hyväksymispäivä arvosana

arvostelija

Mobile IPv6:n tietoturva ja reititystesti

Juhana Kammonen

Helsinki 19.5.2009

Kandidaatintutkielma

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta — Fakultet — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen	Tietojenkäsittelytieteen laitos

Tekijä — Författare — Author
Juhana Kammonen

Työn nimi — Arbetets titel — Title
Mobile IPv6:n tietoturva ja reititystesti

Oppiaine — Läroämne — Subject
Tietojenkäsittelytiede

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Kandidaatintutkielma	19.5.2009	17 sivua

Tiivistelmä — Referat — Abstract

Mobile IPv6 -protokolla (MIPv6) kuvailee ne yhteyskäytännöt, joilla kotiverkkonsa ulkopuolelle vaeltava langaton asiakassolmu kykenee säilyttämään yhteyden mahdollisesti kokonaan eri verkossa sijaitsevaan vastaanottavaan solmuun. Asiakassolmu kommunikoi vastaanottavan solmun kanssa aluksi kotiverkossaan sijaitsevan kotireitittimen välityksellä ja tarvittaessa lopulta ilman kotireitittimen apua. Kotireitittimen tärkein tehtävä on ylläpitää asiakassolmun kotiosoitteen ja tilapäisosoitteen välistä sidontaa.

Solmujen välisen yhteyden säilyttämisen lisäksi yhteys on suojattava mahdollisilta palvelunesto-, välimies-, monistus- ja muilta hyökkäyksiltä. Suojautumiskeinona asiakassolmun ja kotireitittimen välille muodostetaan IPsec-turvayhteys IPsec-protokollakokoelman avulla. IPsec-turvayhteyden kuljetusmoodi suojaa asiakassolmun ja vastaanottavan solmun väliset sidonnan päivitykset. IPsec-turvayhteys ei kuitenkaan sovellu kotireitittimen ja vastaanottavan solmun välisen tietoliikenneverkon osuuden eikä asiakassolmun ja vastaanottavan solmun välisen suoran linkin suojaamiseen. Suoran linkin muodostamisen suojaamista varten MIPv6:een on kehitetty protokollakohtainen turvaratkaisu, reititystesti. Reititystestin tavoitteena on asiakassolmun ja vastaanottavan solmun välisen tietoliikenneyhteyden todentaminen siten, että vastaanottava solmu voi tallentaa asiakassolmun osoitteiden sidonnan. Näin vältytään kotireitittimen kuormittamiselta, ja tiedonsiirto nopeutuu. IPsec-turvayhteyden tunnelimoodilla suojataan osa reititystestin keskeisistä viesteistä.

Tämä tutkielma käsittelee ensin MIPv6:ta yleisellä tasolla. Myöhemmät luvut esittelevät MIPv6:n keskeiset turvallisuusuhat, IPsec-protokollakokoelman ja reititystestin. Aiheet koskevat erityisesti asiakassolmua, kotireititintä ja asiakassolmun kanssa kommunikoivaa vastaanottavaa solmua. Myös tutkielman näkökulma rajoittuu näihin kolmeen solmuun. Pääpaino on MIPv6:n turvallisuusuhkien esittelyssä ja turvaratkaisuissa, joilla vastataan näihin uhkiin. IPsec-protokollakokoelmaan kuuluvan IKE-protokollan yksityiskohtainen käsittely kuten myös reititystestin mahdolliset muunnokset eri verkkoinfrastruktuureissa jäävät tämän tutkielman aihealueiden ulkopuolelle. Tärkeimpänä tuloksenaan tutkielma näyttää reititystestin onnistuneen kulun. Reititystestin avulla asiakassolmun ja vastaanottavan solmun välille muodostetaan riittävän voimakas IPsec:stä riippumaton turvayhteys, jolla siis MIPv6:lle keskeiset sidonnan päivitykset voidaan hyväksyä.

Tietoturvan näkökulmasta MIPv6 on käyttövalmis. IPsec:n avulla saadaan suojattua kriittisimmät vaiheet MIPv6-solmujen välisessä tietoliikenteessä. Reititystesti vastaa hyvin langattoman tiedonsiirron haasteisiin niin tietoturvan kuin yhteysnopeudenkin suhteen. Käytön lisääntymisen myötä MIPv6 tulee lähitulevaisuudessa kokemaan laajamittaista käytännon testausta ja ongelmien ratkaisua, mikä asettaa hyvät suuntaviivat MIPv6:n kehitykselle.

