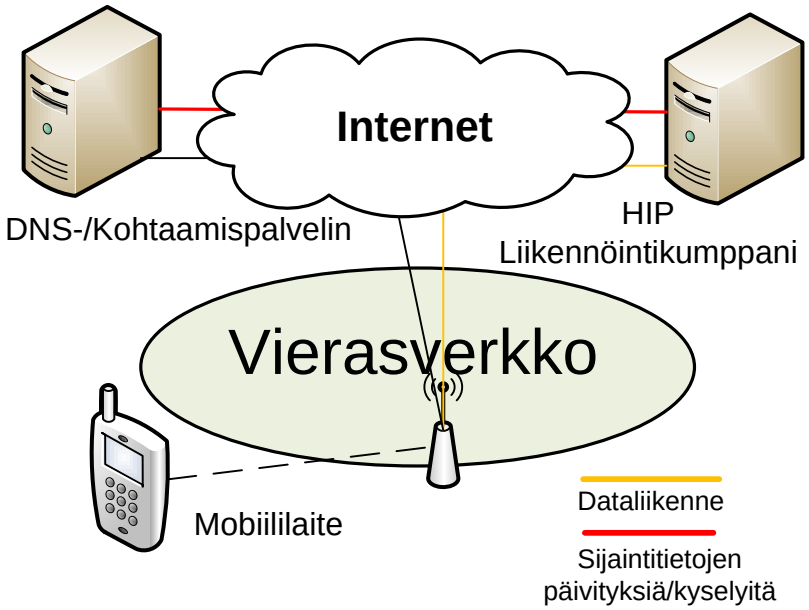


Kuvio 13: FPMIPv6 Topologia

2.3.7 Host Identity Protocol

Isäntätunnisteprotokolla ehdottaa uuden isännäntunnistekerroksen (Host Identity Layer, HIL) verkko- ja kuljetuskerroksen väliin. Kyseisen kerroksen avulla on mahdollista kytkeä kul-

jetusyhteyksiä isäntätunnisteisiin (Host Identifier, HI) IP-osoitteiden sijaan. Isäntätunniste on yksilöllinen julkinen salausavain julkiselle/yksityiselle avainparille. Salausavaimien käyttö on turvallisuuden kulmakivi yhdessä IPsec ESP (IP Security Architecture Encapsulating Security Payload) pakettien kanssa, joita käytetään dataliikenteessä isäntätunnistelaitteiden (Host Identity Protocol Nodes) välillä. Eräs avainmekanismi on isäntätunnisteprotokolla-pohjainen vaihto, jota käytetään kommunikointiin tarkoitettujen isäntätunnisteavainten luomiseen ja vaihtamiseen.



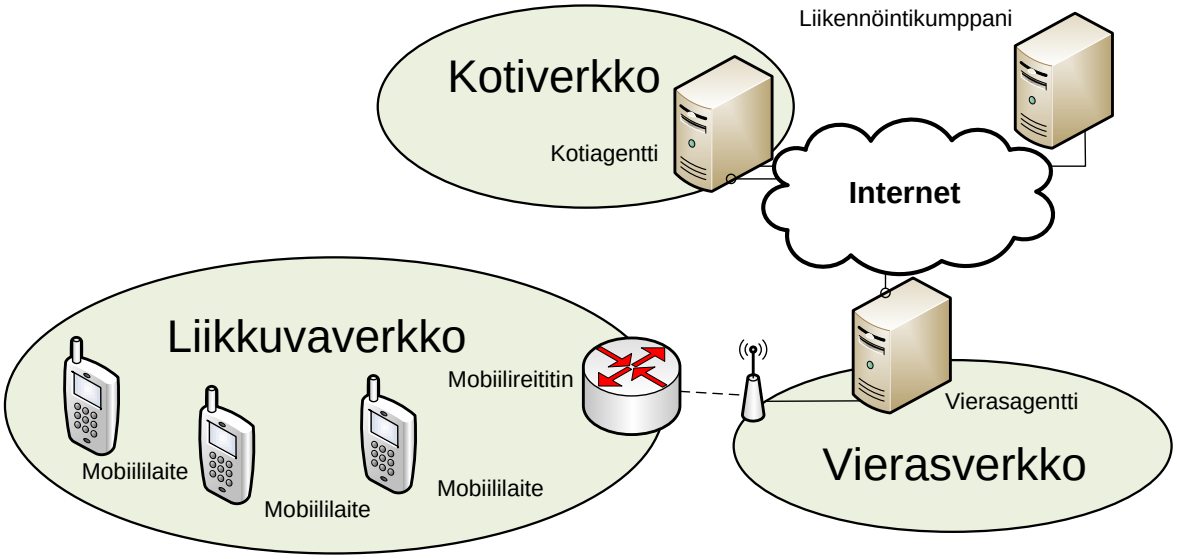
Kuvio 14: HIP Topologia

Sijainnin päivittämiseen HIP-laitteet voivat käyttää DNS- tai erityistä kohtaamispalvelinta (Special Renderzvous Server). Käytännössä tämä tarkoittaa sitä, että isäntätunnistelaitteet pitävät isäntätunnisteisiin kytketyt IP-osoitteensa ajan tasalla kuten kuvassa 14 on esitetty. Isäntätunnisteprotokolla mahdollistaa liikkuvuuden IPv4- ja IPv6-verkkojen välillä ja lisäksi se tukee yhtäaikaisia yhteyksiä. (Mäkelä 2011, s. 35)

2.3.8 Network Mobility Protocol

Koko verkon on mahdollista olla liikkuva. Verkon liikkuvuuden tukea varten on kehitetty verkon liikkuvuusprotokolla . Perusideana on käyttää mobiilireititintä yhdyskäytävänä tarjoamaan internetyhteyttä liikkuvalle verkolle. Kuten kuvasta 15 on nähtävillä, mobiilireititin

on ainoa laite, jonka liitäntäpiste internetiin vaihtuu mobiililaitteiden liitäntäpisteen verkkoon pysyessä samana. Mobiilireititin käyttää NEMO Basic Support Protocol:aa kotiagentin kanssa (Devarapalla et al. 2005). Protokollan tarkoituksena on piilottaa liikkuvuus, jotta muut verkon laitteet näkisivät verkon normaalina lähiverkkona ja mobiilireitittimen oletusyhdyskäytävänä. (Mäkelä 2011)



Kuvio 15: NEMO Topologia

2.3.9 Network-Based Mobility Extensions -työryhmä

Verkkopohjaisten liikkuvuuslaajennusten kehittäminen jatkuu aktiivisena Network-Based Mobility Extensions (netext)[1] -työryhmässä, joka tekee yhteistyötä 3GPP:n EPS:n kanssa. Tästä hyvänä esimerkkinä on IETF:n julkaisema tiedote IPv6-protokollan käytöstä 3GPP:n EPS:ssä. Tiedote käsittelee mobiililaajakaistan internetin sekä muiden datapalveluiden käytön kasvua älypuhelimilla, tableteilla ja kannettavilla tietokoneilla. Tämän seurauksena operaattorit, jotka käyttävät 3GPP:n verkkoarkkitehtuuria joutuvat siirtymään IPv4-osoitteiden loppumisen johdosta IPv6-osoitteisiin. Tiedotteessa kuvataan 3GPP verkkoarkkitehtuurin tuki IPv6-protokollalle. IETF määrittelee joukon työkaluja ja menetelmiä, joiden avulla siirtyminen IPv6-protokollaan onnistuu. Kaksoispinoverkkojen lisäksi siirtymävaiheeseen IPv4-protokollasta IPv6-protokollaan esitetään kaksi vaihtoehtoista menetelmää, jotka ovat kapselointi (encapsulation) ja käännös (translation). IPv6-protokollaan siirtymisen tavoite 3GPP

[1] http://datatracker.ietf.org/wg/netext/

verkoissa on varmistaa, että:

1. Laitteen ja isännät, jotka tukevat vain IPv4-protokollaa, jatkavat IP-yhteyden jakamista internetiin ja palveluihin.
2. Laitteen joissa on kaksoispinotuki kykenevät yhdistämään internetiin joko IPv4- tai IPv6-protokollan kautta. Valinta kumpaa käytetään riippuu:

   (a) käytössä olevasta sovelluksesta
   (b) verkkopalvelun IPv4- ja IPv6-tuesta ja/tai
   (c) palvelimista ja muista verkon päätepisteistä.

(Korhonen, Soininen et al. 2012)

2.4 Tietoturva

MIPv6:n turvallisuus kattaa sidospäivityksien suojauksen kotiagenteille ja liikennöintikumppaneille (Correspondent Node, CN), verkon havainnoinnin suojauksen sekä suojauksen mekanismille, jota MIPv6 käyttää datapakettien kuljettamiseen. Mobiililaitteen ja kotiagentin täytyy käyttää IPsec-suojauskytkentöjä (Security Association, SA) suojatakseen sidospäivityksien ja sidoskuittauksien eheyttä sekä varmennusta. Molempien, mobiililaitteen ja kotiagentin, tulisi tukea ja käyttää pakettivirtojen turvaamiseen tarkoitettua ESP-protokollaa ylätunnisteissa siirtovaiheessa sekä myös käyttää tietoa sisältävien hyötykuormien tunnistamiseen tarkoitettua algoritmia (non-NULL payload authentication algorithm), jolla varmistetaan datan alkuperän varmennus, yhteyden eheys sekä valinnainen suoja toistohyökkäyksiä vastaan (anti-replay protection). Sidospäivityksien eheys ja aitous vastaanottaville laitteille on suojattu käyttämällä syötettyä hash algoritmia (keyed-hash algorithm). Sidoshallinta-avainta (Binding Management Key, Kbm) käytetään avaimena hash algoritmissa. Suojatakseen viestien vaihdon mobiililaitteen ja kotiagentin välillä IPsecillä, tulee luoda tarkoituksenmukaiset viittaukset tietoturvapolitiikassa tietokantoihin. Mobiililaitteen tulee estää käyttämästä omia suojauskytkentäjä sidospäivityksien lähettämisessä toisen mobiililaitteen sijasta käyttäen samaa kotiagenttia. Tämä saavutetaan tarkistamalla kotiagentissa, että annettu kotiosoite täsmää oikean suojauskytkennän kanssa. Kyseinen tarkastus on säädetty IPsec käsittelyssä, tunnistamalla yksiselitteisesti turvallisuuspolitiikka tietokannassa määritellyn yksit-

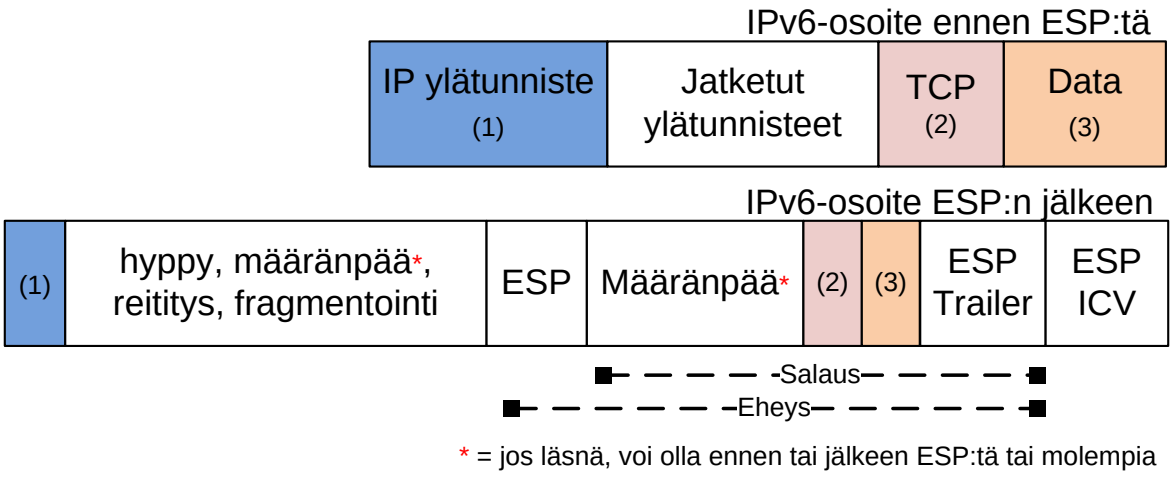
täisen suojauskytkennän suojauksen sidospäivityksiin minkä tahansa annetun kotiosoitteen ja kotiagentin välillä. Jotta tämä olisi mahdollista, on välttämätöntä, että mobiililaitteen kotiosoite on näkyvillä sidospäivityksissä ja kuittauksissa. Kotiosoitetta käytetään näissä paketeissa joko lähteenä tai määränpäänä, Home Address Destination vaihtoehdossa tai tyypin 2 reititys ylätunnisteessa.(Perkins, Johnson ja Arkko 2011) (Gundavelli et al. 2008)

PMIPv6-protokollassa mobiililaite ei osallistu suojauskytkentöjen luomiseen, joilla suojataan signalointiviestit tai sidospäivitykset. Täten mobiililiitoksen tulee rajoittaa sidosten luominen ja hallinnointi erikseen valtuutetuille mobiiliyhdyskäytäville ja osoitteille. Toisin kuin MIPv6-protokollassa, signalointiviestit eivät sisällä kotiosoitteen määränpää vaihtoehtoa tai tyypin 2 reititys ylätunnistetta. Täten valinnat menettelytavoille ja suojauskytkennöille pysyvät samoina, joten IPsec-suojaukset eivät tarvitse lisähuomiota.(Gundavelli et al. 2008)

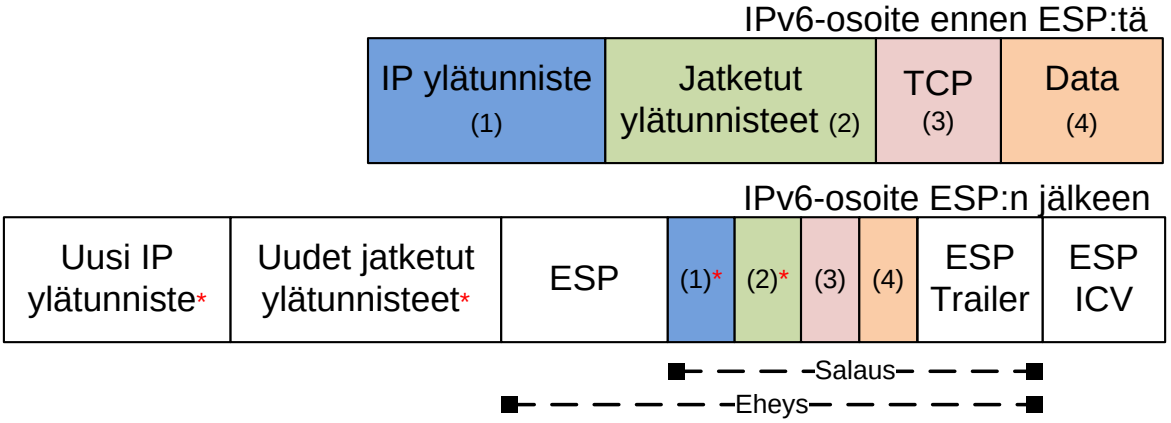
MIPv6:ssa sidospäivitykset suojataan käyttämällä jatkoa IPsec ylätunnisteille (IPsec Extension Headers) tai liitettyä datavarmennusvaihtoehtoa (Binding Authorization Data Option).(Kent ja Seo 2005) Kyseinen vaihtoehto työllistää sidoshallinta-avaimen, joka voidaan määrittää reitityksen palautusproseduurin (Return Routability Procedure) avulla. Mekanismi jota käytetään hyötykuormapakettien kuljettamiseen, kuten kotiosoitteen määränpäävaihtoehtoa ja 2-tyypin reitityksen ylätunnistetta, on spesifioitu siten, että se rajoittaa niiden käyttöä mahdollisissa hyökkäyksissä. Kyseinen menetelmä ei suojaa hyökkääjiltä, jotka ovat kotiverkon ja liikennöintikumppanin välissä. Toisaalta, hyökkääjät pystyvät suorittamaan hyökkäyksiä ilman MIPv6:sta. Suurin hyöty reitityksen palautusproseduurissa on, että se rajoittaa mahdolliset hyökkääjät niihin, joilla on pääsy yhteen tiettyyn reittiin internetissä ja estää väärennettyjen sidospäivityksien vastaanottamisen muualta internetistä.(Perkins, Johnson ja Arkko 2011)

PMIPv6:ssa signalointiviestien, sidospäivityksien ja sidoskuittauksien välitys mobiiliyhdyskäytävän ja mobiililiitoksen välillä tulee suojata päästä päähän käyttäen suojaskytkentöjä, jotka tarjoavat eheyden ja datan alkuperän varmistuksen. Mobiiliyhdyskäytävän ja mobiililiitoksen tulee implementoida IPsec suojatakseen PMIPv6 signalointiviestit. Kuten MIPv6:ssa, IPsec:n käyttö mobiililaitteen tietoliikenteen suojaamiseen on vapaaehtoista. Kuvan 17 IPsec ESP:tä tunnelointitilassa voidaan käyttää mobiililaitteen tunneloidun tietoliikenteen suojaamiseen, jos tietoliikenteen suojaamista vaaditaan. Kuvassa 16 näkyy IPv6 liikenteen suojaa-

minen IPSec ESP:llä kuljetustilassa. (Gundavelli et al. 2008)



Kuvio 16: IPv6 ESP kuljetustilassa(Kent 2005)



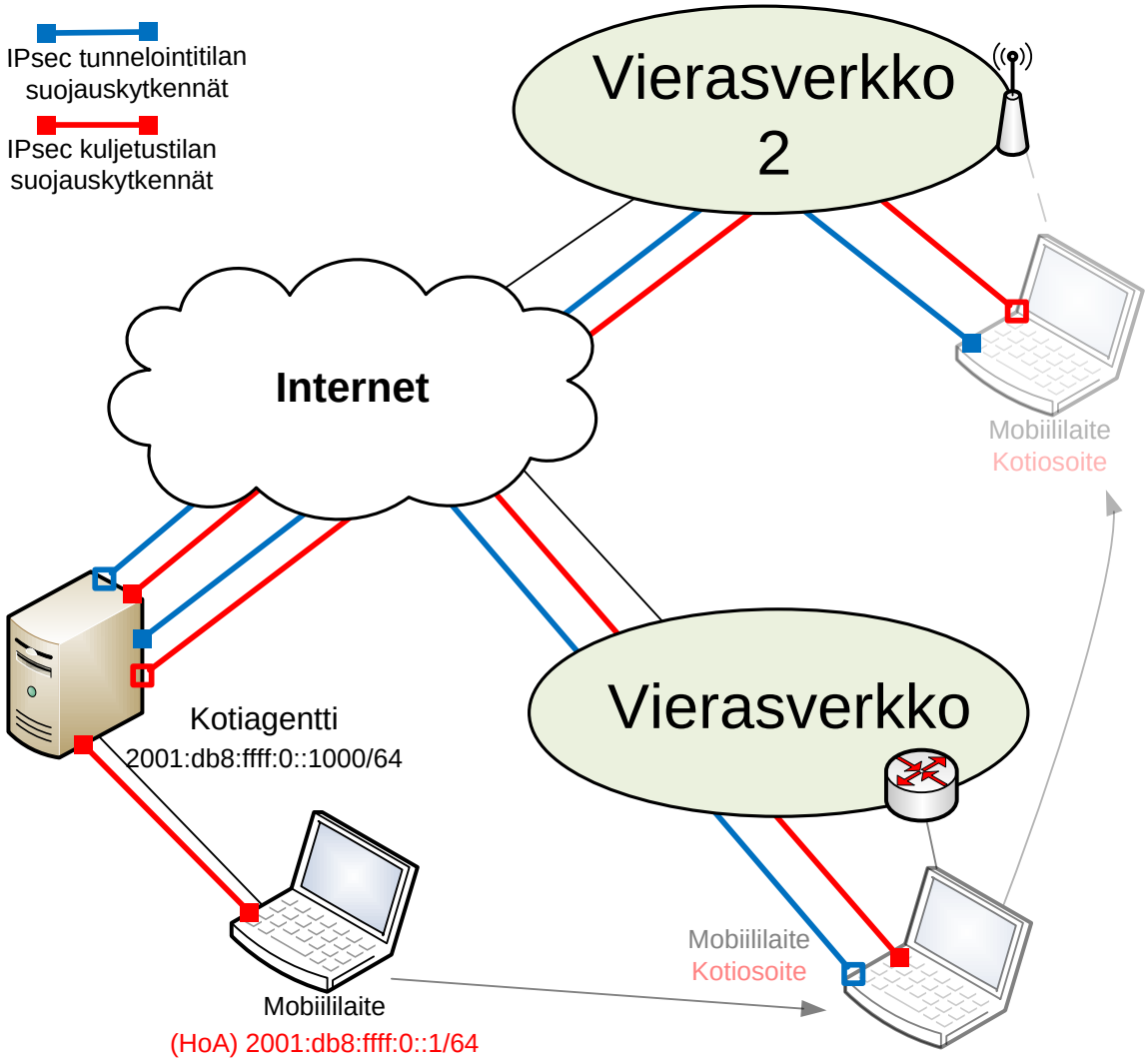
Kuvio 17: IPv6 ESP tunnelointitilassa(Kent 2005)