ACM Computing Classification System (CCS): C.2.0 [General], C.2.1 [Network Architecture and Design], C.2.2 [Network Protocols]

Avainsanat — Nyckelord — Keywords
Mobile IPv6, reititystesti, IPsec, langaton tietoliikenne, tietoturva

Säilytyspaikka — Förvaringsställe — Where deposited

Muita tietoja — övriga uppgifter — Additional information

Tieteellisen kirjoittamisen kurssi - kevät 2009

Sisältö

1 Johdanto

Maailmanlaajuisesti yleisin tietoliikenneyhteyksissä käytetty protokolla on edelleen *IPv4* (Internet Protocol version 4), joka teoriassa pystyy tarjoamaan osoitteita ainoastaan 4,2 miljardille verkkoon kytkettävälle laitteelle [KOO07, s. 7]. Suuri osa verkkoon kytkettävistä laitteista on kytkettynä suljettuihin verkkoihin, jolloin niiden verkko-osoitteiden ei välttämättä tarvitse olla yksilöllisiä. Laitteiden määrän kasvaessa on kuitenkin selvää, että IPv4:n osoiteavaruuskin kapenee koko ajan. IPv4:n verkko-osoitteiden on arveltu loppuvan kolmen vuoden kuluessa, siis vuoteen 2012 mennessä [HAM09]. *IPv6* (Internet Protocol version 6), jota pidetään IPv4:n seuraajana, tarjoaa moninkertaisesti suuremman osoiteavaruuden verkkoon kytkettäville laitteille. Kuitenkin vasta noin neljä prosenttia kaikesta tietoliikenteestä on IPv6:ta hyödyntävää [HAM09]. Monet palveluntarjoajat ja muut alan kaupalliset yritykset suhtautuvat myönteisesti käyttöönoton lisäämiseen ja ovat jo alkaneet tarjota IPv6:ta hyödyntäviä palveluitaan. Samalla IPv6:een liittyvä tutkimustyö on luonnollisesti lisääntynyt. Suurin osa IPv6:n kehitystyöstä on tehty *IETF*:ssä (Internet Engineering Task Force) kansainvälisin voimin.

Langattoman tietoliikenteen toteuttaminen on nykyään lähes välttämätöntä tietoliikenneverkoissa, joten myös IPv6:lle on laadittu kokoelma yhteyskäytäntöjä langattomaan tiedonsiirtoon. Tätä IPv6:n laajennusta kutsutaan nimellä Mobile IPv6 (MIPv6). MIPv6:n toiminnallisuuksien ytimessä on se, miten langattoman tietoliikenneverkon *asiakassolmu* (mobile node) kykenee säilyttämään yhteyden (ja yhteysnopeuden) toisessa verkossa sijaitsevaan *vastaanottavaan solmuun* (correspondent node) erityisesti silloin, kun asiakassolmu *vaeltaa* (roams) kotiverkon ulkopuolella. Kotiverkolla tarkoitetaan tässä tutkielmassa mitä tahansa sellaista tietoliikenneverkkoa, jossa on asiakassolmun kanssa kommunikoiva *kotireititin* (home agent). Kotireitittimellä on keskeinen rooli asiakassolmun ja vastaanottavan solmun välisessä viestienvaihdossa, sillä kotireititin on se taho, joka ylläpitää *sidontaa* (binding) asiakassolmun *kotiosoitteen* (home address) ja *tilapäisosoitteen* (care-of address) välillä. Vastaanottavana solmuna voi periaatteessa olla mikä tahansa IPv6-protokollaa käyttävä verkon päätepiste. Yhteyden säilyttäminen perustuu osoitteiden hallintaan ja kriittisten IP-pakettien todennukseen. IPv6-protokollan osoitteistuksen eräs erityispiirre on *tilaton osoitekonfiguraatio* (stateless autoconfiguration), jonka avulla verkkoon kytkettävälle laitteelle konfiguroidaan verkko-osoite ilman, että käyttäjän tarvitsee tehdä muuta kuin kytkeä laite verkkoon.

Tietoliikenneverkoissa liikkuvan tiedon luotettavuus ja turvallisuus ovat äärimmäi-

sen tärkeitä niin keskenään kommunikoiville solmuille kuin viestien välittämiseen osallistuville tahoillekin. Täysin suojaamaton kahden solmun välinen yhteys on helppo kohde erilaisille hyökkäyksille. MIPv6:ssa suurimmat turvallisuusuhat liittyvät asiakassolmun ja vastaanottavan solmun välisiin *sidonnan päivityksiin* (binding update), reititysotsakkeisiin sekä muuhun asiakassolmun ja kotireitittimen väliseen tietoliikenteeseen [KEM04, s. 3]. IPsec-protokollakokoelma tarjoaa keinoja yhteyden suojaamiseen. Näitä ovat esimerkiksi protokollat pakettivirtojen turvaamiseen ja avaintenvaihtoprotokollat pakettivirtojen muodostamiseen. Asiakassolmun ja kotireitittimen välillä vallitsevaa IPsec:llä suojattua yhteyttä kutsutaan *IPsec:n turvayhteydeksi* (IPsec Security Association). Turvayhteyden avulla edellä mainitut turvallisuuden kannalta keskeiset viestit voidaan todentaa. Todennus auttaa suojautumaan esimerkiksi *palvelunestohyökkäyksiltä* (denial-of-service attack) [OSH01, s. 2] ja joukolta muita hyökkäyksiä.