Jokaisella liikennöintikumppanilla on salainen laiteavain (Node Key), jolla generoidaan satunnainen numero, 20 oktettia pitkä, joka lähetetään mobiililaitteille. Laiteavain auttaa liikennöintikumppania varmistamaan, että mobiililaitteen käyttämät generoidut avainsarjat sidospäivityksien tunnistautumiseen ovat sen omia. Kyseistä avainta ei tule jakaa muiden laitteiden kanssa. Liikennöintikumppani voi generoida uudemman laiteavaimen milloin vain, varmistaen näin ettei avainten turvallinen säilyttämien ole tarpeen.(Perkins, Johnson ja Arkko 2011)

Automaattinen avaintenhallinta voi olla tuettu ja jos se on, niin joko tietoturvapolitiikan tie-

tokantojen viittaukset tai MIPv6 prosessoinnin tulee yksiselitteisesti tunnistautua avaintenvaihtoprotokollan (Internet Key Exchange) vaiheen 1 käyttäjätietojen kanssa. Näitä voidaan käyttää varmistamaan suojauskytkentöjen oikeellisuus suojatakseen sidospäivityksien päivittämisen tietylle kotiosoitteelle. *ID_IPV6_ADDR* Identity Payload:ia ei tule käyttää avaintenvaihtoprotokollan vaiheessa 1, joka käsittää *IKE_SA_INIT* ja *IKE_AUTH* viestinvälitykset. Avaintenvaihtoviestin tietovirta sisältää aina pyynnön, jota seuraa vastaus. Pyynnön lähettäjän vastuulla on varmistaa viestin luotettavuus. Avaitenvaihtoistunnon ensimmäinen viestinvälitys, *IKE_SA_INIT*, käsittelee suojausparametrin avaintenvaihdon suojauskytkennät, lähettää nonce:n ja Diffie-Hellman salausavaimet. Nonce on mielivaltainen luku, jota käytetään salatun yhteyden allekirjoittamisessa. Jokainen liikennöintikumppani generoi nonce:n tasaisin väliajoin, joka tulisi generoida satunnaisnumeron avulla. Liikennöintikumppani voi käyttää samaa salaista avainta sekä nonce:a kaikkien kommunikoitavien mobiililaitteiden kanssa. Diffie-Hellman salausavain koostuu kahdesta julkisesta parametrista, joita vaihtamalla keskenään kaksi käyttäjää voi luoda yhteisen salausavaimen. Seuraava viestinvälitys, *IKE_AUTH*, lähettää identiteetit näin osottaen tietävänsä vastaavien identiteettien salausavaimet ja asettaa suojauskytkennät ensimmäiselle todennustunnisteelle tai ESP alasuojaskytkennälle.(Perkins, Johnson ja Arkko 2011) (Kaufman et al. 2012)

3 MIPv6-testiympäristö



Kuvio 18: MIPv6-testiympäristön topologia(umip.org 2010)

Tässä luvussa käydään läpi UMIP:n asetukset MIPv6-esimerkkitestiympäristössä ja myöhemmin testiympäristössä, joka on toteutettu tämän tutkielman yhteydessä. Ensimmäinen kappale kattaa kotiagentin ja seuraava mobiililaitteen asetukset. Myös staattisen IPsec salauksen (IPsec static keying) asetuksia käydään läpi. Kuvan 18 MIPv6-testiympäristön pääelementit ovat kotiagentti ja mobiililaite:

Kotiagentti:

Verkkoyksikön eth1 rajapinta on kytkettynä internetiin ja eth0 rajapinta on kytkettynä mobiililaitteeseen.

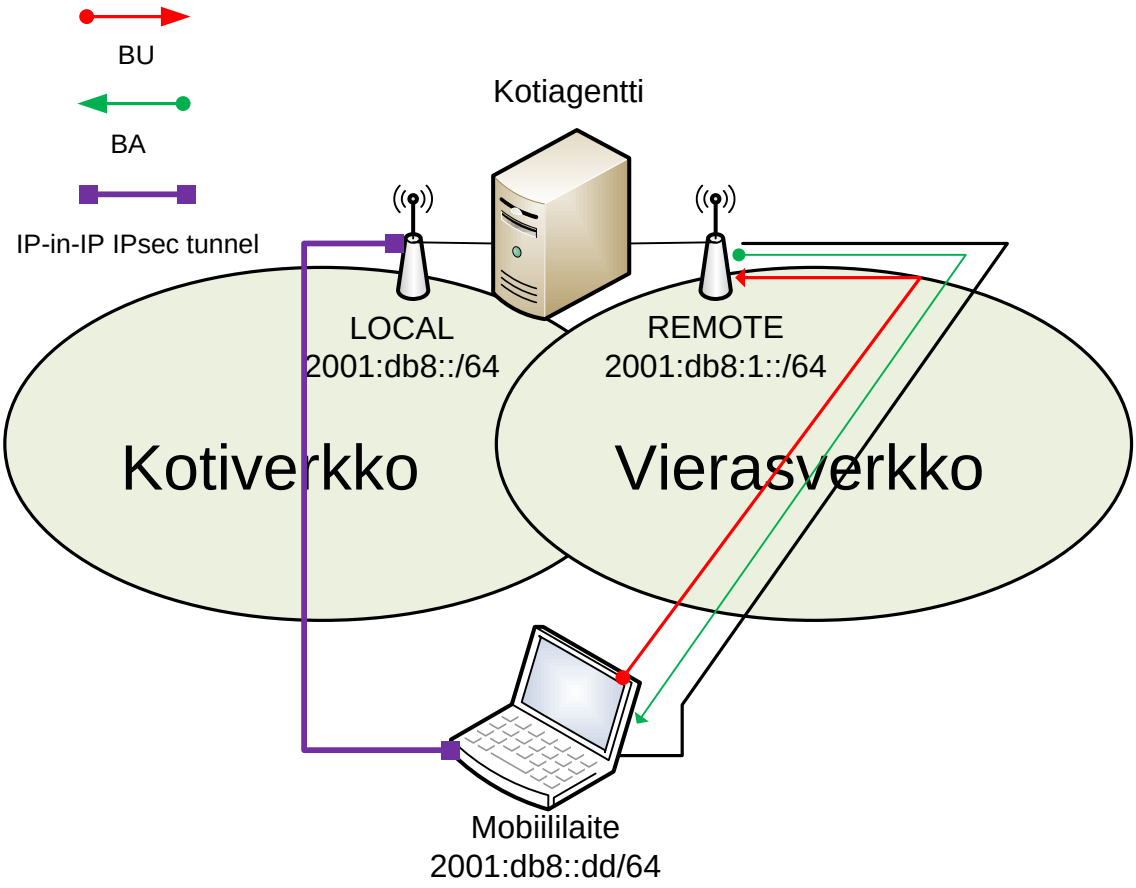
Mobiililaite:

Mobiililaitteessa on kaksi rajapintaa (802.11 ja ethernet), joista suurempi painoarvo on kiinteällä ethernet-yhteydellä.

Jotta UMIP:n operointi onnistuu, tarvitaan mobiilituen sisältävä kernel, joka näkyy liitteen kuvassa 31, sekä erinäisiä verkon- ja järjestelmänhallintaan käytettäviä ohjelmia. Kernel tulee kääntää järjestelmää varten. IPv6-tuki on integroitu kerneliin versiosta 2.6.26 eli uusimpiin kerneleihin tukea IPv6:lle ei erikseen tarvita.(Ridruejo 2000) Kotiagentin tulee myös mainostaa kotiverkkoa, jota varten käytetään RADVD -ohjelmaa. Vaikkei aikoisikaan käyttää kotiverkkoa tulee silti mainostaa reititintä kotiverkossa, koska mip6d tarvitsee sitä kotiagentin listaan. Kyseisessä tapauksessa voi käyttää dummy-rajapintaa ja mainostaa kotiverkkoa siinä. Ohjelmien asetusten asettamisen jälkeen käynnistetään kotiagentin operaatiot. Tätä tarkoitusta varten tulee ensin luoda IPsec-suojauskäytännöt, jotka käynnistetään radvd-ohjelman kanssa. UMIP käyttää IPv6-osoitteen automatisointia asettaakseen vieraan verkon osoitteen oikeaan rajapintaan.

Kotiagentin ollessa käynnissä mobiililaitteen voi käynnistää. Mobiililaitteen käynnistytyttyä varmistetaan pingaamalla, että yhteys toimii kotiverkossa. Ellei se vastaa, joko testiympäristön asetuksissa tai reitityksessä on ongelmia. Mobiililaitteen vastatessa se voidaan siirtää vieraaseen verkkoon. Kyseissä tapauksessa mobiililaitteen tulisi rekisteröityä kotiagenttiin ja siten olla vielä saavutettavissa sen kotiosoitteen avulla. Rekisteröinnin onnistumisen kotiagentin kanssa voi tehdä tarkistamalla sidospäivityslistan (Binding Update List, BUL) mobiililaitteessa ja sidosvälimuistin (Binding Cache, BC) kotiagentissa. Tämä onnistuu käyttämällä UMIP:n virtuaaliterminaalia mobiililaitteessa.

3.1 MIPv6-testiympäristön toteuttaminen



Kuvio 19: Toteutetun MIPv6-testiympäristön topologia

Testiympäristö toteutetaan kahdella kannettavalla tietokoneella, joista toinen toimii mobiililaitteena ja toinen toimii kotiverkon kotiagenttina sekä vieraan verkon rajapintana. Ensimmäisessä kannettavassa tietokoneessa, Lenovossa, on kaksi ZyXelin Wlan-adapteria, joilla koti- ja vierasverkko toteutetaan. Toteutuksessa käytetään apuna hostapd ohjelmistoa, joka mahdollistaa liitäntäpisteiden luomisen. Toisessa kannettavassa tietokoneessa, Acer Aspire one:ssa, joka toimii mobiililaitteena, on yksi ZyXelin Wlan-adapteri jota se käyttää yhteyksien luomiseen ja vaihtamiseen. Koti- ja vierasagenttina toimivalle tietokoneelle asennetaan *autoconf automake bison flex libssl-dev indent ipsec-tools radvd* —ohjelmat. Näiden lisäksi asennetaan koti- ja vierasagentille sekä mobiililaitteelle UMIP:n[1] toteuttama MIPv6 —toteutus.

[1] http://www.umip.org/

Koti- ja vierasagentin proc-tiedostojärjestelmän parametrit	
Tiedosto	**Asetettu arvo**
sysctl.conf	net.ipv6.conf.all.forwarding = 1
	net.ipv6.conf.all.accept_source_route=1
	net.ipv6.conf.all.autoconf = 0
	net.ipv6.conf.all.router_solicitations = 0
	net.ipv6.conf.all.accept_ra = 0
	net.ipv6.conf.<*käytetyt rajapinnat*>.accept_ra = 0
Mobiililaitteiden proc-tiedostojärjestelmän parametrit	
Tiedosto	**Asetettu arvo**
sysctl.conf	net.ipv6.conf.all.forwarding = 1
	net.ipv6.conf.default.use_tempaddr = 0
	net.ipv6.conf.all.use_tempaddr = 0
	net.ipv6.conf.<*käytetyt rajapinnat*>.use_tempaddr = 0

Taulukko 2: MIPv6-domainin verkkoyksiköiden ja mobiililaitteiden proc-tiedostojärjestelmän parametrit

Mobiililaitteelle ja koti- ja vierasagenttina toimivalle tietokoneella käännetään ensimmäiseksi mobiilituen omaava 3.3.0 kernel liitteen kuvan 31 mukaisesti. Verkko luodaan aluksi ilman reitinoptimiointia ja IPsec-salausta. Näiden lisäksi mobiililaitteelle asetetaan staattinen osoite. Kuvassa 19 näkyy testiympäristön topologia IPsec salauksella. Taulukossa 2 näkyy MIPv6-testiympäristön laitteille asetettavat proc-tiedostojärjestelmän parametrit. Ensimmäinen parametri mahdollistaa IPv6-pakettien eteenpäin lähettämisen, toinen parametri mahdollistaa lähdereitityspakettien reitittämisen. Kolme seuraavaa parametria liittyvät osoitteistuksiin, joista ensimmäinen estää osoitteen automaattisen konfiguroinnin vastaanotetusta reititinmainostuksen etuliitteestä, toinen ilmoittaa kuinka monta reititinkyselyä lähetetään ennenkuin oletetaan ettei reitittimiä ole läsnä ja kolmas estää reititinmainostuksien vastaanottamisen. (Narten, Draver ja Krishnan 2007) (Bieringer 2009) Mobiililaitteen kaikille rajapinnoille asetettavat taulukon 2 kolme viimeistä parametriä ilmoittavat, että poistetaan käytöstä IPv6-protokollan tietoturva ominaisuus. Kyseinen tietoturva ominaisuus luo rajapinnalle väliaikaisen IPv6-osoitteen, joka muodostuu rajapinnan tunnisteesta sekä aikaan sidotuista satunnaisista bittijonoista. Parametrin arvolla 2 mobiililaite käyttää kyseistä väliaikaista IPv6-osoitetta oletuksena, arvolla 1 ei käytä ja arvolla 0 väliaikaista osoitetta ei luoda ollenkaan (www.archlinux.org 2012).

Ohjelmien asentamisen ja luotujen konfiguraatioiden jälkeen sammutetaan network-manager palvelu, kytketään wlan-verkkokortit päälle sekä poistetaan virransäästöominaisuus. Luodaan liitänpisteet ”LOCAL” ja ”REMOTE” eri kanavilla, jotta ne eivät aiheuta häiriötä toisilleen. Tämän jälkeen käynnistetään hostapd-ohjelmisto molemmille liitäntäpisteille ja vasta tämän jälkeen asetetaan staattiset IPv6-osoitteet wlan rajapinnoille. Lopuksi käynnistetään radvd- ja mip6d-ohjelmat käyttäen luotuja asetustiedostoja.

Mobiililaitteen yhdistäessä kotiagenttiin rekisteröinnin onnistumisen voi tarkistaa katsomalla sidosvälimuistin kotiagentilta, joka näkyy liitteen kuvassa 6.1, sekä katsomalla sidospäivityslista mobiililaitteelta, joka näkyy liitteen kuvassa 6.2. IPsec salauksen ollessa päällä kotiagentissa ja mobiillaitteessa, vain mobiililaitteen päässä näkyi informaatiota. Ainoa tieto yhteyden olemassa olosta koti- ja vierasagentissa oli hostapd ohjelman LOCAL-terminaali, jossa näkyi tieto mobiililaitteiden yhteyksien tilasta.

4 PMIPv6-testiympäristö

Tässä luvussa käydään ensin läpi PMIPv6-testiympäristön pääelementit ja sen toiminta. Seuraavassa kappaleessa käydään läpi testiympäristön toteutus, siinä käytettävät ohjelmistot ja asetukset. Testiympäristön toteutus —kappaleen jälkeen seuraa vielä kolme alikappaletta, joissa suoritetaan käytännön testit testiympäristössä ensin ilman liikkuvuudenhallintaa ja sen jälkeen liikkuvuudenhallinnan kanssa, lopussa käydään läpi testiympäristössä ilmenneistä ongelmista. PMIPv6-testiympäristön pääelementit ovat mobiililiitos ja mobiiliyhdyskäytävät:

Mobiililiitos:
: Verkkoyksikön eth0 rajapinta on kytketty liikennöintikumppaniin ja eth1 rajapinta on kytketty kytkimeen.

Mobiiliyhdyskäytävä 0:
: Verkkoyksikön eth2 rajapinta on kytketty kytkimeen ja eth1 rajapinta on kytketty erilliseen langattomaan tukiasemaan.

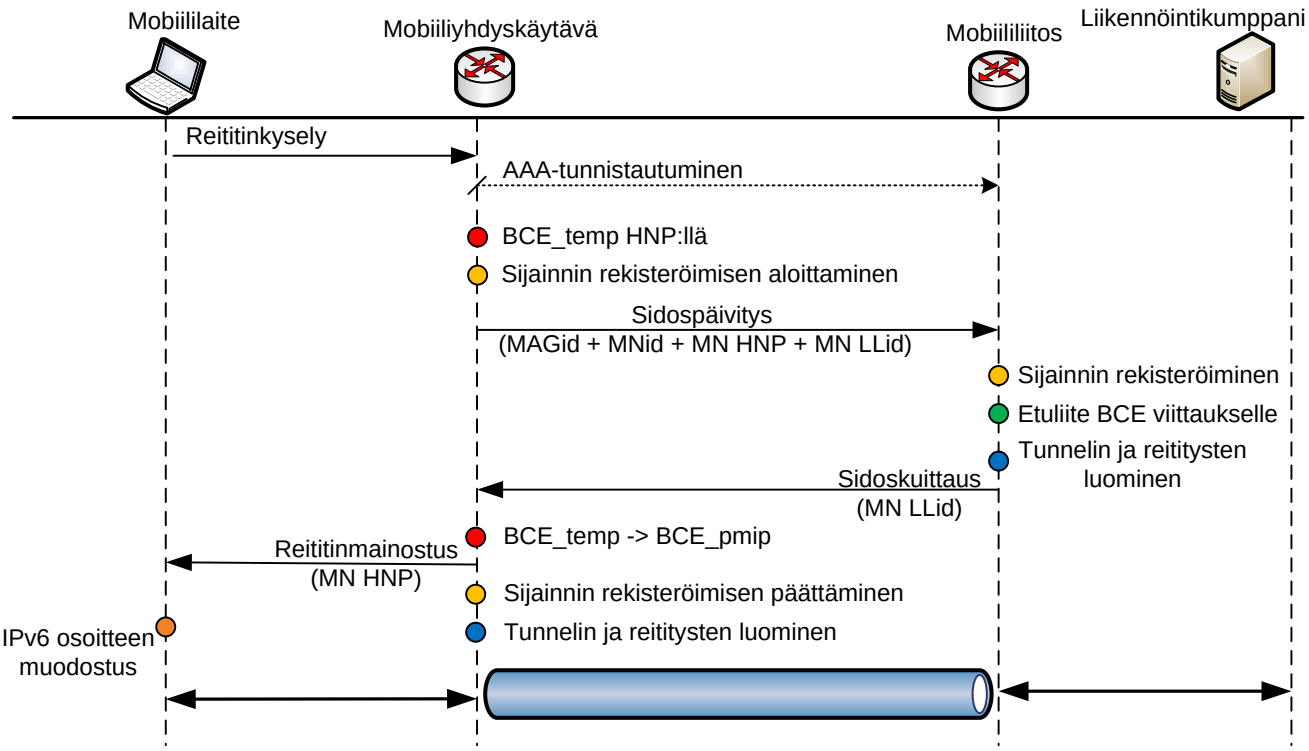
Mobiiliyhdyskäytävä 1:
: Verkkoyksikön eth1 rajapinta on kytketty kytkimeen ja eth0 rajapinta on kytketty erilliseen langattomaan tukiasemaan.

Mobiililaite:
: Mobiililaitteen wlan rajapintaa käytetään PMIPv6-verkkoon yhdistämiseen.

Liikennöintikumppani:
: Liikennöintikumppanin eth0 rajapinta on suoraan kytkettynä mobiililiitokseen ja laitteessa pyörii apache-, vlc- ja linphone-ohjelmistot joita käytetään testiympäristön käytännön testeissä.

Kuvassa 20 nähdään testiympäristön toiminta signalointitasolla. Yhteyden muodostus alkaa mobiililaitteen lähettäessä viestin mobiiliyhdyskäytävälle, joka sisältää mobiililaitteen paikallisen yhteysosoitteen, jota käytetään mobiililaitteen tunnisteena. Mobiiliyhdyskäytävä tarkistaa löytyykö saatu tunniste radiuspalvelimelta ja jos löytyy, luodaan väliaikainen viittaus sidosvälimuistiin, joka sisältää mobiililaitteen tunnisteen sekä radiuspalvelimelta saadun ko-

tiverkon etuliitteen, ja aloitetaan sijainnin rekisteröimisen toimenpiteet. Mobiiliyhdyskäytävä lähettää sidospäivityksen mobiililiitokselle, joka tarkistaa löytyykö aiempia viittauksia välimuistista. Tämän jälkeen aloitetaan sijainnin rekisteröiminen, luodaan tarvittaessa uusi viittaus välimuistiin, johon ensisijainen palveltava mobiiliyhdyskäytävä merkitään. Sidosvälimuistin päivittämisen jälkeen mobiililiitos luo IP-in-IP tunnelin mobiililiitoksen ja ensisijaisen palveltavan mobiiliyhdyskäytävän välille sekä luo tarvittavat reitit. Tunnelin luomisen jälkeen mobiililiitos luo ja lähettää sidoskuittauksen mobiiliyhdyskäytävälle, joka sisältää mobiililaitteen yhteyskerroksen tunnisteen. Sidoskuittauksen vastaanottamisen jälkeen mobiiliyhdyskäytävä lähettää mobiililaitteelle kotiverkon etuliitteen ja siirtää väliaikaisen viittauksen sidosvälimuistista välimuistiin näin päättäen sijainnin rekisteröimisen. Lopuksi mobiiliyhdyskäytävä luo IP-in-IP tunnelin toisen pään mobiililiitokselle sekä tarvittavat reitit.



Kuvio 20: PMIPv6-testiympäristön signalointiviestit

Testiympäristön mobiiliyhdyskäytävät kuuntelevat PMIPv6-verkon ulkorajapinnassa reitinkysely (Router Solicitation, RS)-viestejä, johon vastataan reititinmainostus-viesteillä (Rou-

ter Advertisement, RA). Kyseiset multicast-viestit aktivoivat tunneloinnin luonnin mobiiliyhdyskäytävän ja mobiililiitoksen välille. Kyseinen viestittely näkyy liitteen E kuvasta 38, joka on otettu testiympäristön verkkoyksiköiltä, viestiä on ”sievennetty” turhasta infosta ja jätetty vain oleellinen tilanpuutteen vuoksi. Reititinkysely-viestiä käytetään, kun isäntälaite haluaa saada heti tietää mahdolliset verkon reitittimet odottamatta ajoittain lähetettävää reititinmainostus-viestiä. Tunnelin luonnin jälkeen mobiililaite ja mobiiliyhdyskäytävä lähetettää vaihtelevasti naapurinkysely-viestiä (Neighbor Solicitation, NS), johon vastataan naapurinmainostus-viestillä (Neighbor Advertisement, NA). Kyseinen viestittely ylläpitää tunnelia, ja jos naapurinkysely-viestiä ei tule asetetun sidospäivityksen elinajan aikana, tunneli tuhotaan. (Deering 1991) (Paxson et al. 2011)

PMIPv6-verkon mobiiliyhdyskäytävien rajapinnassa toimivat Cisco 1200 Aironet-tukiasemat on konfiguroitu siten, että niillä on sama langattoman verkon tunniste ja eri IP-osoite ja ne lähettävät logitiedot mobiiliyhdyskäytävälle, mihin ne on fyysisesti kytkeytyneenä. Mobiiliyhdyskäytävien rajapinnat, jotka on liitetty tukiasemiin, omaavat saman Media Access -osoitteen (MAC) joka ilmoitetaan mobiililiitokselle, jotta se tietää mikä on kaikkien mobiiliyhdyskäytävien paikallisosoite. 48-bittinen universaali MAC-osoitteistus perustuu ideaan, että kaikki mahdolliset verkon jäsenet tarvitsevat yksillölisen tunnisteen, jos ne aikovat olla yhtäaikaa samassa verkossa. (ASSOCIATION 2011) (Society 2002). Sama MAC-osoite mahdollistaa mobiililaitteiden siirtymisen verkon alueella ilman, että ne huomaavat muutosta PMIPv6-domainin yhdyspisteen vaihdosta. Liikennöintikumppani on liitetty fyysisesti paikalliseen mobiililiitokseen ja sille on asetettu staattinen IPv6-osoite.

4.1 PMIPv6-testiympäristön toteuttaminen

Aluksi haemme mobiililiitokselle ja mobiiliyhdyskäytäville OpenAirInterfacen UMIP:n luoman MIPv6 ratkaisun päälle rakennetun PMIP totetuksen.[1] Mobiililaitteina toimivat Samsung S ja SII puhelimet sekä kaksi kannettavaa tietokonetta Linux Lubuntu käyttöjärjestelmällä, joihin on käännetty 3.4.4 kernel liitteen kuvan 31 mukaisilla mobiilitukiasetuksilla. Tukiasemiin, jotka on liitetty mobiiliyhdyskäytäviin, yhdistäminen tapahtuu käyttäen lubuntun omaa network-manageria.

[1] http://www.openairinterface.org/openairinterface-proxy-mobile-ipv6-oai-pmipv6

Syslog-palvelimen asetukset	
Tiedosto	**Muokkaus/lisäys ja tarkoitus**
/etc/*syslog.conf*	local7.info /var/log/pmip_syslog.log
	Cisco 1200 Aironet tukiasemalta tulevat logitiedot.
/etc/default/*syslogd*	SYSLOGD=”-r”
	Mahdollistaa etäviestien kuuntelun.
FreeRadius-asiakasohjelmiston asetukset	
Tiedosto	**Muokkaus/lisäys ja tarkoitus**
hosts	2001:100::1 radius6server
	Liitetään radiuspalvelimen IPv6-osoitteeseen *radius6server* nimi.
ld.so.conf	include /usr/local/lib/
	Liitetään FreeRadius kirjastot PMIP6D:iin.
radiusclient.conf	authserver radius6server
	Ilmoitetaan asiakasohjelmistolle tunnistautumisessa käytettävä osoite.
radiusclient.conf	acctserver radius6server
	Ilmoitetaan asiakasohjelmistolle kirjanpidossa käytettävä osoite.

Taulukko 3: Mobiiliyhdyskäytävälle tehtävät asetukset

Mobiililiitokseen ja mobiiliyhdyskäytäviin asennetaan seuraavat ohjelmat: *libpcap-dev indent bison flex iproute-dev libc6-dev libssl-dev autoconf libtool macchanger python-netaddr* ja näiden lisäksi mobiiliyhdyskäytäville *socklog sysklogd radvd* -ohjelmat.

Mobiiliyhdyskäytävien Syslog-palvelinohjelmiston asetukset konfiguroidaan taulukon 3 mukaisesti. Seuraavaksi asennetaan ja konfiguroidaan FreeRadius asiakasohjelmisto mobiililiitokselle ja mobiiliyhdyskäytäville taulukoiden 3 ja 4 mukaisesti. Taulukossa 4 on esimerkki mobiililiitoksella sijaitsevan FreeRadius palvelimen käyttäjästä, jossa näkyy kahden mobiililaitteen MAC-osoite sekä sille määrätty kotiverkonosoite.

Tarvittavien ohjelmistojen asentamisen ja luomisen jälkeen voidaan käynnistää kuvan 25 mukainen testiympäristö. Verkon liitäntäpisteinä toimi kaksi Cisco 1200 Aironet-tukiasemaa, joissa on 12.3(3)JCE ohjelmistot. Testiympäristö toimii siten, että mobiililaite ottaa yhteyden tukiasemaan, joka ilmoittaa mobiiliyhdyskäytävälle, jossa radius-asiakasohjelmisto sijaitsee, syslog-viesteillä uudesta yhteydestä. Mobiiliyhdyskäytävä ottaa yhteyden mobiililiitoksessa sijaitsevaan radius-palvelimeen, jossa suoritetaan tarkistus löytyykö sieltä mobiililaitteen tunniste (MAC-osoite). Siinä tapauksessa, jos radius-palvelimelta löytyy kyseinen käyttäjä, lähetetään radius-asiakkaalle määritelty etuliite, josta mobiililaite luo itselleen IPv6

osoitteen. Taulukossa 5 näkyy eri verkkoyksiköiden muutetut proc-tiedostojärjestelmän arvot.(Draves 2003) (A et al. 2005) Taulukossa näkyvät parametrien tarkoitukset on selitetty aikaisemmassa luvussa 3. Testeissä käytettiin verkkoprokollien analysointiin tarkoitettuja ohjelmia. Verkkoyksiköissä ja kannettavissa tietokoneissa käytettiin Wireshark:ia[2] ja kännyköissä käytettiin tcpdump:ia[3].

FreeRadius käyttäjät (mobiililaitteet)	
Liitetään mobiililaitteiden MAC-osoitteet Freeradius-palvelimelle	
Tiedosto	**Lisäys**
users	0000002268aca5f5 Auth-Type := Accept, User-Password == "linux" Service-Type = Authenticate-Only, Framed-Interface-Id = 0000:0000:0000:0000, Framed-IPv6-Prefix = 2001:db8::/64" *... kaikki mobiililaitteet samalla tavalla, vähintään tunniste vaihtuu*
FreeRadius asiakkaat (mobiiliyhdyskäytävät)	
Liitetään mobiiliyhdyskäytävien IPv6-osoitteet ja tunnisteet Freeradius-palvelimelle.	
Tiedosto	**Lisäys**
clients.conf	client 2001:100::2 { secret = testing123 shortname = MAG0 nastype = other password = linux } *... kaikki mobiiliyhdyskäytävät samalla tavalla, IPv6-osoite vaihtuu*

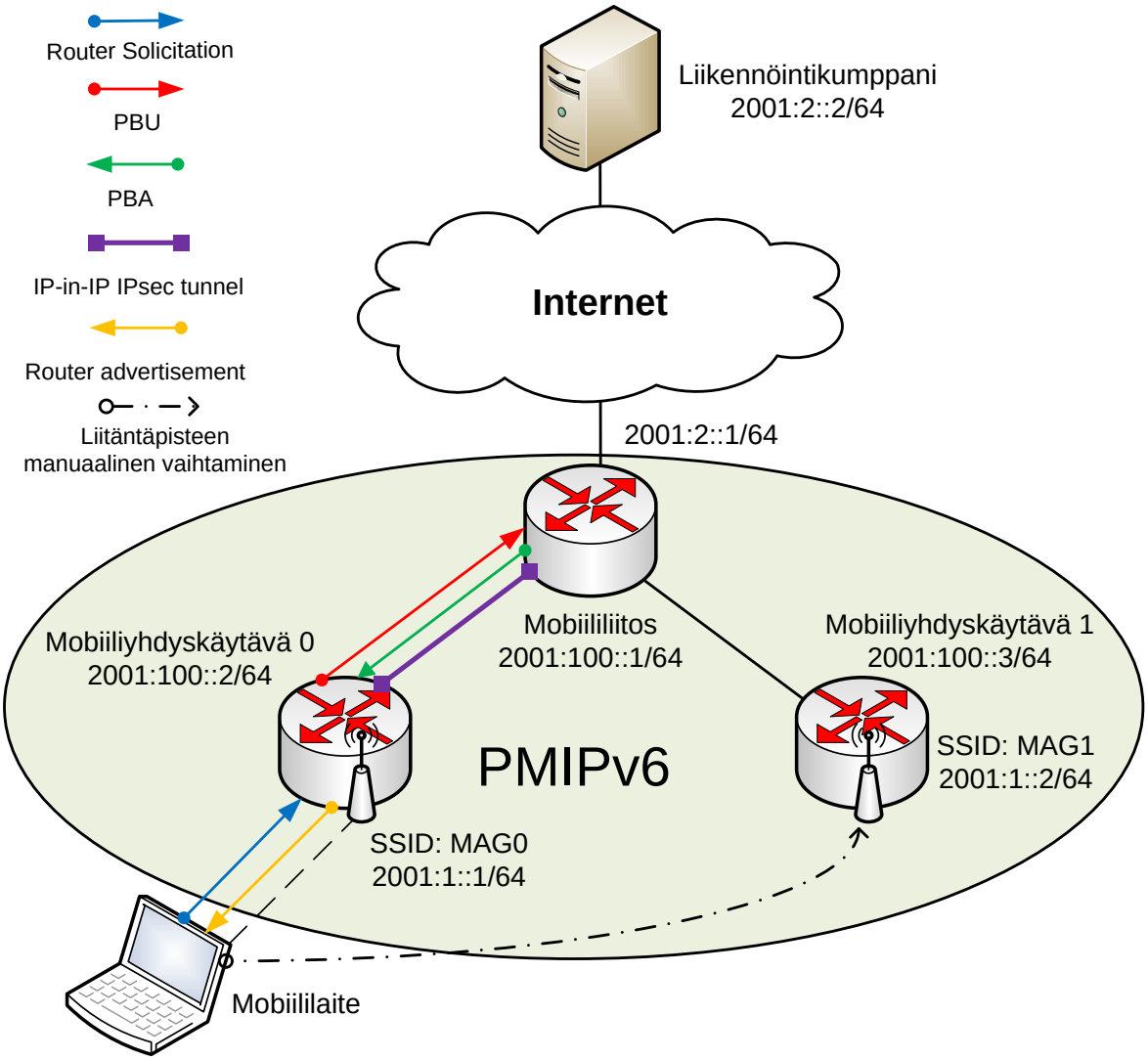
Taulukko 4: Mobiililiitokselle tehtävät asetukset

[2]http://www.wireshark.org/
[3]http://www.tcpdump.org/

Mobiililiitoksen ja mobiiliyhdyskäytävien proc-tiedostojärjestelmän parametrit	
Tiedosto	**Asetettu arvo**
sysctl.conf	net.ipv6.conf.all.forwarding = 1
	net.ipv6.conf.all.accept_ra = 0
	net.ipv6.conf.<*käytetyt rajapinnat*>.accept_ra = 0
Mobiililaitteiden proc-tiedostojärjestelmän parametrit	
Tiedosto	**Asetettu arvo**
sysctl.conf	net.ipv6.conf.all.forwarding = 1
	net.ipv6.conf.default.use_tempaddr = 0
	net.ipv6.conf.all.use_tempaddr = 0
	net.ipv6.conf.<*käytetyt rajapinnat*>.use_tempaddr = 0

Taulukko 5: PMIPv6-domainin Verkkoyksiköiden ja mobiililaitteiden proc-tiedostojärjestelmän parametrit

4.1.1 Käytännöntestit ilman liikkuvuudenhallintaa



Kuvio 21: Toteutetun PMIPv6-testiympäristön topologia ilman liikkuvuudenhallintaa

Testit suoritettiin ensin kuvan 22 mukaisessa salaamattomassa, tämän jälkeen kuvan 23 mukaisessa IPsec-salatussa ja lopuksi kuvan 24 mukaisessa IPsec- sekä WPA-salatussa PMIPv6-testiympäristössä. Manuaalisen verkonvaihdon tilastot näkyvät taulukossa 6, josta ilmenee kuinka paljon hävikkiä paketeissa tulee manuaalisesti vaihtamalla verkon liitäntäpistettä. PMIPv6-verkon rajapintoina toimineet mobiiliyhdyskäytävät olivat toisistaan noin 10 metrin päässä. Verkossa ei ollut muuta liikennettä kuin mobiililaitteen tuottama liikenne. Aiemmin luvun alussa 4 mainitusta testiympäristöstä poiketen käytettiin mobiiliyhdyskäytävien

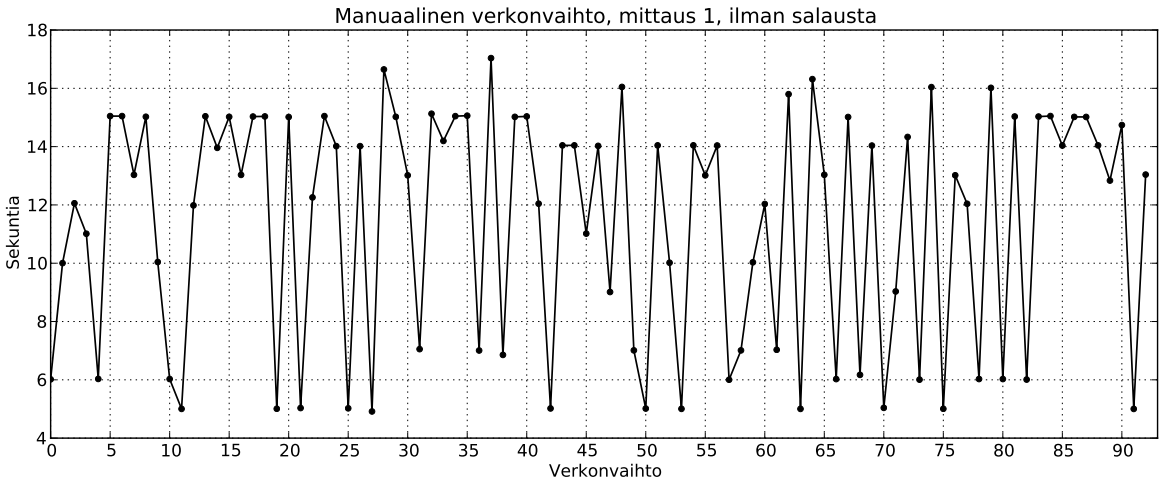
ulkorajapintoina Zyxel langattomia verkkoadaptereita sekä hostapd-ohjelmistolla luotuja tukiasemia. Koska PMIPv6-domainin mobiiliyhdyskäytävien ulkorajapinnoilla tulee olla sama MAC-osoite, ei ollut mahdollista käyttää samaa langattoman verkon tunnistetta tukiasemilla, käytettäessä PMIPv6-verkon ulkorajapintana langatonta tukiasemaa. Kyseinen järjestely häiritsi mobiililaitteita, eivätkä ne kyenneet erottamaan PMIPv6-verkon liitäntäpisteitä toisistaan, koska niillä oli samat langattoman verkon tunnisteet myös ilman liitäntäpistettä (ESSID ja BSSID).

Mobiiliyhdyskäytävien ja mobiililiitoksen välinen tunneloitu liikenne salattiin IPsec:llä. Asetustiedostoesimerkit ovat nähtävillä liitteessä D. Viimeisessä testissä käytettiin myös WPA-salausta yhteyden suojaamiseen mobiililaitteen ja mobiiliyhdyskäytävien välillä. Testissä mobiililaitteelta aloitettiin liikennöintikumppanin pingaaminen (ping6) osoitteeseen 2001:2::2 ja kyseisen komennon kulkiessa mobiililaite vaihtoi langatonta verkkoa aina, kun uusi yhteys oli saatu muodostettua ja ping alkoi taas kulkemaan liikennöintikumppanille.