IPsec-protokollakokoelman kehitys on kuitenkin ollut hidasta MIPv6:een verrattuna. IPsec:n käyttö ja ylläpito tekevät solmujen välisestä tietoliikenteestä myös raskasta. Yksinkertaisenkin tiedon turvaaminen vaatii suhteessa massiivisia turvatoimenpiteitä. Lisäksi IPsec ei sovellu asiakassolmun ja vastaanottavan solmun välisen suoran tietoliikenteen suojaamiseen. Tätä varten MIPv6:een on kehitetty erityinen suojausmenetelmä, *reititystesti* (return routability). Reititystesti ei ole täysin vedenpitävä turvaratkaisu, mutta tarjoaa MIPv6-solmuille riittävän tietoturvan tason.

Aiheiden käsittelyjärjestys tässä tutkielmassa on seuraava: Luku 2 esittelee MIPv6:n ja protokollan toimintaperiaatteet. Luku 3 käsittelee MIPv6:n keskeisimpiä turvallisuusuhkia ja IPsec:iä. Luku 4 käsittelee reititystestiä melko yksityiskohtaisesti. Luku 5 hahmottelee MIPv6:n ja langattoman tietoliikenteen tulevaisuutta edeltävissä kappaleissa todetun valossa, ja luku 6 kertaa tutkielmassa käsitellyt asiat ja kokoaa ne johtopäätöksiksi.

2 Mobile IPv6

MIPv6 kuvailee yhteyskäytännöt langattomaan tiedonsiirtoon verkossa, jossa on käytössä IPv6-protokolla. MIPv6:n etuna on myös 128-bittisten IPv6-osoitteiden käyttö, mikä siis tekee potentiaalisesta osoiteavaruudesta paljon IPv4:ää suuremman. MIPv6:n kehitystyö ja standardointi on tehty pääasiassa protokollaan erikoistuneessa työryhmässä IETF:ssä. Työryhmä ehdottaa, että MIPv6 olisi luonnollinen seuraaja IPv4:n nykyisille langatonta tiedonsiirtoa tukeville protokollille. Toisaalta

MIPv6:n kehittämistä voi edistää jokainen palveluntarjoaja ottamalla protokolla ennakkoluulottomasti käyttöön. Luku 2.1 käsittelee MIPv6:n haasteita ja ratkaisuja. Luku 2.2 käsittelee lyhyesti MIPv6:n historiaa ja kehitystä.

2.1 MIPv6:n haasteet ja ratkaisut

Langattoman tiedonsiirron ja siten myös MIPv6:n tärkein haaste on, miten vaeltava *asiakassolmu* (mobile node) kykenee säilyttämään yhteyden toisessa verkossa sijaitsevaan *vastaanottavaan solmuun* (correspondent node). Tärkeässä asemassa yhteyden säilyttämisessä on kotiverkossa toimiva ja asiakassolmun kanssa kommunikoiva *kotireititin* (home agent). Kotireititin on se taho, joka ylläpitää asiakssolmun *kotiosoitteen* (home address) ja *tilapäisosoitteen* (care-of address) välistä sidontaa ja todentaa näin, että tilapäisosoitteesta kommunikoiva solmu todella on kotiverkosta vaeltanut asiakassolmu. Lisäksi ongelmana on, että vaikka yhteys kyettäisiinkin säilyttämään, solmujen väliseen tiedonsiirtoon tulee (usein sietämättömän pitkä) katkos silloin, kun asiakassolmu vaeltaa. Tämä ongelma korostuu esimerkiksi silloin, kun ääntä siirretään tietoliikenneverkossa (Voice over IP). Pohjimmiltaan MIPv6:ssa on kyse siitä, miten reititystaulujen hallinta hoidetaan kotireitittimellä silloin, kun asiakassolmu vaeltaa, ja mitä toimenpiteitä vaeltavan asiakassolmun ja vastaanottavan solmun on lisäksi suoritettava. Lisäksi MIPv6:n perusoletuksiin kuuluu, että protokollan käyttöympäristössä alempien protokollapinon kerrosten reititysinfrastruktuuri on yleisellä tasolla luotettava [NIK03, s. 1].