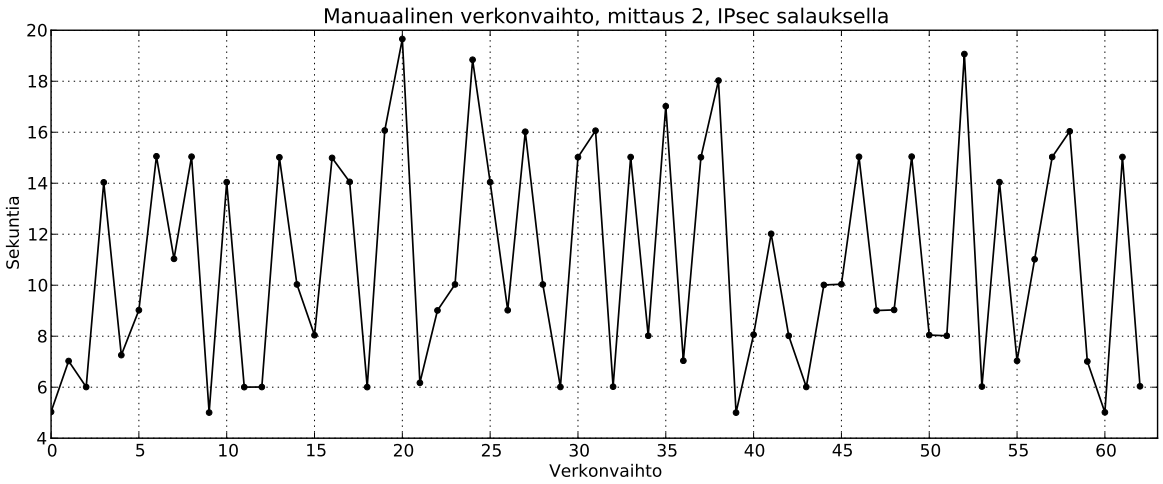
Mobiililaitteen manuaalinen verkonvaihto, toistoja 100kpl	
Kuva 22	
Ympäristö	**Minimi / keskiarvo / maksimi (sekuntia)**
Salaamaton	4,91 / 11,40 / 17,04
Lähetetyt / Vastaanotetut paketit	**Pakettien hävikki (% / kpl)**
1887 / 834	55,8 / 1053
Kiertoaika minimi / keskiarvo / maksimi (millisekuntia)	**Duplikaatteja / virheitä (kpl)**
2,661 / 11,746 / 237,856	81 / 826
Kuva 23	
Ympäristö	**Minimi / keskiarvo / maksimi (sekuntia)**
IPsec salattu	5,00 / 10,88 / 19,66
Lähetetyt / Vastaanotetut paketit	**Pakettien hävikki (% / kpl)**
1241 / 475	61,7 / 766
Kiertoaika minimi / keskiarvo / maksimi (millisekuntia)	**Duplikaatteja / virheitä (kpl)**
3,203 / 12,337 / 234,439	53 / 510
Kuva 24	
Ympäristö	**Minimi / keskiarvo / maksimi (sekuntia)**
IPsec ja WPA salattu	3,00 / 12,13 / 20,06
Lähetetyt / Vastaanotetut paketit	**Pakettien hävikki (% / kpl)**
1312 / 418	68,1 / 894
Kiertoaika minimi / keskiarvo / maksimi (millisekuntia)	**Duplikaatteja / virheitä (kpl)**
2,810 / 10,987 / 225,605	20 / 588

Taulukko 6: Verkonvaihto mobiiliyhdyskäytävien välillä

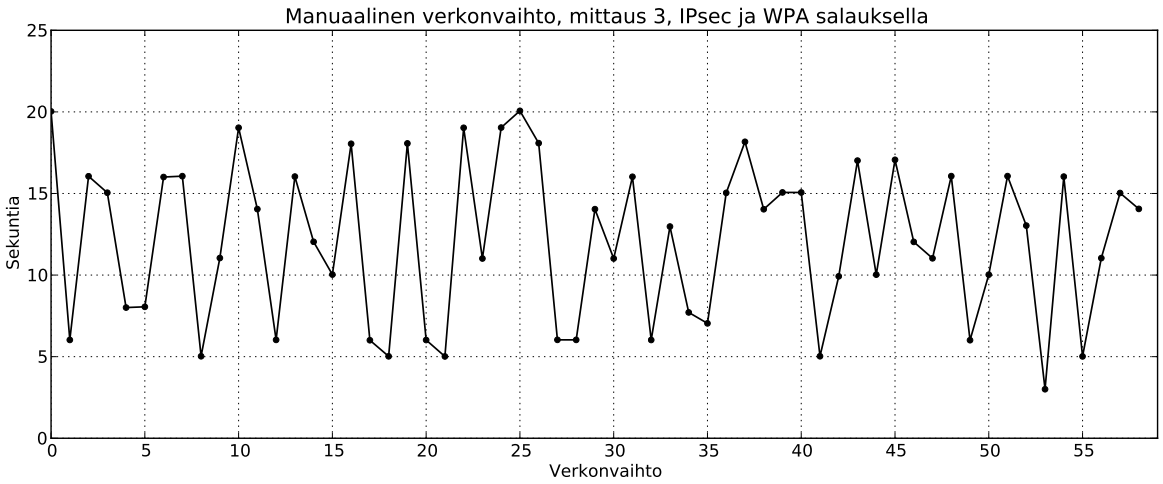
Testejä jatkettiin asentamalla liikennöintikumppanille Service Initiation Protocol -palvelin (SIP), jonka kautta on mahdollista soittaa toiselle käyttäjälle. Mobiililaite, joka on rekisteröitynyt SIP-palvelimelle, soittaa äänitiedostoa toiselle rekisteröityneelle mobiililaitteelle, jota seuraamalla näkee konkreettisemmin mitä mobiiliyhdyskäytävää vaihtamalla tapahtuu paketeille. Ongelmaksi ilmeni Samsunging puhelimien Android-käyttöjärjestelmä, josta enemmän kappaleessa 4.1.3. Samsung puhelimissa on näennäisesti samat asetukset kuin mobiililaitteins toimivissa kannettavissa tietokoneissa, jossa yhteys ei katkea. Kannettavissa tietokoneissa on Ubuntu ja Lubuntu käyttöjärjestelmät



Kuvio 22: Salaamaton verkonvaihto mobiiliyhdyskäytävien välillä

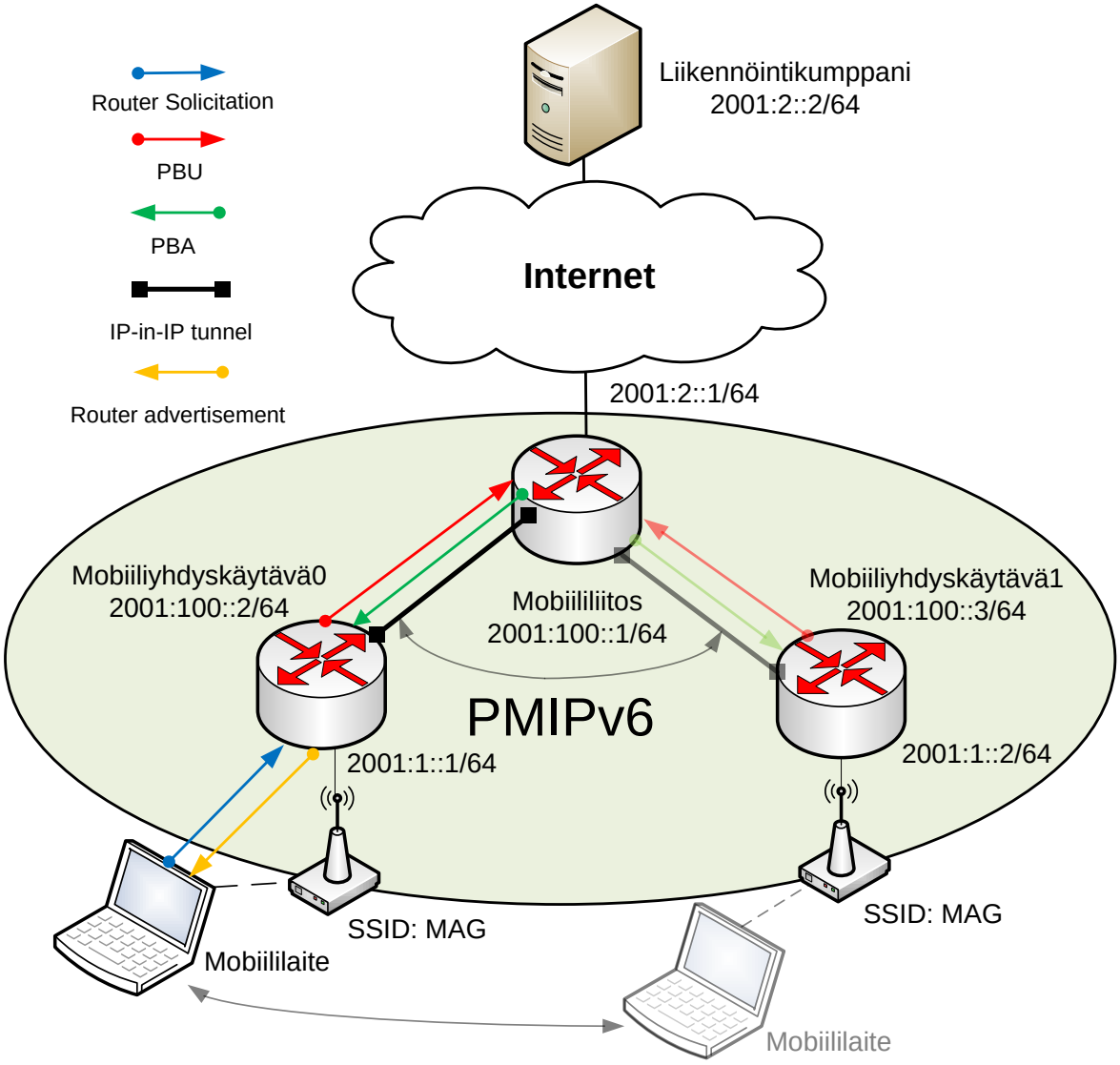


Kuvio 23: IPsec salattu verkonvaihto mobiiliyhdyskäytävien välillä



Kuvio 24: IPsec ja WPA salattu verkonvaihto mobiiliyhdyskäytävien välillä

4.1.2 Käytännöntestit liikkuvuudenhallinnalla



Kuvio 25: Toteutetun PMIPv6-testiympäristön topologia liikkuvuudenhallinnalla

Testiympäristön topologia muuttui hieman liikkuvuudenhallinnan kanssa, molemmat mobiiliyhdyskäytävät asennettiin pöytäkoneeseen ja PMIPv6-verkon verkkoyksiköt kykettiin HP ProCurve 2650 kytkimeen ja liikennöintikumppani oli yhdistetty suoraan mobiililiitokseen. Näin tehden PMIPv6-domainin verkkoyksiköt sekä liikennöintikumppani saatiin yhdistettyä toisiinsa verkkokaapeleilla, joka poisti aiemmin ilmenneet duplikaatit pingatessa. Kuvasta 25 näkee liikkuvuudenhallinnan toiminnan periaatteen ja eron verkkoon ilman liikkuvuudenhallintaa (vertaa kuvaan 21).

Mobiililaitteen automaattinen verkonvaihto, toistoja 50kpl	
1. Mittaus.	Kuva 26
Lähetetyt / Vastaanotetut paketit	**Pakettien hävikki (% / kpl)**
12800 / 12527	2,1 / 273
Kiertoaika minimi / keskiarvo / maksimi (millisekuntia)	
1,270 / 7,668 / 202,00	
Ilman verkonvaihtoja	
Kiertoaika minimi / keskiarvo / maksimi (millisekuntia)	
1,270 / 5,402 / 20,00	

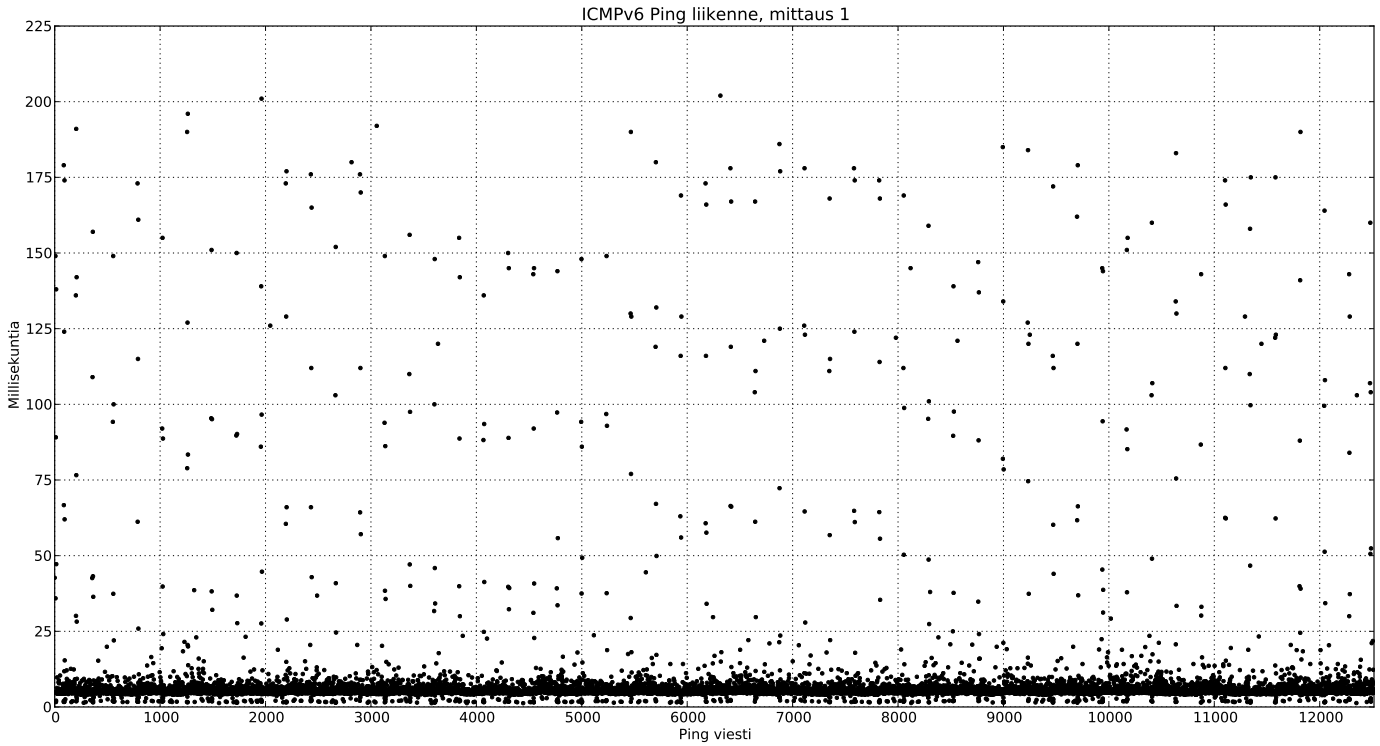
Taulukko 7: Verkonvaihto mobiiliyhdyskäytävien välillä liikkuvuudenhallinnalla

Taulukossa 7 ilmenee testiympäristön toiminta liikkuvuudenhallinnalla (vertaa taulukkoon 6), pakettien hävikki putoaa murto-osaan koska yhteyttä ei tarvitse käyttää alhaalla, vain tunnelin vaihdon yhteydessä muutama paketti katoaa. Huomioitavaa on kuitenkin, että testiympäristö ilman liikkuvuudenhallintaa käytti langatonta yhteyttä, josta aiheutui taulukossa 6 ilmenevät duplikaatit. Kuvasta 26 näkee kuinka ICMPv6 ping paketit pääosin sijoittuvat alle kahdeksan (8) millisekunnin alueelle, korkeammalla olevat paketit ilmaisevat verkonvaihtoa. Testaus tapahtui yhdistämällä mobiililaite PMIPv6-domainiin mobiiliyhdyskäytävän kautta ja alkamalla pingaamaan liikennöintikumppania, joka oli PMIPv6-domainin ulkopuolella, 64 tavun paketilla 0.5 sekunnin välein. Pingin kulkiessa liikuttiin PMIPv6-domainin alueella siten, että lähestetyttiin mobiiliyhdyskäytävien liitäntäpisteitä kunnes mobiiliyhdyskäytävä ilmoitti mobiililiitokselle mobiililaitteen liikkeestä. Tämän seurauksena aikaisempi tunneli vanhan mobiiliyhdyskäytävän ja mobiililiitoksen välillä tuhottiin ja luotiin uusi tunneli uuden mobiiliyhdyskäytävän ja mobiililiitoksen välille.

Seuraavat testit suoritettiin jälleen samassa testiympäristössä, jossa liikennöintikumppani lähetti RTP-protokollan yli ääntä vaihtelevilla suoratoistoprotokollilla sekä asetuksilla suoraan mobiililaitteelle. Kyseinen asetelma kuvastaa IP-puhelinyhteyttä, joka näkyy kuvassa 27. Jälleen liikuttiin mobiiliyhdyskäytävien välillä ja saatiin tulokset, jotka näkyvät taulukossa 8. Testeissä ainoa missä ilmeni jitteriä, toisin sanoen viiveen suuruuden vaihtelua, oli, kun ääntä lähetettiin pakkaamattomana verkon yli mobiililaitteelle.

Tiedostomuoto .wav	
1. Mittaus.	Kuvat 28 ja 29
Puskuri (millisekuntia)	**Kesto (sekuntia)**
300	900
Suoratoistoprotokolla	**Jitter keskiarvo / maksimi (millisekuntia)**
MPEG-II streams	0 / 0
Lähetetyt / Vastaanotetut paketit	**Pakettien hävikki (% / kpl)**
17524 / 16738	2,9 / 507
6. Mittaus	
Puskuri (millisekuntia)	**Kesto (sekuntia)**
100	660
Suoratoistoprotokolla	**Jitter keskiarvo / maksimi (millisekuntia)**
16-bit audio, monoaural	20,99 / 294,91
Lähetetyt / Vastaanotetut paketit	**Pakettien hävikki (% / kpl)**
48515 / 44264	8,1 / 4251

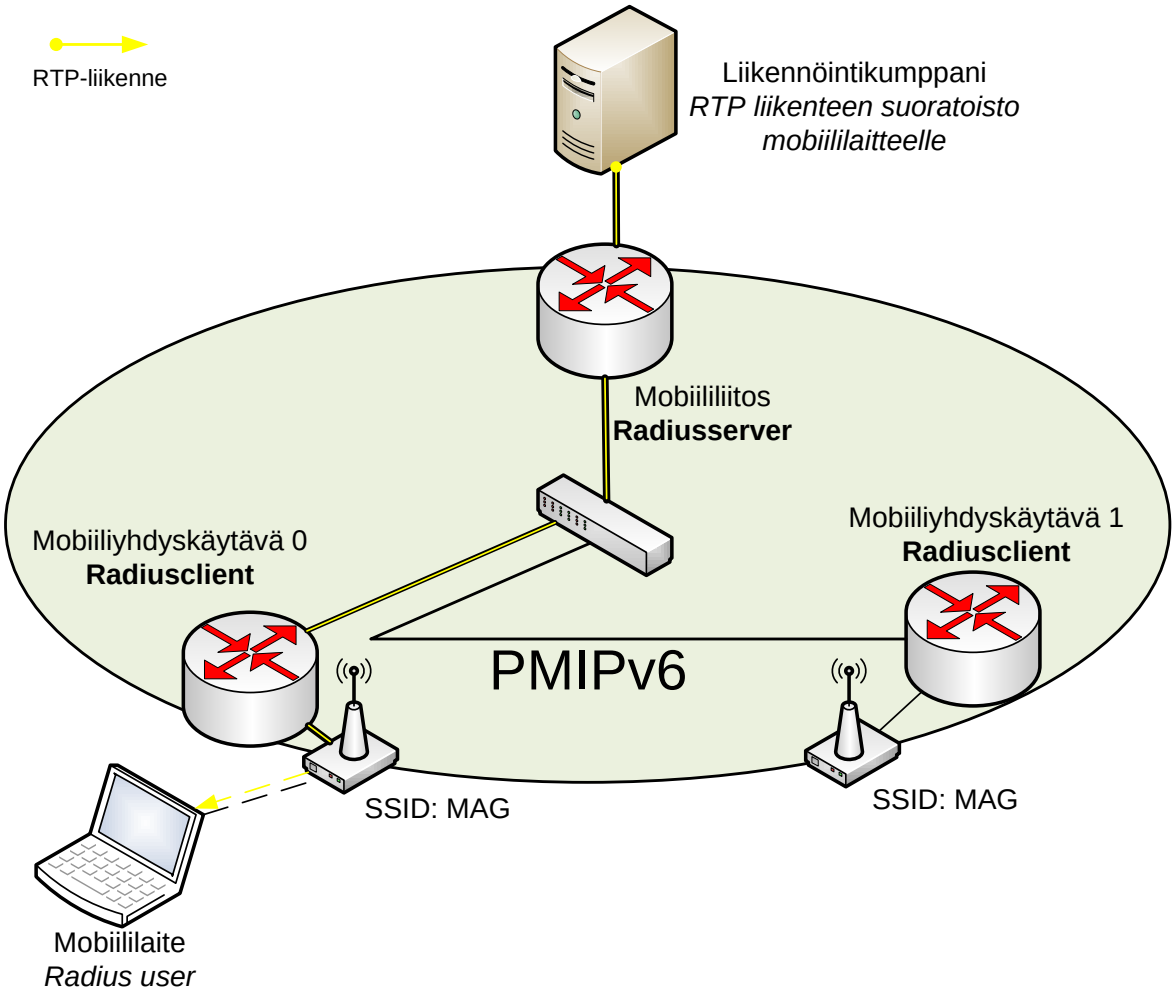
Taulukko 8: Äänensiirto wav-tiedostolla RTP-protokollalla PMIPv6-verkon yli mobiililaitteelle. Katso liite C



Kuvio 26: Mobiililaitteen ICMPv6 Ping-liikenne mobiililaitteelta liikennöintikumppanille

Sidospäivitys- ja sidoskuittausviesteihin kuluva aika	
Verkkoyksikkö	**Minimi / keskiarvo / maksimi (millisekuntia)**
Mobiililiitos	0,711 / 5,203 / 17,675
Mobiiliyhdyskäytävä 0	1,047 / 5,539 / 18,004
Mobiiliyhdyskäytävä 1	0,823 / 6,146 / 17,648

Taulukko 9: PMIPv6 Verkkoyksiköiden sidoskuittaukseen kuluva aika



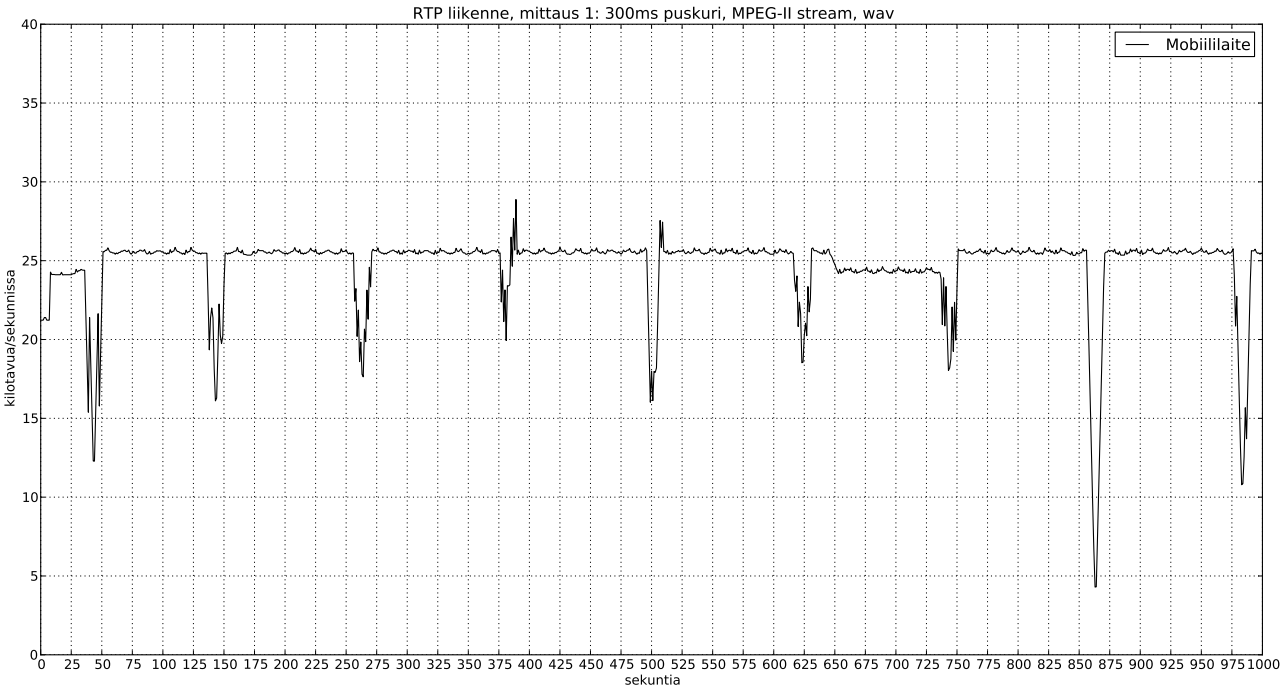
Kuvio 27: PMIPv6-testiympäristön toiminta RTP-liikenteen suoratoistolla

Tiedostomuoto .mp3	
2. Mittaus	
Puskuri (millisekuntia)	**Kesto (sekuntia)**
200	820
Suoratoistoprotokolla	**Jitter keskiarvo / maksimi (millisekuntia)**
MPEG-I/II streams	0 / 0
Lähetetyt / Vastaanotetut paketit	**Pakettien hävikki (% / kpl)**
13503 / 12822	4,8 / 681
3. Mittaus	
Puskuri (millisekuntia)	**Kesto (sekuntia)**
200	838
Suoratoistoprotokolla	**Jitter keskiarvo / maksimi (millisekuntia)**
MPEG-I/II streams	0 / 0
Lähetetyt / Vastaanotetut paketit	**Pakettien hävikki (% / kpl)**
30484 / 29114	4,3 / 1370
4. Mittaus	
Puskuri (millisekuntia)	**Kesto (sekuntia)**
300	600
Suoratoistoprotokolla	**Jitter keskiarvo / maksimi (millisekuntia)**
MPEG-I/II streams	0 / 0
Lähetetyt / Vastaanotetut paketit	**Pakettien hävikki (% / kpl)**
22077 / 21184	3,9 / 893
5. Mittaus	
Puskuri (millisekuntia)	**Kesto (sekuntia)**
200	642
Suoratoistoprotokolla	**Jitter keskiarvo / maksimi (millisekuntia)**
MPEG-I/II streams	0 / 0
Lähetetyt / Vastaanotetut paketit	**Pakettien hävikki (% / kpl)**
23259 / 21930	5,4 / 1329
7. Mittaus	
Puskuri (millisekuntia)	**Kesto (sekuntia)**
100	660
Suoratoistoprotokolla	**Jitter keskiarvo / maksimi (millisekuntia)**
MPEG-I/II Audio	0 / 0
Lähetetyt / Vastaanotetut paketit	**Pakettien hävikki (% / kpl)**
23634 / 21970	6,6 / 1664

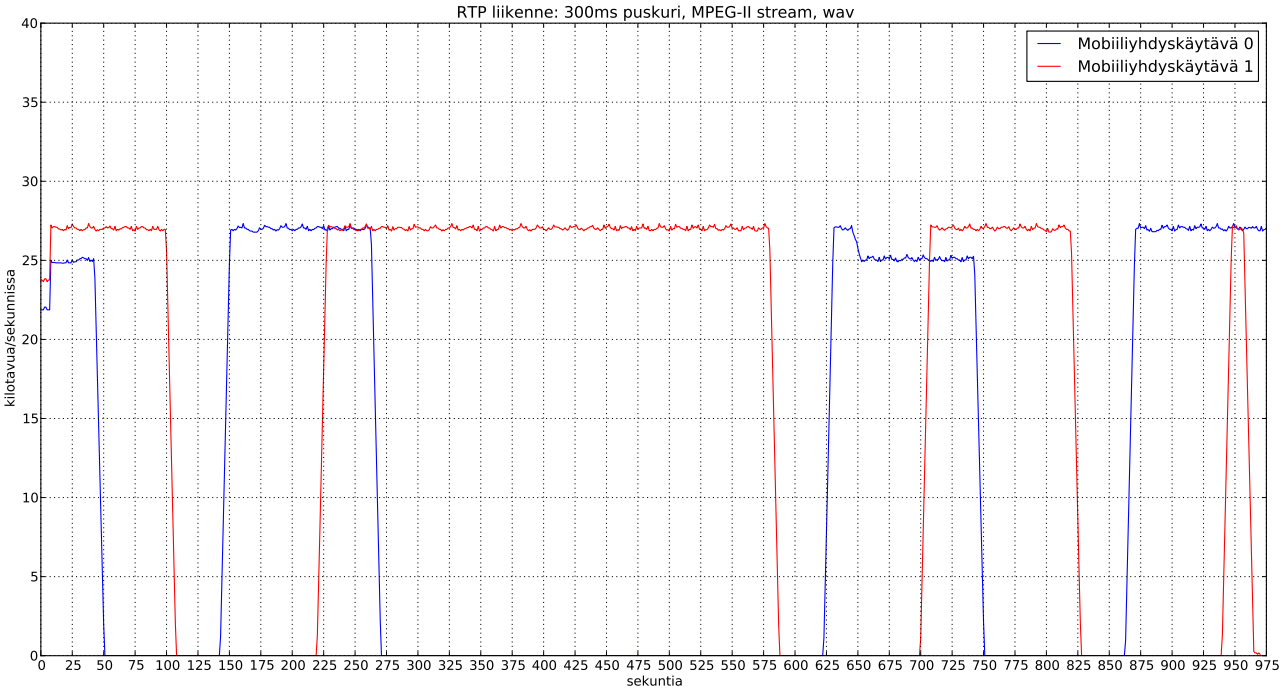
Taulukko 10: Äänensiirto mp3-tiedostolla RTP-protokollalla PMIPv6-verkon yli mobiililaitteelle. Katso liite C

Kuvassa 28 näkyy mobiililaitteen ja kuvassa 29 mobiiliyhdyskäytävien RTP-liikenne verkossa taulukon 8 1. mittauksen asetuksilla. Taulukossa 9 näkyy PMIPv6-verkon verkkoyksiköiden sidoskuittaus ajat 1. mittauksesta. Kuvissa ilmenevät piikit kuvastavat verkon liitäntäpisteen muutosta, tässä tapauksessa mobiiliyhdyskäytävän vaihtoa. Taulukoiden 8 ja 10 muiden mittauksien kuvat löytyvät liitteestä C. Liitteen C sekä 28, 29 ja 30 kuvissa on käytetty SMA (Simple Moving Average)-filtteriä, kahdeksan (8) otoksen liikkuvalla keskiarvolla. Alunperin testaukseen suunniteltussa SIP-protokollassa ilmeni, ettei kyseinen protokolla tue verkon liitäntäpisteen vaihtoa istunnon aikana vaan katkaisee automaattisesti yhteyden liitäntäpisteen vaihtuessa. RTP-protokolla käyttää yhteydettömän UDP-protokollan lisäksi myös TCP-protokollaa, joka keskittyy ajan sijasta yhteyden eheyteen. Suoritetuissa testeissä liikenne kuljetettiin verkon yli UDP-protokollan avulla mobiililaitteelle.

Testejä jatkettiin suoratoistamalla liikenöinnintikumppanilta, joka sijaitsi PMIPv6-domainin ulkopuolella, HTTP-protokollan yli 480p videokuvaa. Mobiililaite, joka sijaitsi PMIPv6-domainissa, yhdisti kyseiseen suoratoisto tiedonsiirtoon ja liikkui mobiiliyhdyskäytävien välillä. Kun puskuriksi asetti 200ms, ei verkon liitäntäpisteen vaihtoa huomannut ollenkaan kuvan- tai äänenlaadussa. Puskurin ollessa 0ms, verkonvaihdon yhteydessä vain kuvassa ilmeni hieman viivettä, äänenlaadun pysyessä normaalina.



Kuvio 28: Mobiililaitteen RTP-liikenne



Kuvio 29: Mobiiliyhdyskäytävien RTP-liikenne

4.1.3 Testiympäristössä ilmenneet ongelmat

Testiympäristön testaukseen oli myös tarkoituksena ottaa Android-puhelin (Samsung Galaxy S ja SII), mutta ilmeni virheitä jotka haittaavat Android-käyttöjärjestelmän käyttöä IPv6-verkossa. Android-käyttöjärjestelmää käyttävät laitteet (testattiin myös puhelimien lisäksi Asus TF300 tabletilla) eivät suostuneet liittymään PMIPv6-verkkoon ilman, että asetti IPv4-osoitteeksi 0.0.0.0 verkkomaskilla 0.0.0.0. Tilanteessa jossa IPv4-osoite kenttä jätettiin tyhjäksi, mobiililaite ei edes yrittänyt yhdistää IPv6-verkkoon. Android on siis vielä riippuvainen IPv4-protokollasta. Ohessa googlelle jätettyjä virheraportteja Android-käyttäjärjestelmässä havaituista ongelmista:

Puuttellinen tuki langattomiin IPv6-verkkoihin yhdistämisessä.[4]

Yhdistettäessä verkkoon, joka toimittaa vain IPv6 yhteyden, mobiililaite yhdistyy verkon liitäntäpisteeseen oikein, vastaanottaa IPv6 osoitteen ja oletusreitin, näin ollen täysin yhdistety verkkoon. Yhteys toimii vain hetken sillä Android käyttöjärjestelmä odottaa DHCPv4 vastausta. Määrätyn ajan jälkeen jos vastaust DHCPv4 kyseleen ei saatu, mobiililaite katkaisee yhteyden liitänpisteeseen ja menettäen näin yhteyden verkkoon. Hetken kuluttua se yrittää muodostaa yhteyttä uudelleen ja tämä toistuu loputtomasti.

Liitäntäpisteen nimi (Access Point Name, APN) protokollan sivuuttaminen liikkuessa.[5]

Virhe ilmenee kun APN protokollan kenttään asetetaan arvo *IPv4/IPv6* tai *IPv6*. Mobiilialitteen liikkuessa verkon alueella mobiililaite sivuuttaa pyydetyn protokollan ja aina kysyy pakettidataprotokollan (Packet Data Protocol, PDP) IP-tyypin sisältöä, joka vastaa APN protokollan tyyppiä *IPv4*

ICMPv6-reititinmainostusviestien ja muun multicast liikenteen toistuva sivuuttaminen.[6]

Perinteisessä IPv6-verkossa reitittimet lähettävät ICMPv6-reititinmainostusviestejä kaikille verkon solmuille tietyin väliajoin. Kyseinen toiminta nollaa IPv6-osoitteiden ja oletusreitittimen laskurin. Andoid-käyttöjärjestelmä alkaa sivuuttamaan kyseisiä viestejä ollessaan hetken yhdistettynä verkkoon. Kyseinen sivuutus aiheuttaa IPv6-yhteyden menetyksen.

[4] `http://code.google.com/p/android/issues/detail?id=32630`

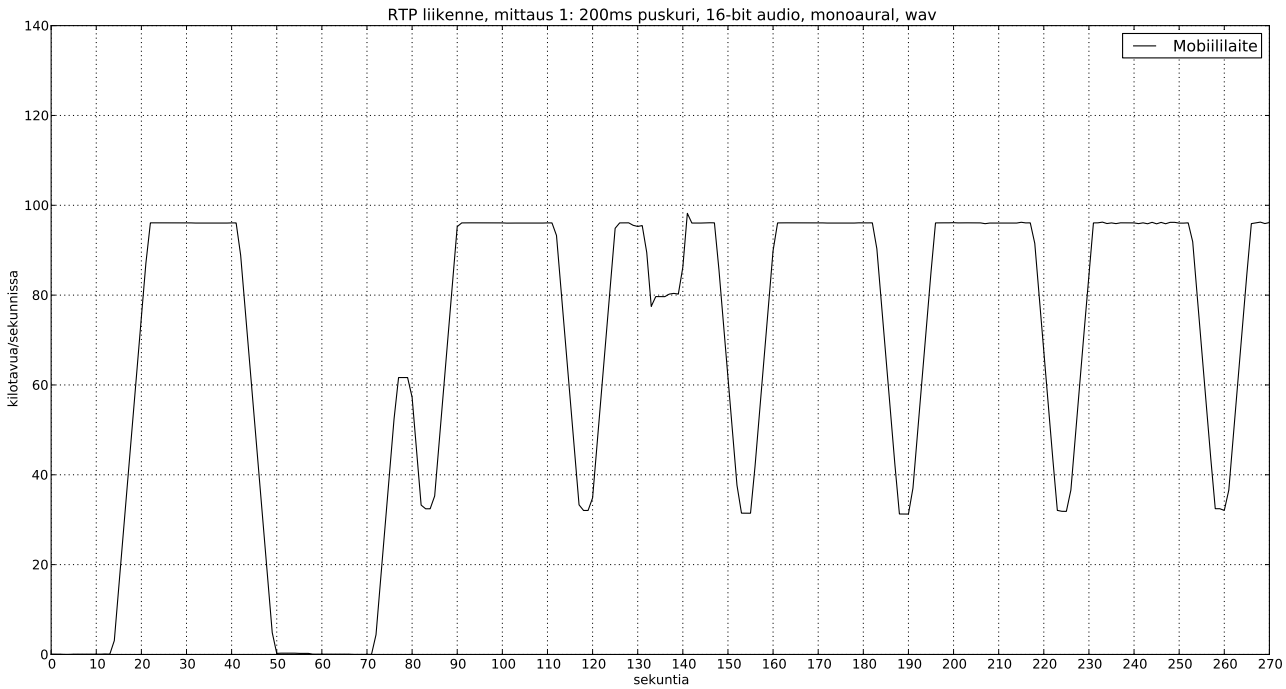
[5] `http://code.google.com/p/android/issues/detail?id=32631`

[6] `http://code.google.com/p/android/issues/detail?id=32662` viitattu 26.11.2012

Tiedostomuoto .wav	
Puskuri (millisekuntia)	**Kesto (sekuntia)**
200	275
Suoratoistoprotokolla	**Jitter keskiarvo / maksimi (millisekuntia)**
16-bit audio, monoaural	20,44 / 51,24
Lähetetyt / Vastaanotetut paketit	**Pakettien hävikki (% / kpl)**
16353 / 11256	23,8 / 5097

Taulukko 11: Äänensiirto wav-tiedostolla RTP-protokollalla PMIPv6-verkon yli mobiililaitteelle.

Taulukossa 11 on Samsung Galaxy SII:lla tehty mittaus ja siitä piirretty kuva 30. Mittauksia saatiin mutta sidospäivityksen elinajan ollessa yli 15 sekuntia, puhelin oli yhteydessä mobiiliyhdyskäytävään, jolloin tunneli sen ja mobiililiitoksen välillä pysyi pystyssä mutta liikkuessa PMIPv6-verkon alueella puhelin ei vaihtanut mobiiliyhdyskäytävästä toiseen. Sidospäivityksen elinajan asettaessa 10 sekunniksi, puhelin vaihtoi PMIPv6-verkon liitäntäpistettä heti lähetyttäessä toista mobiiliyhdyskäytävää. Sidospäivityksen ollessa 10 sekuntia ongelmaksi koitui tunnelin tuhoutuminen ja uudelleen luonti aina verkon liitäntäpisteen vaihtuessa, josta aiheutui suuri pakettihävikki.



Kuvio 30: Mobiililaitteen (Samsung Galaxy SII) RTP-liikenne

5 Liikkuvuudenhallinnan nykyhetki ja tulevaisuus

PMIPv6-protokolla pyrkii tilanteeseen, jossa mobiililaitteelle ei tarvitse asentaa ohjelmia tai tehdä muutoksia, toisin kuin MIPv6-protokollassa, jossa mobiililaitteella luodaan protokollan mukainen IP-tunneli kotiagentin kanssa. Testiympäristöä toteuttaessa kävi selväksi kuinka vajavainen tuki laitteilla ja ohjelmistoilla IPv6-protokollalle on. Tästä syystä joutui useamman kerran tekemään poikkeavia ratkaisuja, jotta testiympäristön toteuttaminen puhtaasti IPv6-protokollalla oli mahdollista. Tämä tutkimus on osa suurempaa kokonaisuutta, jonka lähtökohtainen lähestymistapa ja päämäärä on, että tehdään mahdollisimman vähän muutoksia loppukäyttäjän mobiililaitteeseen ja mahdollistetaan palveluntarjoajan palveluiden sekä käyttäjien hallinnan ja priorisoinnin tehokas käyttö. Liikkuvuuden- ja palvelunhallinnan tehostamisen tarkoituksena on mahdollistaa yhtäaikaiset yhteydet mobiililaitteille, jotta kyseinen skenaario olisi käytännössä mahdollista mobiililaitteelta tulee löytyä eri rajapintoja joita voi käyttää olemassa ja vapaana olevien verkkojen yhdistämiseen. Yhtäaikaisten yhteyden tuoma hyöty on siinä, että kun siirrytään yhteydestä toiseen, vanhan ollessa vielä yhdistettynä siihen pisteeseen asti kunnes uusi yhteys on muodostettu, ei käyttäjän yhteys missään vaiheessa katkea ja yhteydensiirto on huomaamaton. Yhtäaikaisten yhteyksien mahdollisuuksista hyötyvät myös palveluntarjoajat, nykypäivänä on yhä enemmän tarjolla erilaisia yhteystekniikoita joita hyväksikäyttämällä palveluntarjoajat pystyvät hallinnoimaan ja priorisoimaan verkossa tapahtuvaa liikennettä sekä helpottamaan tiettyjen verkkojen kuormitusta. Palveluntarjoajan ja tietysti loppukäyttäjän näkökulmasta tietoturva on aina iso osa kokonaisuutta. Testiympäristössä käytettiin IPsec-tunnelilointia pakettivirtojen salaamiselle mobiililiitoksen ja mobiiliyhdyskäytävän välillä. Toisin kuin MIPv6-protokollassa, PMIPv6-verkossa mobiililaitteen lähettämät viestit eivät sisällä kotiosoitteen päämäärää tai tyypin 2 reititys ylätunnistetta, jonka seuraksena erillistä suojausta niiden välille ei tarvita. Halutessaan mobiililaitteen ja mobiiliyhdyskäytävän välinen liikenne voidaan tunneloimalla suojata, jos dataliikenteen suojaus koetaan tarpeelliseksi.