MIPv6:n merkittävin ero IPv4:n langatonta tietoliikennettä tukeviin protokolliin on ns. *vierasreitittimen* (foreign agent) käytön puuttuminen asiakassolmun vaeltaessa. Vaeltaminen aiheuttaa sen, etteivät asiakassolmun kotiosoitteeseen suunnatut viestit enää tavoita asiakassolmua. Tämä johtuu siitä, että vaeltaessaan uuteen verkkoon asiakassolmu joutuu ottamaan käyttöön tilapäisosoitteen, jonka alkuosana on asiakassolmun uuden verkon *aliverkkopeite* (subnet mask). Tämä alkuosa ei ole sama kuin asiakassolmun kotiosoitteen alkuosa, joten alkuosan perusteella määrittettävä asiakassolmun sijainti menetetään, kun asiakassolmu vaeltaa. Tilapäisosoite muodostetaan johdantokappaleessa mainitun tilattoman osoitekonfiguraation avulla. Tilapäisosoitteen on oltava yksilöllinen ja hierarkkisesti oikea. Osoitteen alkuosan ja siten myös uuden verkon hierarkian asiakassolmu saa kuuntelemalla uudessa verkossa kulkevia *reititinilmoituksia* (router advertisement), joita MIPv6:ta käyttävät reitittimet lähettävät 30 millisekunnin välein [KOO07, s. 73]. Osoitteen loppuosan asiakassolmu johtaa (yleensä) omasta MAC-osoitteestaan. Tällä tavoin asiakassol-

mu luo itse tilapäisosoitteensa ilman, että solmuun liittyvää sovellusta käyttävän tai verkon ylläpitäjän tarvitsee tehdä mitään erityistä. Saatu osoite on useimmissa tapauksissa myös yksilöllinen [OSH01, s. 2], mutta yksilöllisyyden varmistamiseksi asiakassolmu *havaitsee kaksoisosoitteet* (duplicate address detection).

Kaksoisosoitteiden havaitsemisessa asiakassolmu liittyy ensin *alustavalla* (tentative) tilapäisosoitteellaan tarvittaviin IPv6:n *osoiteryhmiin* (multicast address). Liittyminen mahdollistaa sen, että asiakassolmu voi vastaanottaa *naapuri-ilmoituksia* (Neighbor Advertisement) muilta osoiteryhmien solmuilta ja havaita osoiteryhmistä mahdollisesti solmun, jolla on yksikäsitteiseksi havaittu osoite, joka on sama kuin asiakassolmulla. Asiakassolmu lähettää osoiteryhmiin *kaksoisosoitteiden havaitsemiskyselyn* (duplicate address detection probe), joka sisältää asiakassolmun alustavan osoitteen. Mikäli asiakassolmu vastaanottaa kyselyn vastaukseksi naapuri-ilmoituksen, on asiakassolmun tavoittelema osoite jo käytössä. Jos taas jollakin osoiteryhmän solmulla on sama alustava osoite kuin asiakassolmulla, tuo solmu tietää kyselyn vastaanottaessaan, ettei sen alustava osoite ole yksikäsitteinen. Lisähuomiona todettakoon, etteivät MIPv6-solmut mitenkään erityisesti ”omista” IPv6-osoitteita, vaan osoitekonfiguraation toiminta riippuu edellä kuvattujen havaitsemisviestien saapumisjärjestyksestä. Jos kaksoisosoite havaitaan, alustava osoite hylätään, ja tilaton osoitekonfiguraatio suoritetaan uudelleen eri osoitteella. Kaksoisosoitteiden havaitseminen on välttämätön toimenpide MIPv6-protokollassa. Toisaalta juuri kaksoisosoitteiden havaitsemisen on todettu vievän ylivoimaisesti suurimman osan yhteyskelpoisuuden muodostamiseen kuluvasta ajasta, kun asiakassolmu kiinnittyy uuteen verkkoon [LAI05, s. 2].

Seuraava asiakassolmun toimenpide on *sidonnan päivityksen* (binding update) lähettäminen asiakassolmun kotireitittimelle. Sidonnan päivityksessä asiakassolmu ikään kuin sanoo: ”Olen vaeltanut uuteen verkkoon. Kommunikoidessanne kanssani käyttäkää tilapäisesti tätä ilmoittamaani osoitetta.” Sidonnan päivitys lähetetään myös kaikille vastaanottaville solmuille, jotka kommunikoivat asiakassolmun kanssa kotireitittimen välityksellä. Kotireitittimellä on oma *välimuisti* (binding cache) sidontaan liittyvien osoitteiden ylläpitoa varten. Vastaanottavalla solmulla välimuistia ei useinkaan ole. Vastaukseksi sidonnan päivitykseen kotireititin lähettää asiakassolmulle kuittauksen, jonka vastaanotettuaan asiakassolmu on viestiyhteysvalmiina uudessa verkossaan. Näihin kriittisiin viesteihin liittyy useita turvallisuusuhkia, joista tärkeimpiä luvut 3.1 - 3.3 esittelevät. Luku 3.4 taas käsittelee sitä, miten näihin turvallisuusuhkiin vastataan MIPv6:ssa.