5.1 Proxy Mobile IPv6 -protokollan kehitys

Koska PMIPv6 sallii useita mobiiliitoksia saman domainin sisällä, on mahdollista, että mobiililaitteen eri rajapinnat ovat kytkeytyneet eri mobiililiitoksiin. Tätä varten on kehitteillä IETF:n luonnos, joka ehdottaa vaihtoehdon tietovirran liikkuvuuteen usean mobiililiitoksen ympäristössä, kehitystä kuvaavat netext[1] -työryhmän työ jossa näkyy 3GPP EPC yhteistyö.(Xue et al. 2012) Erilaiset skenaariot eri rajapintojen ja mobiiliyhdyskäytävien välillä usean mobiililiitoksen ympäristössä eivät voi käyttää perinteistä tapaa olemassaolevien rajapintojen tietovirtojen liikkuuvuudenhallintaan. Luonnos olettaa mobiililaitteen käyttävän loogista rajapintaa, joka piilottaa fyysisen rajapinnan siirtokerroksen implementointien avulla IP-pinoilta ja muilta verkkoon yhdistyneiltä verkkosolmuilta. Verkon etuliitteet tietyiltä tietovirroilta siirretään erillisille fyysisille rajapinnoille välittämättä määrätyistä etuliitteistä kyseisissä rajapinnoissa.

Usean mobiililiitoksen ympäristössä jokainen mobiililiitos hallinnoi eri mobiiliyhdyskäytäväryhmiä, kuitenkaan se ei ole tietoinen muihin mobiililiitoksiin rekisteröityneistä mobiiliyhdyskäytävistä eikä niihin kytketyistä vastaavista rajapinnoista. Tästä syystä tietty mobiililiitos ei voi kommunikoida toisen mobiililiitoksen mobiiliyhdyskäytävän kanssa ilman kyseisen mobiililiitoksen apua. Määrittelyssä valitut tietovirrat eivät vaihda valittua mobiililiitosta, mutta mobiililaitteen ja siihen liittyvien mobiiliyhdyskäytävien asetukset tulisi asettua oikein. Käytäntöpolitiikka tulisi sijaita PMIPv6-domainiin yhdistetyllä AAA-palvelimella (Authentication, Authorization, Accounting), joka ylläpitää kaikkien samassa domainissa sijaitsevien, mobiililiitoksien rajapintojen osoitteita.(Xue et al. 2012) (Korhonen, Gundavelli et al. 2012) Tietovirran liikkuvuuden skenaariot usean mobiililiitoksen ympäristössä ovat seuraavanlaiset:

Eri rajapinnat jaetulla mobiiliyhdyskäytävällä.

Mobiililaitteen rajapinnat ovat kytkeytyneet samaan mobiiliyhdyskäytävään mutta tietovirrat ovat kytkeytyneet eri mobiililiitoksiin. Tietovirta voi muuttua mobiililaitteen ja mobiiliyhdyskäytävän välillä muttei mobiiliyhdyskäytävän ja mobiililiitoksen välille pakettien kuljettamista varten luotu tunneli. Ainoastaan mobiiliyhdyskäytävä päivittää reititystilaansa, eikä siten muuta liikennöintiä mobiiliyhdyskäytävän ja mobiililiitok-

[1] http://datatracker.ietf.org/wg/netext/

sen välillä tarvita.

Eri rajapinnat eri mobiiliyhdyskäytävillä.

Mobiililaitteen rajapinnat ovat kytkeytyneet eri mobiiliyhdyskäytäviin ja mobiililiitoksiin. Jokaisella mobiiliyhdyskäytävällä on vain tieto siihen liitetyistä rajapinnoista ja jokainen mobiililiitos ylläpitää tietoa siihen kytketyistä mobiiliyhdyskäytävistä. Tietovirran siirtyessä uuteen polkuun luodaan uusi tunneli käytössä olevan mobiililiitoksen ja uuden mobiiliyhdyskäytävän välille. Mobiililiitos, joka pysyy muuttumattomana, ei ole tietoinen uuden mobiiliyhdyskäytävän vastaavasta rajapinnasta toisessa polussa, jonka takia se tarvitsee apua toiselta mobiililiitokselta. Mahdollistaakseen tietovirran liikkuvuuden mobiililiitoksen tulee lähettää Policy Profile -pyyntö etsiäkseen toisesta mobiililiitoksesta mobiililaitteen tunnisteelle (Mobile Node Identifier, MN-ID) kuuluva oikea rajapinta.

PMIPv6 sallii mobiililaitteen yhdistää samaan PMIPv6-domainiin käyttäen eri rajapintoja. IETF:llä on kehitteillä luonnos, joka ehdottaa lisäystä PMIPv6-protokollaan mahdollistaakseen tietovirran liikkuvuudenhallinnan mobiililiitoksen ja mobiiliyhdyskäytävän välillä siten mahdollistaaksen tiettyjen tietovirtojen jakamisen fyysisille rajapinnoille. Oletetaan, että mobiililaitteen IP-kerroksen rajapinta osaa samanaikaisesti ja/tai peräkkäin liittyä useisiin mobiiliyhdyskäytäviin, mahdollisesti käyttäen eri yhteystapoja. Osassa tietovirtojen liikkuvuuden skenaarioissa mobiililaite voi jakaa osoitteita tietystä osoiteavaruudesta fyysisten rajapintojen kanssa, kun taas osassa mobiililaite asettaa osoitteet eri osoiteavaruuksista jokaiselle fyysiselle rajapinnalle. Luonnos esittelee uuden muuttujan, yhteydensiirron osoittimen arvon (Handoff Indicator Value), joka ilmaisee mobiililiitokselle että samat osoitteistot tulee kiinnittää mobiililaitteelle.(Bernardos, Calderon ja Soto 2012) Liikkuvan tietovirran skenaariot ovat seuraavanlaiset:

Jaettu osoite tai jaetut osoitteet istuntojen välillä.

Uuden rajapinnan liittyessä PMIPv6-verkkoon se jakaa jo olemassa olevan osoitteen tai osoitteet toisen istunnon kanssa. Kyseinen toiminta ei ole oletuksena PMIPv6-protokollassa ja mobiililiitoksen tulee kyetä tarjoamaan kiinnitys samaan yhteyteen, joka näin ollen poikkeaa yhteydensiirron skenaariosta. Kyseinen skenaario tarvitsee lisäystä PMIPv6-protokollan signalointiin uuden kytkennän tapahtuessa jolla varmis-

tetaan mobiililaitteen rajapintoihin jaetun osoitteen tai jaettujen osoitteiden samanaikainen kytkentä. Muuta signalointia mobiililiitoksen ja mobiililaitteen välillä ei tarvita. Tietovirrat lähetetään eteenpäin mobiililaitteelle ja mobiililiitokselle asetettujen määritelmien mukaan. Mobiililiitoksen tulee tietää milloin asettaa jaettuja osoitteita mobiililaitteen eri rajapinnoille.

Uusi osoite tai uudet osoitteet istunnolle.

Uuden rajapinnan liittyessä PMIPv6-verkkoon, se saa uuden osoitteen tai uudet osoitteistot istunnolle, joka toimii PMIPv6:ssa oletuksena. Tietovirran siirtäminen liitäntöjen välillä vaatii erityistä signalointia mobiililiitoksen ja mobiiliyhdyskäytävän välillä. Mobiiliyhdyskäytävien tulee olla tietoisia mobiililaitteen osoitteista johon se vastaanottaa liikennettä jotta paikalliset reitit ykset osataan asettaa oikein. Siinä tapauksessa jos tietovirta siirretään sen oletuspolulta toiseen mobiililiitoksen, joka on määritelty määränpääosoitteella, tulee luoda viesti uudelle mobiiliyhdyskäytävälle tietovirran liikkeestä (Flow Mobility Indicator, FMI).

Jaettuja ja uusia osoitteita istuntojen välillä.

Uuden rajapinnan liittyessä PMIPv6-verkkoon, se saa yhdistelmän käytössä olevia osoitteita ja uusia osoitteita. Kyseessä on kahden yllä mainitun skenaarion yhdistelmä. Paikallinen määrittely päättää, käytetäänkö uusia osoitteita pelkästään uudelle istunnolle vai voiko sitä jakaa jo olemassa olevan istunnon kanssa. Mobiililaite on jo kytkeytynyt PMIPv6-domainiin mobiiliyhdyskäytävän kautta. Jossain vaiheessa mobiililaite yhdistää uuden rajapinnan toiseen mobiiliyhdyskäytävään, joka lähettää proxysidospäivityksen jonka avulla mobiililiitos mahdollistaa tietovirran liikkuvuuden.

Mobiililiitoksessa ja mobiililaitteessa tulisi olla paikallisasetukset kunnossa, jotta pakettien johdonmukainen eteenpäin lähettäminen toimii yksi- ja kaksisuuntaisissa yhteyksissä.(Bernardos 2012)(Tsirtsis et al. 2011)

6 Yhteenveto

Aloitin perehtymisen liikkuvuuden ja verkon rajapintojen hallintaan lukemalla kaksi väitöskirjaa aiheesta (Fekete 2012) ja (Mäkelä 2011). Niiden avulla sai hyvän yleiskuvan IPv6- ja liikkuvuudenhallintaprotokollien eduista verrattuna vanhaan IPv4-protokollaan. Aloitin tutkielman tekemisen dokumentoimalla liikkuvuudenhallintaprotokollien eroavaisuudet, hyödyt ja mahdollisuudet.

Aiheeseen tutustuttua aloitin testiympäristön toteutuksen, jossa MIPv6 reitityksen käytännön testaus erilaisilla skenaarioilla olisi mahdollista. Aiheesta löytyi muutama artikkeli (Al-Buraiky 2008) ja (umip.org 2010), joiden pohjalta lähdin testiympäristöä toteuttamaan. Koska aiheesta löytyi huonosti dokumentaatiota, pois lukien IETF:n tekemiä Request for Comments -dokumentaatioita (RFC), jotka sisältävät tekniset määrittelyt, jouduin yrityksen ja erehdyksen kautta konfiguroimaan verkkoa. MIPv6-testiympäristön toteuttamisessa mielenkiintoinen yksityiskohta oli, että kotiagenttina toiminut kannettava tietokone toimi myös vieraan verkon rajapintana.

Alusta asti suurin ongelma yhteyksien luomisessa oli saada toimimaan IPv6-protokollaa tukeva, liikkuvuusohjelmisto (mip6d). MIP Linux ympäristössä käsittää kaksi komponenttia, joista toinen toimii kernel- ja toinen käyttäjätasolla. Käyttäjätasoinen liikkuvuusohjelmisto käsittää useimmat toiminnot ja se myöskin havaitsee sijainnin, liikkeen, lähettää ja käsittelee sidospäivityksiä sekä ylläpitää sidosvälimuistia. Kernel-tason päivitys mahdollistaa muun muassa tuen mobiiliylätunnisteprotokollalle (Mobility Header protocol), joka on lisä IPv6 ylätunnisteeseen ja jota käytetään sidospäivityksien, sidoskuittauksien ja muiden sidoksiin liittyvien viestien kuljettamiseen. Toimivien liikkuvuusohjelmien ollessa koti- ja vieraskoneessa sekä mobiililaitteena toimivassa kannettavassa, seuraavaksi piti saada yhteys toimimaan laitteiden välillä. Yhteyden testaus tapahtui käyttämällä ping6- ja tracert6-työkaluja samanaikaisesti kun yhteyttä verkkoon vaihdettiin. Yhteydet verkkoyksiköiden ja mobiililaitteen välillä saatiin toimimaan salaamattomana ja IPsec salausta käyttäen.

Ensimmäinen toimiva yhteys saatiin IPsec salauksella ja tästä syystä juurikaan liikennettä koneiden välillä ei näkynyt. Kotiagenttina toimivan koneen liikkuvuusohjelmistossa ei

näkynyt mitään liikennettä tai tapahtumia, vaikka mobiililaite yhdisti siihen onnistuneesti. Mobiililaitteen liikkuvuusohjelmistossa sen sijaan näkyivät kaikki tapahtumat. Kotiagentin rajapinnoissa, LOCAL ja REMOTE, näkyi mobiililaitteen yhteyden luominen ja sen katkaiseminen. Sidospäivitykset näkyivät mobiililaitteen virtuaaliterminaalissa normaalisti toisin kuin kotiagentin virtuaaliterminaalissa, jossa ei näkynyt mitään merkkiä pakettien vaihdosta.

Salaamattoman yhteyden luominen ja sen seuranta tuotti luonnollisesti enemmän liikennettä ja tapahtumia. Tämän seurauksena myös kotiagentin liikkuvuusohjelmistossa näkyi tapahtumia, sidospäivityksiä ja sidoskuittauksia. Molemmissa tapauksissa, salaamatonta tai salattua yhteyttä käyttäen, mielenkiintoista oli ICMPv6 ping pakettien lähettäminen mobiililaitteelta. Mobiililaitteen ollessa yhdistettynä kotiverkkoon, vasteajat olivat 5-10 millisekunnin luokkaa. Mobiililaitteen yhdistettäessä vierasverkkoon jonka seurauksena mip6d otti tunnelin käyttöön vasteajat tippuivat 0.08-0.1 millisekuntiin, joka on murto-osa aiemmasta.

PMIPv6-protokolla pyrkii tilanteeseen, jossa loppukäyttäjän mobiililaitteelle ei tarvitse asentaa ohjelmia tai tehdä mitään muutoksia, toisin kuin MIPv6-protokollassa, jossa mobiililaite luo itse protokollan mukaisen IP-tunnelin kotiagentin kanssa.(Gundavelli et al. 2008) PMIPv6-testiympäristöä rakentaessa, MIPv6 ympäristön rakentamisesta saatu kokemus oli avuksi. Alunperin PMIPv6-testiympäristön luomiseen tarkoitetut laitteet vaihtuivat tarpeen mukaan. Loppujen lopuksi kaikki PMIPv6-verkon verkkoyksiköt olivat vaihtuneet sekä niiden välinen liikenne kuljetettiin verkkokaapeleita pitkin, aiemmin käytetyn langattoman vaihtoehdon sijaan. PMIPv6-testiympäristön ensimmäiset mittaukset suoritettiin kappaleen 4.1.1 mukaisesti ilman liikkuvuudenhallintaa, mikä antaa käsityksen verkon toiminnan ja tehokkuuden eroavaisuudesta verrattuna verkon toimintaan kappaleen 4.1.2 liikkuvuudenhallinnan kanssa. Huomioitavaa on kuitenkin se, että testeissä käytetyt laitteet erosivat toisistaan.

Työn ensimmäisenä osa-alueena oli liikkuvuudenhallinta. Testiympäristössä suoritetut testit liikkuvuudenhallinnalla osoittavat sen tehokkuuden ja hyödyn verrattuna. Haittana oli lievä pakettihävikki verkon liitäntäpisteen vaihtumisen aikana, kun mobiililiitos luo uuden tunnelin lähempänä olevan mobiiliyhdyskäytävän välille, ellei sellaista jo ole olemassa toisen mobiililaitteen liitäntäpisteen sijainnin johdosta. Kyseiseen ongelmaan on kehitteillä ratkaisu, joka mahdollistaa usean mobiililaitteen eri rajapintojen olevan yhtä aikaa käytössä ja yhdistettynä verkkoon, kuten on mainittu kappaleessa 5.1. Toinen mahdollinen ratkai-

su kyseiseen pakettihävikkiin verkon liitäntäpisteen vaihtuessa on käyttää kappaleen 2.3.6 FPMIPv6-protokollaa, jossa mobiiliyhdyskäytävät luovat välillensä tunnelin, johon mobiililaitteelle tarkoitetut paketit lähetetään mobiililaitteen vaihtaessa verkon liitäntäpistettä.

Työn toisena osa-alueena oli käyttäjän tunnistaminen, joka hoidettiin AAA-palvelimella. Mobiililaitteen tunnisteena käytettiin PMIPv6-verkon yhdistämiseen käyttämää rajapinnan tunnistetta, joka oli testiympäristön tapauksessa MAC-osoite. Käyttäjien tunnistautumisen, valtuutuksen ja kirjanpidon kanssa ei ilmennyt minkäänlaisia ongelmia ja se toimi ongelmitta testauksessa käytetyillä kannettavilla tietokoneilla, kännyköillä ja tabletilla ongelmitta. PMIPv6-verkkoon ei voinut yhdistää onnistuneesti ilman, että käyttäjää olisi lisätty mobiililiitoksella sijaitsevan radius-palvelimen tietokantaan.

Työn kolmantena osa-alueena oli tietoturva, joka on aina ajankohtainen ja aiheellinen aihe, kun on kyse mobiililaitteista tai tietoverkoista. Testiympäristö suojattiin IPsec-salauksella, jonka kanssa ei ilmennyt ongelmia. Kysymys siitä, miten mobiililaitteen ja PMIPv6-verkon väli suojataan, ei suoranaisesti kuulu tämän työn piiriin. Siihen on olemassa jo monia menetelmiä, kuten on nähtävillä kappaleessa 4.1.1 jossa käytettiin WPA-salausta mobiililaitteen ja mobiiliyhdyskäytävän välin suojaamiseen. Tässä työssä tähdättiin verkonhallintaan operaattorin näkökulmasta.

Jatkotutkimuksia ja verkon laajentamista varten ajatellen olisi hyvä implementoida PMIPv6-verkkoon IPv6-protokollaa tukeva reititysprotokolla kuten esimerkiksi Open Shortest Path First (OSPF) (Coltun et al. 2008), Border Gateway Protocol (BGP) (Marques ja dupont 1999) tai Routing Information Protocol (RIP) (Malkin ja Minnear 1997). Reititysprotokolla helpottaa verkonhallintaan. Kuten aikaisemmin mainittiin verkkopohjaisten liikkuvuuslaajennusten kehittämisen jatkumisesta aktiivisena netext työryhmässä, jonka alueeseen myös EPC verkot kuuluvat. Kyseisen työryhmän tehdyistä ja tekeillä olevista standardeista sekä luonnoksista ilmenee nykyisen kehityksen suunta, joka on saumattoman liikkuvuuden- ja tietovirtojenhallinta langattomien verkkojen välillä. Tästä syystä olisi luonnollista jatkaa tutkimusta kyseiseen suuntaan. Jatkotutkimus näin ollen keskittyisi verkon puolella tapahtuvaan tietovirtojenhallintaan ja sen priorisointiin sekä saumattomaan liikkuvuuteen eri verkkojen ja teknologioiden välillä. Tulisi myös tutkia, kuinka eri tietovirtojenhallintaa ja priorisointia voidaan hyödyntää loppukäyttäjän mobiililaitteen eri teknologioiden rajapinnoissa ja

miten sen toteuttaminen käytännössä olisi mahdollista. Tutkimuksen prioriteetti pysyy näin ollen verkkoperustaisessa liikkuvuuden- ja tietovirtojenhallinnassa, jonka lähtökohtana pysyy edelleen se ettei loppukäyttäjän mobiililaitteeseen tehdä muutoksia.

Lähteet

A, Patel, K. Leung, M. Khalil, H. Akhtar ja K. Chowdhury. 2005. *Mobile Node Identifier Option for Mobile IPv6 (MIPv6).* Internet Engineering Task Force. http://www.ietf.org/rfc/rfc4283.txt.

Arkko, J., G. Kuijpers, H. Soliman, J. Loughney ja J. Wiljakka. 2003. *Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts.* Viitattu 16.10.2012. Network Working Group. http://www.ietf.org/rfc/rfc3316.txt.