Kaiken tietoliikenteen asiakassolmun ja vastaanottavan solmun välillä ei välttämättä tarvitse kulkea kotireitittimen kautta. MIPv6 tarjoaa asiakassolmulle erityisen *kotiosoiteoption* (home address option), joka sisällytetään *reititystestillä* (return routability) suojattuihin sidonnan päivityksiin asiakassolmulta vastaanottavalle solmulle. Pakettien ei tällöin tarvitse kulkea kotireitittimen kautta muuten kuin linkin muodostamisen yhteydessä. Etu saavutetaan sillä, että asiakassolmun ja vastaanottavan solmun välisen *suoran linkin* (optimized route) käyttö ei nyt kuormita kotireititintä, ja tiedonsiirto nopeutuu. MIPv6:n toiseksi keskeiseksi haasteeksi nousee liikenteen suojaaminen juuri tätä suoraa linkkiä muodostettaessa. Lisäksi suoran linkin käyttö vaatii sitä, että myös vastaanottavalla solmulla on välimuisti voimassa oleville sidonnoille. Reititystesti on eräs keino suojata suoran linkin muodostus. Luku 4 käsittelee reititystestiä yksityiskohtaisemmin.

2.2 MIPv6:n historia, kehitys ja kehittäjät

MIPv6-protokollan kehitys lähti liikkeelle tarpeesta luoda selkeät yhteyskäytännöt langattomalle tietoliikenteelle IPv6:ssa. MIPv6:n on standardoinut IETF:n langattomiin Internet-protokolliin erikoistunut työryhmä. Tutkijat kuten Jari Arkko, Tuomas Aura, Pekka Nikander, Greg O'Shea ja Michael Roe ovat protokollan kenties näkyvimmät yksittäiset kehittäjät. Kehitystyö on ollut ripeää, vaikka IPv6:n käyttöönotto asiakas- ja kaupallisissa yhteyksissä onkin ollut arveltua hitaampaa [HAM09]. Protokollan ratkaisujen turvallisuuteen on kiinnitetty huomiota alusta alkaen, mutta silti varsinaisen MIPv6:n kehityksessä on pidetty kovempaa vauhtia kuin luvussa 3.4 esiteltävän IPsec-protokollakokoelman kehityksessä [KOO07, s. 61-68]. Esimerkiksi kaikki tässä tutkielmassa lähteinä käytetyt MIPv6:n tietoturvaa koskevat artikkelit on kirjoitettu vasta tämän vuosituhannen puolella.

Kuten niin usein tietojenkäsittelytieteessä, myös MIPv6:ta on kehitetty yrityksen ja erehdyksen kautta. Esimerkiksi useat protokollan tietoturvalle herkät ratkaisut, kuten CAM-protokolla [OSH01] tai [AUR02, 3.4.]:ssa esitellyt ideat, ovat testeissä paljastuneet liian heikoiksi. Koska tietoturva on noussut täysin erottamattomaksi osaksi nykyaikaista tietoliikennettä, myös nykyiset MIPv6:n tietoturvalle herkät ratkaisut ovat tiukan tarkastelun kohteina. Protokollan kehitys jatkuu yhä.

3 MIPv6:n turvallisuus ja IPsec

MIPv6:n merkittävimmät turvallisuusuhat jakautuvat kolmeen ryhmään. Näitä ovat ensinnäkin sidonnan päivityksiä koskevaan viestienvaihtoon liittyvät uhat, toiseksi kotiosoiteoptioon ja reititysotsakkeisiin liittyvät uhat ja kolmanneksi muuhun asiakassolmun ja kotireitittimen väliseen viestienvaihtoon liittyvät uhat. Tämä luku käsittelee jokaista näistä kolmesta ryhmästä omana alilukunaan. IPsec:iin kuuluvat protokollat suojaavat verrattain hyvin tietoliikenteen asiakassolmun ja kotireitittimen välillä ja vastaavat siten kaikkiin kriittisiin tässä luvussa esiteltäviin uhkiin. Protokollat eivät kuitenkaan sovellu asiakassolmun ja vastaanottavan solmun välisen suoran linkin suojaamiseen. IPsec ei myöskään suojaa kotireitittimen ja vastaanottavan solmun välistä verkon osaa. Luku 3.4. käsittelee tarkemmin IPsec-protokollakokoelmaa.

3.1 Sidonnan päivityksiin liittyvät uhat

Sidonnan päivityksiin liittyvistä uhista kenties tavallisin on luvaton liikenteen uudelleenohjaus. Hyökkääjän on helppo luoda ja lähettää valheellisia sidonnan päivityksiä kotireitittimelle. Jos kotireititin ei käyttäisi mitään todennusmekanismia sidonnan päivityksille, se joutuisi usein hyväksymään myös valheellisia viestejä. Kun kotireititin vastaanottaa sidonnan päivityksen, kotireitittimen välimuistia muutetaan vastaamaan päivityksessä ilmoitettua sidontaa asiakassolmun kotiosoitteen ja tilapäisosoitteen välillä. Koska sidonnan päivityksen lähettäjä ei aina välttämättä ole hyväntahtoinen, on kotireitittimen kyettävä varmistamaan, että lähettävällä solmulla on oikeus tehdä kyseinen päivitys [AUR02, s. 1]. Onnistuessaan hyökkääjä saattaa kyetä muuttamaan vallitsevia sidontoja vaikkapa siten, että suuri osa verkon tietoliikenteestä ohjautuu yhdelle ainoalle asiakassolmulle. Tämä ”uhrisolmu” ei välttämättä kykene käsittelemään kaikkea saapuvaa liikennettä ja on tällöin joutunut palvelunestohyökkäyksen kohteeksi. Mikäli hyökkääjä taas onnistuisi esimerkiksi anastamaan asiakassolmun tilapäisosoitteen, tulisi hyökkääjästä *välimies* (man-in-the-middle). Hyökkääjä voisi tuolloin käyttää yhteyttä mielivaltaisesti. Tällaisia hyökkäyksiä varten hyökkääjä tarvitsee kuitenkin sekä lähettävän solmun että vastaanottavan solmun osoitteet ja lisäksi siis tiedon siitä, miten kotireititin saadaan vakuuttuneeksi siitä, että viesti tulee luotettavalta asiakassolmulta, jolla on oikeus tehdä kyseinen päivitys.

Langattomassa tietoliikenneverkossa asiakassolmujen osoitteet vaihtuvat niin usein,

että yhteen asiakassolmuun kohdistuvan pitkäkestoisen ja onnistuvan hyökkäyksen todennäköisyys jää pieneksi. Kotireititin ja muut mahdolliset isäntäkoneet, joiden osoitteet pysyvät pitkään muuttumattomina, ovat kuitenkin varteenotettavia kohteita tällaisille hyökkäyksille. Lisäksi tällaisissa ”staattisissa” isäntäkoneissa on usein käytössä vanhentunut kokoelma sovellustason ohjelmistoja, jolloin hyökkäyksiin reagointi saattaa olla hidasta tai sitä ei ole lainkaan [KEM04, s. 5]. Sidonnan päivitykset on myös numeroitu MIPv6:ssa. Numeroinnissa käytetään liukuvan ikkunan protokollaa ja sen avulla minimoidaan *monistushyökkäysten* (replay attack) vaikutukset.

Kotireititttimellä ja useissa tapauksissa myös vastaanottavalla solmulla on mahdollisuus tehdä erityinen pyyntö sidonnan päivityksestä asiakassolmulle. Hyökkääjä voi näin ollen myös tehdä *voimahyökkäyksen* (brute force attack) pyytämällä uhrisolmulta sidonnan päivityksen hyvin suureen määrään osoitteita. Asiakassolmun toiminta hidastuisi merkittävästi, koska se joutuisi käsittelemään kaikki nämä päivityspyynnöt ja mahdollisesti odottamaan kuittauksia kaikkiin lähettämiinsä päivityksiin. Asiakassolmulla on keinot esimerkiksi asettaa maksimiarvo käsiteltäville sidonnan päivityksille tai vastaanottaville solmuille, joille asiakassolmu lähettää sidonnan päivityksiä. Lisäksi asiakassolmu voi suojautua yksinkertaisesti jättämällä *suoran linkin muodostamisen* (route optimization) vastaanottavaan solmuun tekemättä. Koska tällöin asiakassolmun pakettien välittäminen vastaanottavalle solmulle jäisi kotireititttimen huoleksi, tiedonsiirto hidastuisi. Vaikutukset näkyisivät suoraan esimerkiksi siirrettäessä kuvaa tai ääntä asiakassolmun ja vastaanottavan solmun välillä.

3.2 Kotiosoiteoptioon ja reititysotsakkeisiin liittyvät uhat

Mobile IPv6:n kotiosoiteoptio on asiakassolmun keino ilmoittaa vastaanottavalle solmulle oma kotiosoitteensa, vaikka asiakassolmun senhetkisenä lähdeosoitteena onkin asiakassolmun tilapäisosoite. Kotiosoiteoption avulla vastaanottava solmu voi muodostaa suoran linkin asiakassolmuun tallentamalla sidonnan asiakassolmun kotiosoitteen ja tilapäisosoitteen välillä. Luku 4 käsittelee tätä yksityiskohtaisemmin. MIPv6:ssa kotiosoiteoptiot ovat käytössä kaikissa niissä viesteissä, jotka asiakassolmu lähettää vastaanottavalle solmulle tätä *suoraa linkkiä* (optimized route) käyttäen. Kotiosoiteoption ongelmana ja vaarana on se, että hyökkääjälle tarjoutuu mahdollisuus saada asiat näyttämään siltä, että hyökkäys tulee hyökkäyksen kohteeksi joutuneen verkon sisältä, kun hyökkääjä oikeasti sijaitsee verkon ulkopuolella. Esimerkkinä tästä on [KEM04, s. 7]:ssa kuvattu tapaus.