ASSOCIATION, IEEE STANDARDS. 2011. *Standard Group MAC Addresses: A Tutorial Guide.* Standardi, viitattu 23.11.2012. The institute of Electrical ja Electronics Engineers, Inc. http://standards.ieee.org/develop/regauth/tut/macgrp.pdf.

Bernardos, CJ. 2012. *Proxy Mobile IPv6 Extensions to Support Flow Mobility.* Luonnos, viitattu 26.11.2012. Internet Engineering Task Force. http://tools.ietf.org/id/draft-ietf-netext-pmipv6-flowmob-05.txt.

Bernardos, CJ., M. Calderon ja I. Soto. 2012. *PMIPv6 and Network Mobility Problem Statement.* Luonnos, viitattu 1.6.2012. Internet Engineering Task Force. http://tools.ietf.org/id/draft-bernardos-netext-pmipv6-nemo-ps-02.txt.

Bieringer, P. 2009. *Linux IPv6 HOWTO (en).* Viitattu viitattu 29. marraskuuta 2012. http://www.tldp.org/HOWTO/Linux+IPv6-HOWTO/index.html.

Al-Buraiky, S. 2008. "Mobile IPv6 with Linux". Viitattu viitattu kesäkuuta 2012. http://www.linuxjournal.com/magazine/mobile-ipv6-linux.

Coltun, R., D. Ferguson, J. Moy ja A. Lindem. 2008. *OSPF for IPv6.* Standardi, viitattu 23.11.2012. Network Working Group. http://tools.ietf.org/rfc/rfc5340.txt.

Deering, S. 1991. *ICMP Router Discover Messages.* Standardi, viitattu 21.11.2012. Network Working Group. http://www.ietf.org/rfc/rfc1256.txt.

Deering, S., ja R. Hinden. 1995. *Internet Protocol, Version 6 (IPv6) Specification.* Standardi, vanhentunut RFC 2460 toimesta. Network Working Group. http://www.ietf.org/rfc/rfc1883.txt.

———. 1998. *Internet Protocol, Version 6 (IPv6) Specification.* Standardi, viitattu 19.11.2012. Network Working Group. http://www.ietf.org/rfc/rfc2460.txt.

Devarapalla, V., R. Wakikawa, A. Petrescu ja P. Thubert. 2005. *Network Mobility (NEMO) Basic Support Protocol.* Standardi, viitattu 27.11.2012. Network Working Group. http://tools.ietf.org/rfc/rfc5340.txt.

Devarapalli, V., R. Koodli, H. Lim, N. Kant, S. Krishnan ja J. Laganier. 2010. *Heartbeat Mechanism for Proxy Mobile IPv6.* Internet Engineering Task Force. http://tools.ietf.org/rfc/rfc5847.txt.

Draves, R. 2003. *Default Address Selection for Internet Protocol version 6 (IPv6).* Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3484.txt.

Fekete, G. 2012. "Network Interface Management in Mobile and Multihomed Nodes". Tohtorinväitöskirja, Jyväskylän yliopisto.

Filipe, B., ja S. Santos. 2011. "Localized Mobility Management Protocol Implementation using PMIPv6" [**inlang** English]. Pro Gradu, Universidade de Aveiro. Viitattu viitattu 20. marraskuuta 2012. http://ria.ua.pt/bitstream/10773/7198/1/5456.pdf.

Firmin, F. 2008. "The Evolved Packet core". *The-Evolved-Packet-Core.* http://www.3gpp.org/The-Evolved-Packet-Core.

Gundavelli, S., K. Leung, V. Devarapalli, K. Chowdhury ja B. Patil. 2008. *Proxy Mobile IPv6.* Internet Engineering Task Force. http://www.faqs.org/rfcs/rfc5213.html.

Hinden, R., ja S. Deering. 1995. *IP Version 6 Addressing Architecture.* Standardi, vanhentunut RFC 2373 toimesta. Network Working Group. http://www.ietf.org/rfc/rfc1884.txt.

———. 2003. *Internet Protocol Version (IPv6) Addressing Architecture.* Standardi, viitattu 19.11.2012. Network Working Group. http://www.ietf.org/rfc/rfc3513.txt.

Kaufman, C., P. Hoffman, Y. Nir ja P. Eronen. 2012. *Internet Key Exchange Protocol Version 2 (IKEv2).* Internet Engineering Task Force. http://tools.ietf.org/rfc/rfc5996.txt.

Kent, S. 2005. *IP Encapsulating Security Payload (ESP).* Internet Engineering Task Force. http://tools.ietf.org/rfc/rfc4303.txt.

Kent, S., ja K. Seo. 2005. *Security Architecture for the internet Protocol.* http://www.faqs.org/rfcs/rfc4301.html.

Kim, M., ja S. Lee. 2009. "A novel load balancing scheme for PMIPv6-based wireless networks". *AEU - International Journal of Electronics and Communications.*

Kong, H., Y. Jang ja H. Choo. 2010. "An Efficient Load Balancing of Mobile Access Gateways in Proxy Mobile IPv6 Domains". *International Conference on Computational Science and Its Applications.*

Koodli, R. 2005. *Fast Handovers for Mobile IPv6.* Kokeellinen, viitattu 16.10.2012. Network Working Group. http://www.ietf.org/rfc/rfc4068.txt.

———. 2009. *Mobile IPv6 Fast Handovers.* Viitattu 21.9.2012. Network Working Group. http://tools.ietf.org/rfc/rfc5568.txt.

Korhonen, J., S. Gundavelli, H. Yokota ja X. Cui. 2012. *Runtime Local Mobility Anchor (LMA) Assignment Support for Proxy Mobile IPv6.* Internet Engineering Task Force. http://tools.ietf.org/rfc/rfc6463.txt.

Korhonen, J., J. Soininen, B. Patil, T. Savolainen, G. Bajko ja K. Iisakkila. 2012. "IPv6 in 3rd Generation Partnership Project (3GPP) Evolved Packet System (EPS)". Internet Engineering Task Force. Viitattu viitattu 27. marraskuuta 2012. http://tools.ietf.org/rfc/rfc6459.txt.

Mäkelä, J. 2011. "Mobility Management in Heterogeneous IP-networks". Tohtorinväitöskirja, Jyväskylän yliopisto.

Malkin, G., ja R. Minnear. 1997. *RIPng for IPv6.* Standardi, viitattu 23.11.2012. Network Working Group. http://tools.ietf.org/rfc/rfc2080.txt.

Marques, P., ja F. dupont. 1999. *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*. Standardi, viitattu 23.11.2012. Network Working Group. http://tools.ietf.org/rfc/rfc2545.txt.

MSDN. 2010. *Multicast IPv6 Addresses.* Viitattu 19.11.2012. Microsoft. http://msdn.microsoft.com/en-us/library/aa924142.aspx.

Narten, T., R. Draver ja S. Krishnan. 2007. *Privacy Extensions for Stateless Address Autoconfiguration in IPv6.* Standardi, viitattu 21.11.2012. Network Working Group. http://tools.ietf.org/rfc/rfc4941.txt.

Paxson, V., M. Allman, J. Chu ja M. Sargent. 2011. *Computing TCP's Retransmission Timer.* Standardi, viitattu 21.11.2012. Network Working Group. http://tools.ietf.org/rfc/rfc6298.txt.

Perkins, C., D. Johnson ja J. Arkko. 2011. *Mobility Support in IPv6.* Internet Engineering Task Force. http://www.ietf.org/rfc/rfc6275.txt.

Postel, J. 1981. *Internet Protocol.* Standardi, viitattu 19.11.2012. DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION. http://www.ietf.org/rfc/rfc791.txt.

Ridruejo, D. 2000. *The Linux Networking Overview HOWTO.* Viitattu viitattu 21. marraskuuta 2012. http://www.linuxdoc.org/HOWTO/Networking-Overview-HOWTO.html.

Society, IEEE Computer. 2002. *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.* Standardi, viitattu 23.11.2012. The institute of Electrical ja Electronics Engineers, Inc. http://standards.ieee.org/getieee802/download/802-2001.pdf.

Soliman, H., C. Castellunccia, K. Elmalki ja L. Bellnier. 2008. *Hierarchical Mobile IPv6 (HMIPv6) Mobility Management.* Network Working Group. http://tools.ietf.org/rfc/rfc5380.txt.

Tsirtsis, G., H. Soliman, N. Montavont, G. Giaretta ja K. Kuladinithi. 2011. *Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support.* Internet Engineering Task Force. http://tools.ietf.org/rfc/rfc6089.txt.

umip.org. 2010. *How to setup a Mobile IPv6 testbed with IPsec static keying.* http://umip.org/docs/umip-mip6.html.

www.archlinux.org. 2012. *IPv6.* This article covers IPv6, and basics of configuring different IPv6 related things like static IP adresses. Viitattu viitattu 21. marraskuuta 2012. https://wiki.archlinux.org/index.php/IPv6.

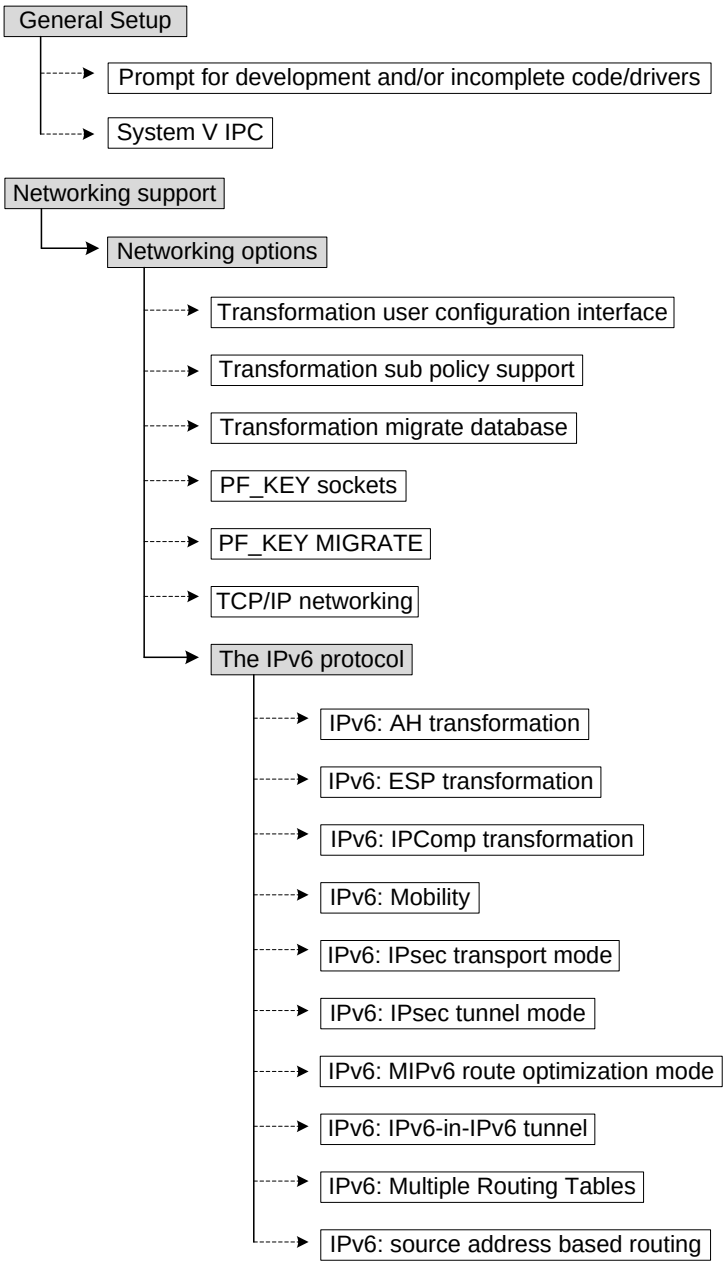
Xue, K., D. Ni, P. Hong ja H. Chan. 2012. *Multi-LMA flow mobility.* Luonnos, viitattu 16.10.2012. Internet Engineering Task Force. http://www.ietf.org/id/draft-xue-netext-flowmo-multilma-00.txt.

Yukota, H., K. Chowdhury, R. Koodli, B. Patil ja F. Xia. 2010. *Fast handover for Proxy Mobile IPv6.* Viitattu 21.9.2012. Internet Engineering Task Force. http://tools.ietf.org/rfc/rfc5949.txt.

Liitteet

A Kernelin mobiilitukiasetukset

Jotta mobiilituki tulee käyttöön kerneliä tulee muokata kuvan 31 asetuksien mukaisesti.



Kuvio 31: Kerneliin asetettavat mobiilitukiasetukset

B MIPv6 sidospäivityslista ja sidosvälimuisti

Asetuskuvassa 6.1 on koti- ja vierasagentin sidosvälimuisti ja asetuskuvassa 6.2 on mobiililaitteen sidospäivityslista.

```
$ telnet localhost 7777
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
mip6d> verbose yes
yes
mip6d> hal
wlan0 2001:db8:0:0:0:0:0:0
preference 10 lifetime 1800
mip6d> stats
Input Statistics:
6 Mobility Headers
0 HoTI messages
0 CoTI messages
0 HoT messages
0 CoT messages
3 BU messages
0 BA messages
0 BR messages
0 BE messages
0 DHAAD request
0 DHAAD reply
0 MPA
0 MPS
0 Home Address Option
0 unverified Home Address Option
0 Routing Header type 2
0 reverse tunnel input
0 bad MH checksum
0 bad payload protocol
0 unknown MH type
0 not my home address
0 no related binding update entry
0 home init cookie mismatch
0 careof init cookie mismatch
0 unprotected binding signaling packets
0 BUs discarded due to bad HAO
0 RR authentication failed
0 seqno mismatch
0 parameter problem for HAO
0 parameter problem for MH
0 Invalid Care−of address
0 Invalid mobility options
Output Statistics:
9 Mobility Headers
0 HoTI messages
```

```
0 CoTI messages
0 HoT messages
0 CoT messages
0 BU messages
3 BA messages
0 BR messages
6 BE messages
0 DHAAD request
0 DHAAD reply
0 MPA
0 MPS
0 Home Address Option
0 Routing Header type 2
0 reverse tunneled input
mip6d> thread
bu: 0
mip6d>
```

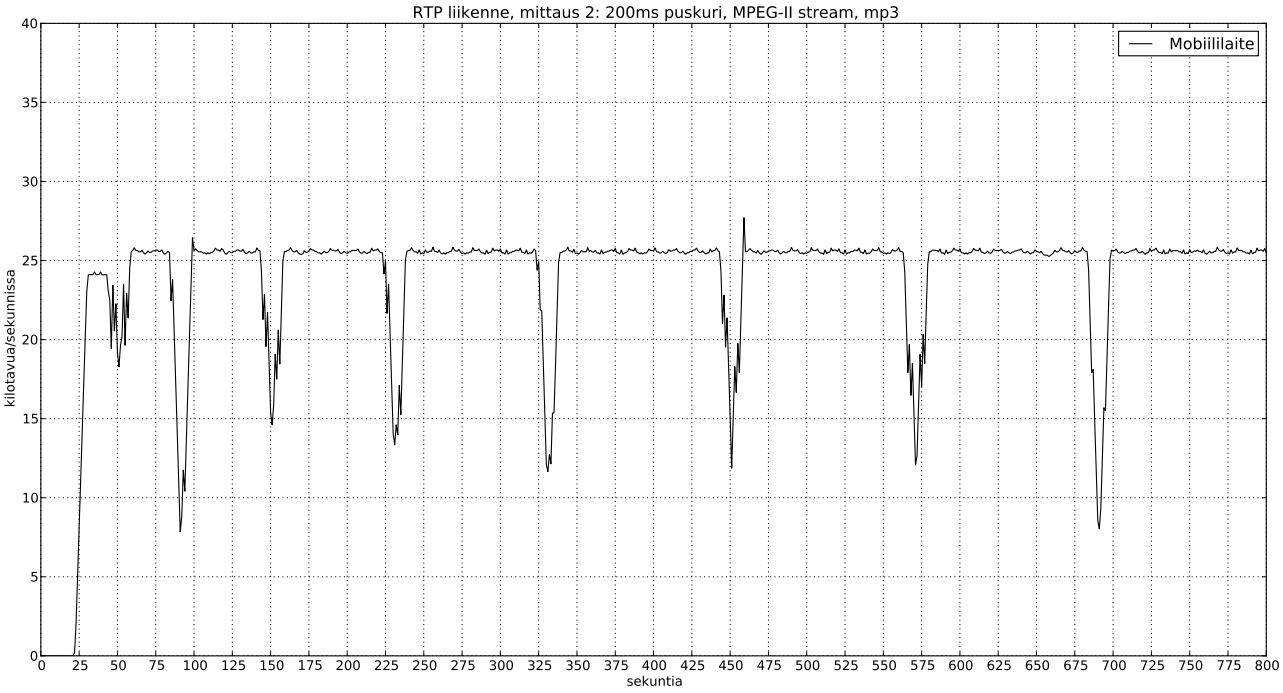
Asetus 6.1: MIPv6 Koti- ja vierasagentin sidosvälimuisti

```
$ telnet localhost 7777
Trying ::1...
Connected to localhost.
Escape character is '^]'.
mip6d> stats
Input Statistics:
2 Mobility Headers
0 HoTI messages
0 CoTI messages
0 HoT messages
0 CoT messages
0 BU messages
0 BA messages
0 BR messages
1 BE messages
0 DHAAD request
0 DHAAD reply
0 MPA
0 MPS
0 Home Address Option
0 unverified Home Address Option
0 Routing Header type 2
0 reverse tunnel input
0 bad MH checksum
0 bad payload protocol
0 unknown MH type
0 not my home address
0 no related binding update entry
0 home init cookie mismatch
0 careof init cookie mismatch
0 unprotected binding signaling packets
0 BUs discarded due to bad HAO
```

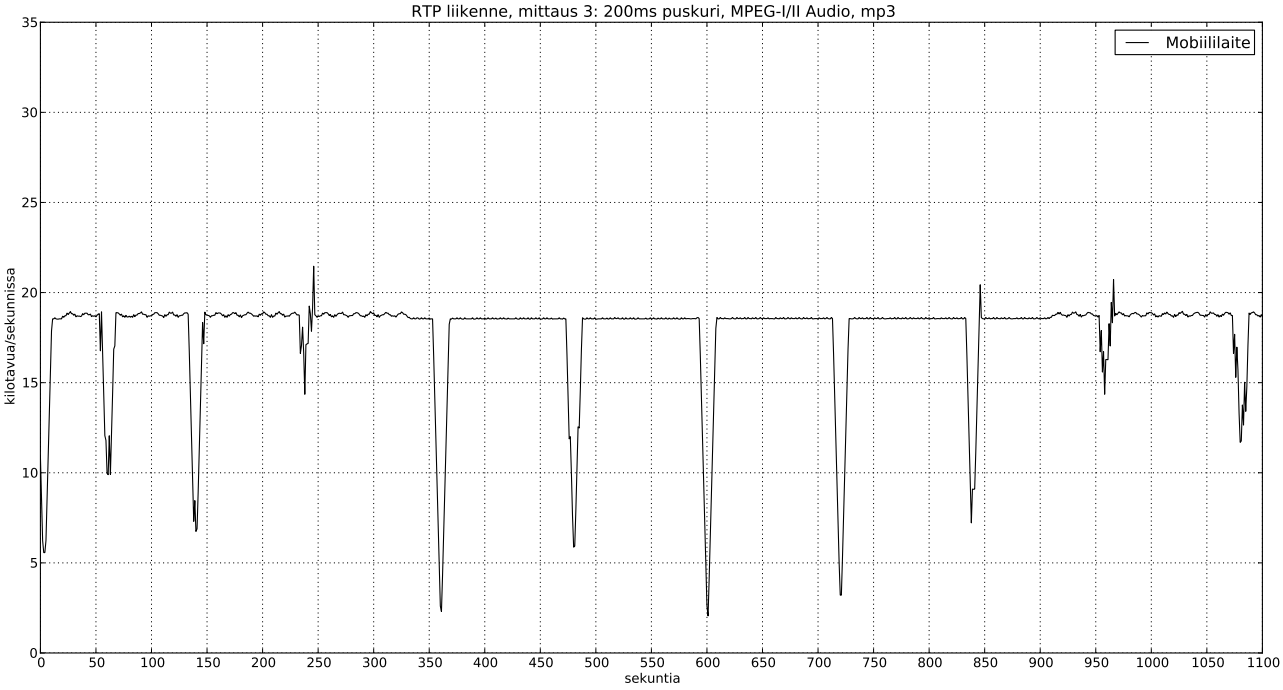
```
0 RR authentication failed
0 seqno mismatch
0 parameter problem for HAO
0 parameter problem for MH
0 Invalid Care−of address
0 Invalid mobility options
Output Statistics:
24 Mobility Headers
0 HoTI messages
0 CoTI messages
0 HoT messages
0 CoT messages
24 BU messages
0 BA messages
0 BR messages
0 BE messages
0 DHAAD request
0 DHAAD reply
0 MPA
0 MPS
0 Home Address Option
0 Routing Header type 2
0 reverse tunneled input
mip6d> help
bc bul fancy nonce prompt quit rr stats verbose
mip6d> verbose yes
yes
mip6d> bul
== NON_MIP_CN_ENTRY ==
Home address 2001:db8:0:0:0:0:0:dd
Care−of address 0:0:0:0:0:0:0:0
CN address 2001:db8:0:0:0:0:0:0
lifetime = 420, delay = 420000
flags: IP6_MH_BU_HOME IP6_MH_BU_ACK
ack ready
dev (0) last_coa 2001:db8:0:0:0:0:0:dd
lifetime 415 / 420 seq 61349 resend 0 delay 420(after 415s) expires −
```