Reititysotsakkeet ovat yleinen turvallisuusongelma langattomassa (ja muussakin) tietoliikenteessä. IP-paketeissa päällimmäisinä olevat reititysotsakkeet sisältävät tiedon siitä, mikä paketin seuraava kohdesolmu on. Kun *reititin* (router) vastaanottaa IP-paketin, se poistaa päällimmäisen reititysotsakkeen ja kirjoittaa otsakkeessa olevan osoitteen paketin uudeksi kohdeosoitteeksi. Tämä ”reititysotsakepino” saattaa reitityksestä riippuen olla hyvinkin suuri. Tavalliset reititysotsakkeet saattavat sisältää myös useampia kohdesolmujen osoitteita. Turvallisuusongelma muodostuu siitä, että hyökkääjä kykenee hankaloittamaan oman lähdeosoitteensa jäljitystä reitittämällä lähettämänsä paketit sopivien välikäsien kautta. Näin ollen hyökkäyksiin reagoitaessa epäilykset kohdistuisivat aluksi noihin välikäsiin, kun taas hyökkääjä saisi lisäaikaa suorittaa tarvittavia toimenpiteitä jälkiensä peittämiseksi. *Tyypin 2 reititysotsakkeet* (type 2 routing header) ovat oleellisesti samanlaisia kuin yllä kuvatut reititysotsakkeet, mutta niihin voidaan sisällyttää ainoastaan yksi vastaanottajan osoite. MIPv6:ssa ne ovat käytössä vastaanottavalta solmulta asiakassolmulle lähetettävissä sidonnan kuittausviesteissä ja kaikissa viesteissä suoraa linkkiä käyttäen.

3.3 Muuhun asiakassolmun ja kotireitittimen väliseen viestienvaihtoon liittyvät uhat

Asiakassolmu ja kotireititin vaihtavat usein tärkeitä viestejä pian sen jälkeen, kun asiakassolmu on vaeltanut kotiverkon ulkopuolelle. Jos asiakassolmun yhteys kotireitittimeen syystä tai toisesta katkeaa (vaeltamisen vuoksi tai muusta syystä), asiakassolmu lähettää kotiverkkoon *kotireitittimen löytämispyynnön* (Home Agent Discovery Request). Pyyntö kohdistetaan *edullisimpaan* (anycast) kotiverkon osoitteeseen, ja osoitteesta mahdollisesti löytyvä kotireititin vastaa kuittausviestillä, johon sisältyy kotireitittimen osoite. Asiakassolmulla ei ole keinoja todentaa näitä kuittausviestejä, koska IPsec-turvayhteyttä ei voida muodostaa asiakassolmun ja edullisimman osoitteen välille [KEM04, s. 8]. Tämä on suoraan MIPv6:een liittyvä uhka, koska esimerkiksi IPv4:n langatonta tietoliikennettä tukevissa protokollissa kotireitittimen löytämispyynnöt eivät ole käytössä. MIPv6:n tietoturvaratkaisujen on siis myös vastattava tähän uhkaan.

Jos taas esimerkiksi asiakassolmun kotiverkossa tapahtuisi *osoitteiden uudelleennumerointi* (address renumbering), olisi kotireitittimen luonnollisesti ilmoitettava asiakassolmulle tästä. Asiakassolmu saa tällöin tietoonsa vastaanottavan solmun uuden aliverkon osoitteen alkuosan. Mikäli hyökkääjä onnistuisi puuttumaan tähän viestienvaihtoon esimerkiksi siten, että saisi asiakassolmun uskomaan vastaanottavan

solmun uudeksi aliverkon osoitteen alkuosaksi hyökkääjän aliverkon osoitteen alkuosan, kaikki asiakassolmulta lähtevät viestit ohjautuisivat joko suoraan hyökkääjälle tai muuhun haluttuun osoitteeseen hyökkääjän aliverkossa. Hyökkääjä saattaa myös kuuntelun avulla saada asiakassolmun kotiverkon rakenteesta tietoja, joita käytetään hyväksi mahdollisessa tulevassa hyökkäyksessä. On kriittisen tärkeää estää tällaiset hyökkäykset, ja IPsec-protokollakokoelma myös vastaa tähän tarpeeseen.