Asetus 6.2: Mobiililaitteen sidospäivityslista

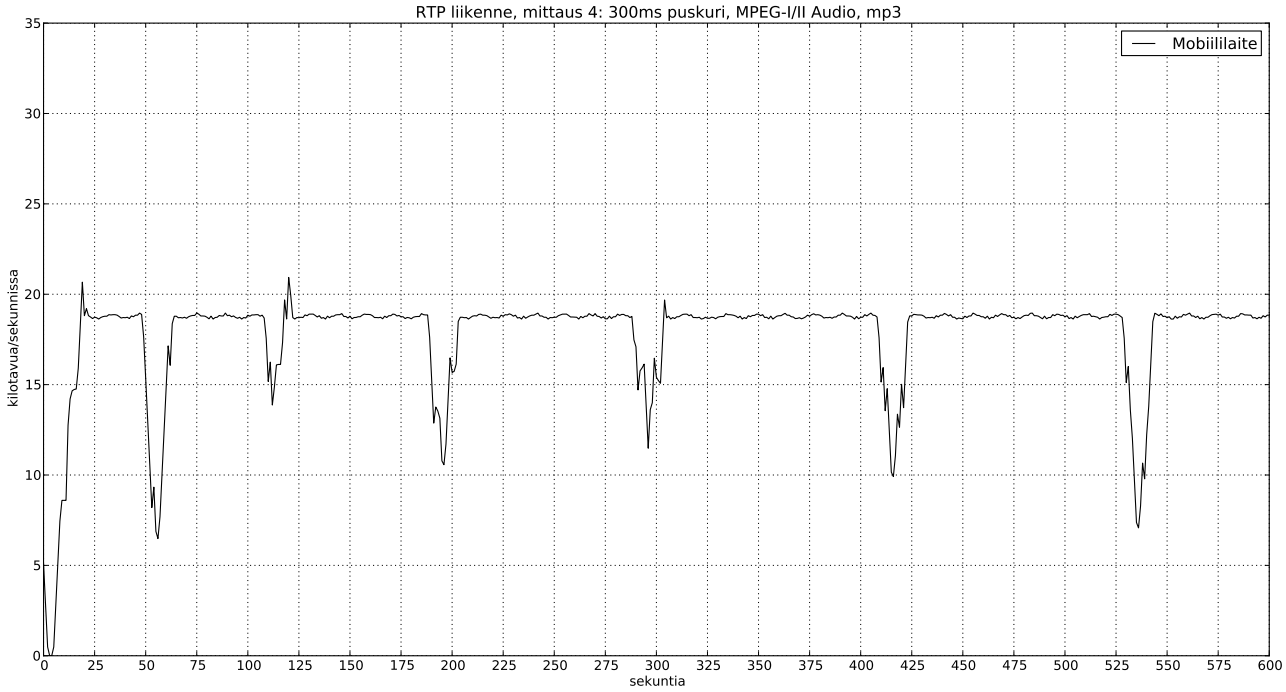
C RTP-liikenteen kuvat



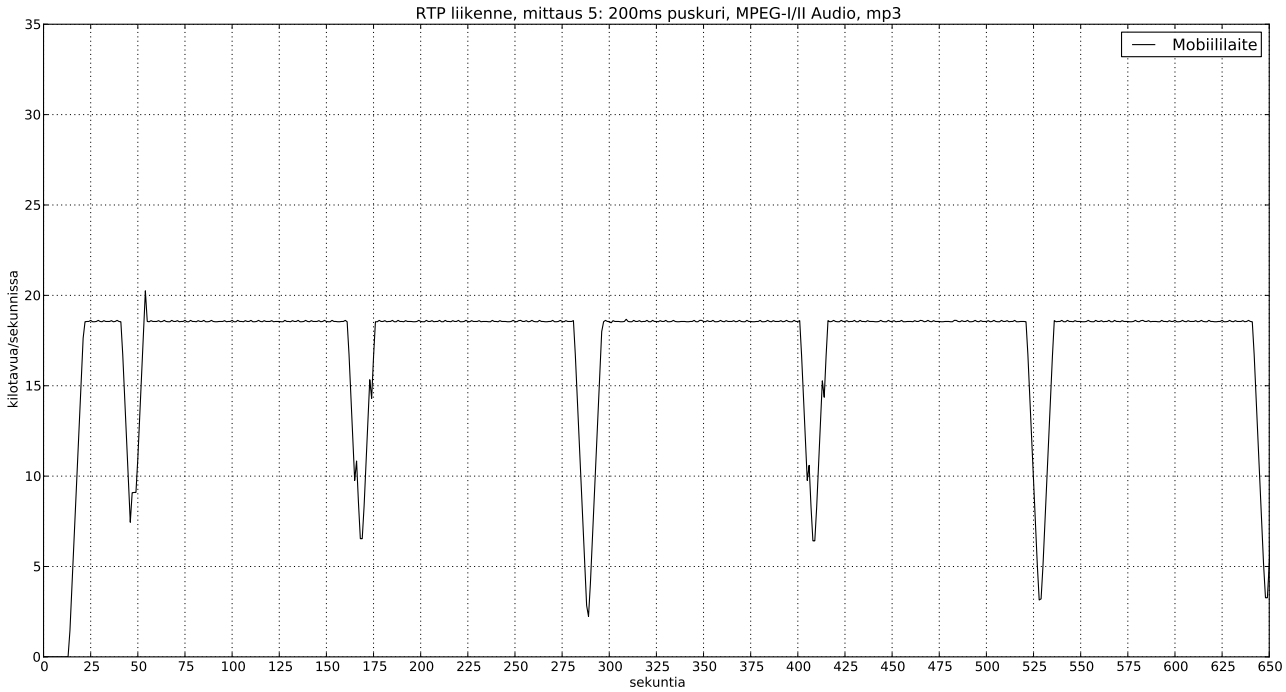
Kuvio 32: Mobiililaitteen RTP-liikenne, 2. mittaus



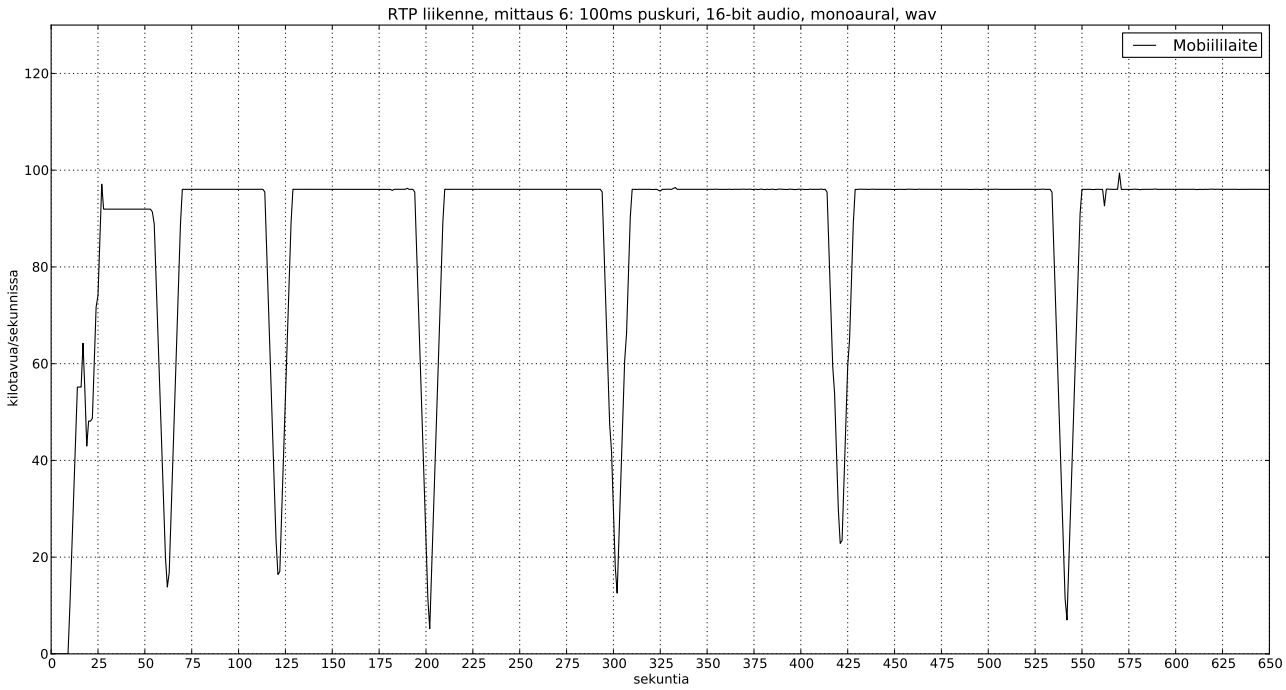
Kuvio 33: Mobiililaitteen RTP-liikenne, 3. mittaus



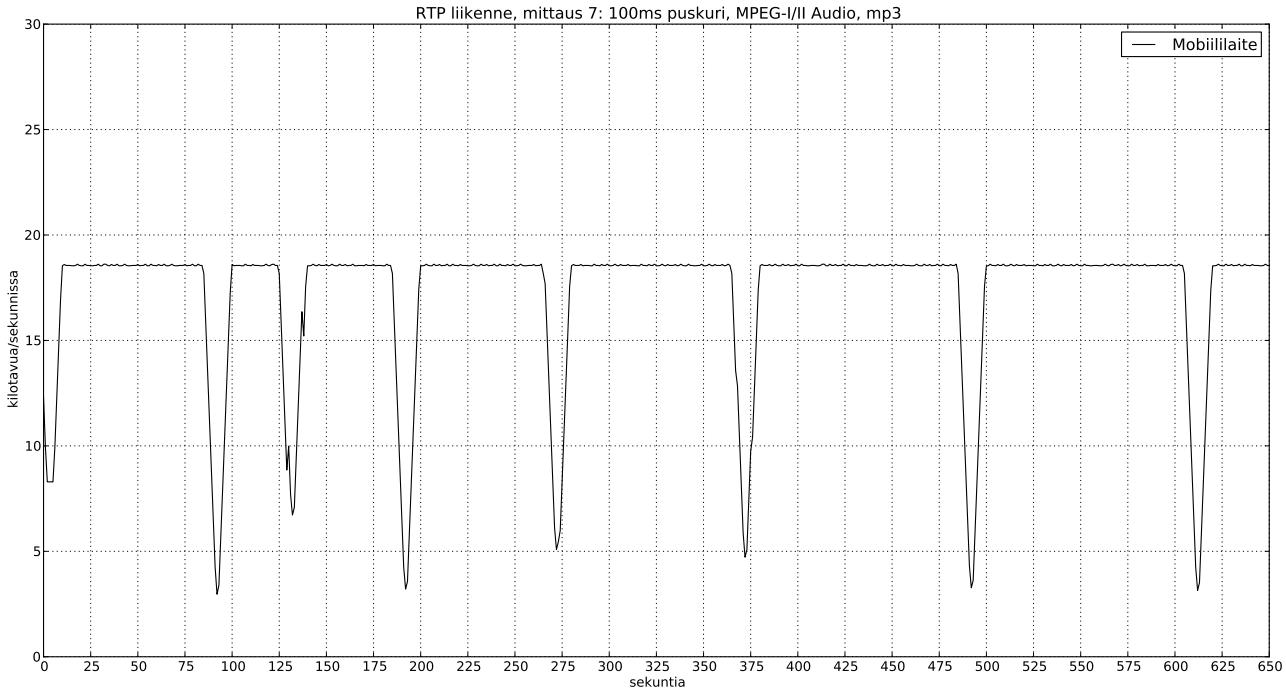
Kuvio 34: Mobiililaitteen RTP-liikenne, 4. mittaus



Kuvio 35: Mobiililaitteen RTP-liikenne, 5. mittaus



Kuvio 36: Mobiililaitteen RTP-liikenne, 6. mittaus



Kuvio 37: Mobiililaitteen RTP-liikenne, 7. mittaus

D IPsec suojauskytkennät

Asetuskuvassa 6.3 IPsec suojauskytkennät mobiililiitoksen ja mobiiliyhdyskäytävien välille.

```
flush;
spdflush;
## Mobiiliyhdyskäytävä 0
add 2001:100::2 2001:100::1 esp 1000
−u 10
−m transport
−E 3des−cbc "PMIP6−010−−1234567890123"
−A hmac−sha1 "PMIP6−010−−123456789" ;
add 2001:100::1 2001:100::2 esp 1001
−u 10
−m transport
−E 3des−cbc "PMIP6−010−−1234567890123"
−A hmac−sha1 "PMIP6−010−−123456789" ;
add 2001:100::2 2001:100::1 esp 1002
−u 11
−m tunnel
−E 3des−cbc "PMIP6−011−−1234567890123"
−A hmac−sha1 "PMIP6−011−−123456789" ;
add 2001:100::1 2001:100::2 esp 1003
−u 11
−m tunnel
−E 3des−cbc "PMIP6−011−−1234567890123"
−A hmac−sha1 "PMIP6−011−−123456789" ;
## Mobiiliyhdyskäytävä 1
add 2001:100::3 2001:100::1 esp 1004
−u 12
−m transport
−E 3des−cbc "PMIP6−012−−1234567890123"
−A hmac−sha1 "PMIP6−012−−123456789" ;
add 2001:100::1 2001:100::3 esp 1005
−u 12
−m transport
−E 3des−cbc "PMIP6−012−−1234567890123"
−A hmac−sha1 "PMIP6−012−−123456789" ;
add 2001:100::3 2001:100::1 esp 1006
−u 13
−m tunnel
−E 3des−cbc "PMIP6−013−−1234567890123"
−A hmac−sha1 "PMIP6−013−−123456789" ;
add 2001:100::1 2001:100::3 esp 1007
−u 13
−m tunnel
−E 3des−cbc "PMIP6−013−−1234567890123"
−A hmac−sha1 "PMIP6−013−−123456789" ;
```

Asetus 6.3: Mobiililiitoksen IPsec suojauskytkentä

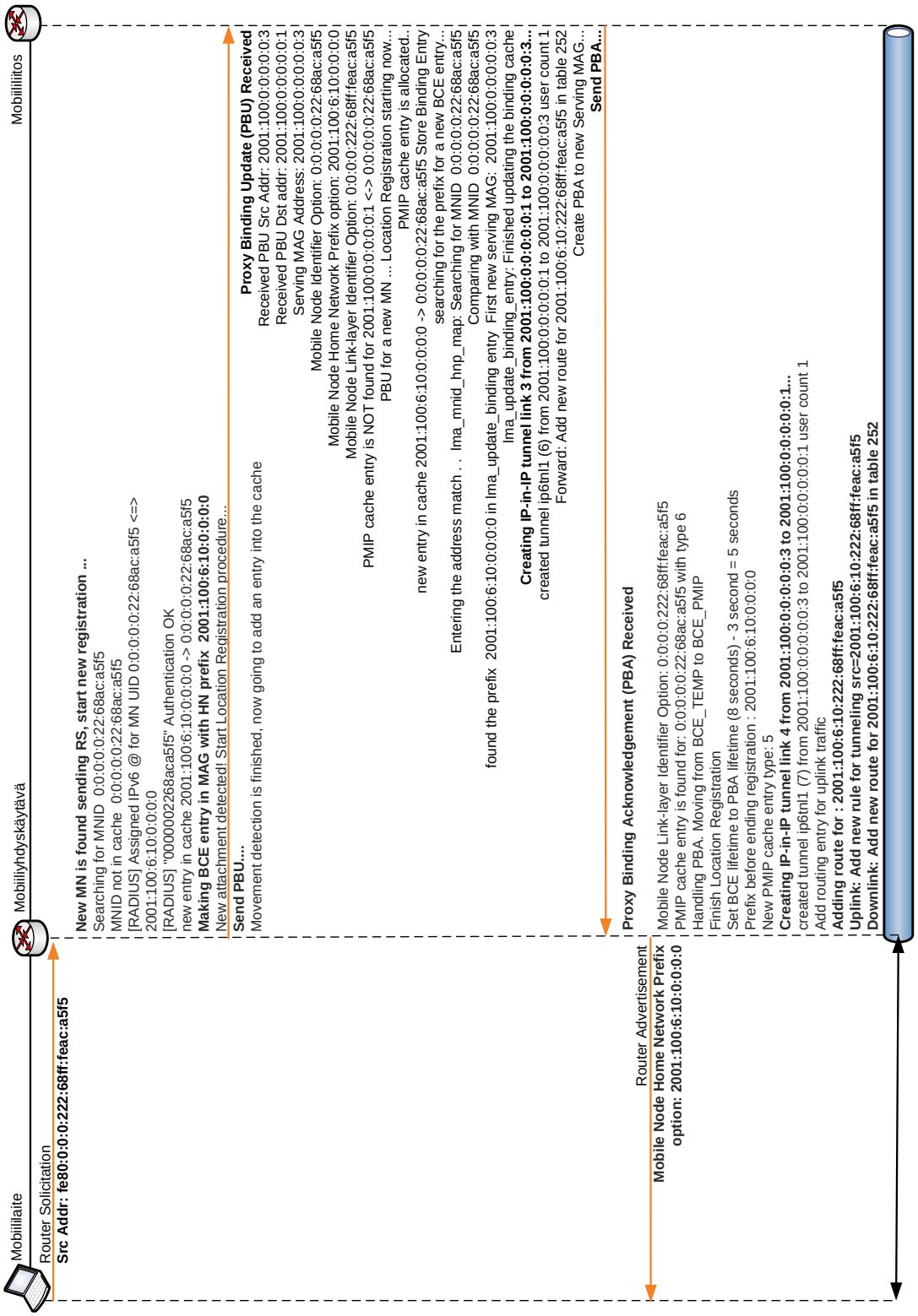
Asetuskuvassa 6.4 IPsec suojauskytkentä mobiiliyhdyskäytävä 0:n[1] ja mobiililiitoksen välille.

```
flush;
spdflush;
## Mobiililiitos
add 2001:100::2 2001:100::1 esp 1000
−u 10
−m transport
−E 3des−cbc "PMIP6−010−12345678901234"
−A hmac−sha1 "PMIP6−010−1234567890" ;
add 2001:100::1 2001:100::2 esp 1001
−u 10
−m transport
−E 3des−cbc "PMIP6−010−12345678901234"
−A hmac−sha1 "PMIP6−010−1234567890" ;
add 2001:100::2 2001:100::1 esp 1002
−u 11
−m tunnel
−E 3des−cbc "PMIP6−011−12345678901234"
−A hmac−sha1 "PMIP6−011−1234567890" ;
add 2001:100::1 2001:100::2 esp 1003
−u 11
−m tunnel
−E 3des−cbc "PMIP6−011−12345678901234"
−A hmac−sha1 "PMIP6−011−1234567890" ;
```

Asetus 6.4: Mobiiliyhdyskäytävä 0:n IPsec suojauskytkentä

[1]Muille mobiiliyhdyskäytäville samanlainen, vain IPv6-osoite muuttuu

E PMIPv6 yhteysviestit



Kuvio 38: PMIPv6-verkon viestiliikenne mobiililaitteen siihen yhdistettäessä