3.4 IPsec-protokollakokoelma

IPsec-protokollaokokoelma vastaa MIPv6:n asettamiin vaatimuksiin solmujen välisen tietoliikenteen turvaamiseksi. IETF:ssä on myös IPsec:iin erikoistunut työryhmä. Tämän tutkielman kannalta huomio kiinnittyy erityisesti asiakassolmun ja kotireitittimen väliseen liikenteeseen ja sidonnan päivitysten suojaamiseen. IPsec soveltuu tähän hyvin, koska asiakassolmun ja kotireitittimen välisen *hallinnollisen suhteen* (administrative relationship) voidaan olettaa kestävän sen verran pitkään, että raskaankin turvayhteyden muodostaminen kannattaa. Turvayhteyden muodostaminen perustuu solmujen väliseen *avaintenvaihtoon* (key exchange). Lisäksi sekä asiakassolmu että kotireititin käyttävät erityisiä tietokantoja turvayhteyden parametrien säilyttämiseen. Tämä tutkielma ei käsittele näitä tietokantoja tämän tarkemmin, mutta tietokantojen avulla varmistetaan, että jo olemassa olevan IPsec-turvayhteyden tietyt osat eivät muutu vaikka asiakassolmu vaeltaisi.

MIPv6:n spesifikaatio määrää, että sidonnan päivityksissä asiakassolmun ja kotireitittimen välillä tulee vallita *kuljetusmoodin* (transport-mode) IPsec-turvayhteys, joka suojaa paketit tällä yhteydellä *ESP*:tä (Encapsulating Security Payload) käyttämällä. Tällaisen turvayhteyden tulee vallita myös silloin, kun asiakassolmu lähettää kotireitittimen löytämispyynnön kotiverkkoon tai kotiverkossa tapahtuu osoitteiden uudelleennumerointi. Tätä määräystä voidaan pitää ratkaisuna luvussa 3.3 esiteltyihin uhkiin. ESP on ikään kuin ylimääräinen pakettiin liitettävä otsaketieto, joka piilottaa paketin varsinaisen otsakkeen ”syvemmälle” paketin sisään ja ilmoittaa paketin vastaanottajalle tarvittavat parametrit suojatun tiedon käsittelemiseksi. Näistä syistä ESP-otsake sijaitsee tällaisissa paketeissa juuri ennen suojattavaa tietoa. Osa reititystestin (luku 4) viesteistä on määrätty suojattavaksi *tunnelimoodin* (tunnel-mode) IPsec-turvayhteydellä. Tunnelimoodin avulla ESP suojaa kokonaisen IP-paketin, ei ainoastaan tiettyä paketin sisällä olevaa tietoa. Tällä turvayhteydellä voidaan tarvittaessa suojata myös asiakassolmun ja kotireitittimen välinen osa polusta silloin kun asiakassolmu ja vastaanottava solmu kommunikoivat keskenään

kotireitittimen avulla. Kuljetusmoodin IPsec-turvayhteys on tarkoitettu ensisijaisesti kahden solmun - tässä tutkielmassa asiakassolmun ja kotireitittimen - välisen yhteyden suojaamiseen, kun taas tunnelimoodin IPsec-turvayhteys on tarkoitettu suojaamaan tunneloitavan viestin välitys kolmannelle taholle. Tässä tutkielmassa tämä kolmas taho on toisaalta vastaanottava solmu, joka vastaanottaa asiakassolmulta lähteviä viestejä kotireitittimen välityksellä, toisaalta asiakassolmu, jolle vastaanottavan solmun lähettämät viestit tunneloidaan kotireitittimeltä.

IPsec-turvayhteyden muodostamisen ensimmäinen vaihe on asiakassolmun ja vastaanottavan solmun välinen tunnisteiden vaihto. Yleensä tämä suoritetaan IPsec-protokollakokoelmaan kuuluvan *IKE*-protokollan (Internet Key Exchange) avulla, mutta vaihto voidaan suorittaa manuaalisestikin. Kuljetusmoodin IPsec-turvayhteys muodostuu asiakassolmun ja kotireitittimen välille, kun asiakassolmu ja kotireititin vaihtavat osoitteita käyttäen näiden ”vaihtoviestien” autentikointiin ensimmäisessä vaiheessa vaihdettuja tunnisteita. Asiakassolmu ilmoittaa (muuttumattoman) kotiosoitteensa kotireitittimelle, ja kotireititin vastaa omalla osoitteellaan. Nämä osoitteet sidotaan ensimmäisessä vaiheessa vaihdettuihin tunnisteisiin. Kun turvayhteys astuu voimaan, voidaan asiakassolmun ja kotireitittimen välillä suorittaa IPsec:iin kuuluvien muiden protokollien avulla suojattua viestienvaihtoa, ensimmäiseksi erityisesti sidonnan päivitys asiakassolmulta kotireitittimelle ja sidonnan kuittaus kotireitittimeltä asiakassolmulle. Kuljetusmoodin IPsec-turvayhteys voidaan aina muodostaa uudelleen ensimmäisessä vaiheessa vaihdettujen tunnisteiden avulla. Tämä tutkielma ei käsittele IKE-protokollaa edellä kuvattua yksityiskohtaisemmin.

Tunnelimoodin IPsec-turvayhteys muodostetaan oleellisesti samoin kuin kuljetusmoodinkin, mutta ongelmana on se, että kotiosoitteen sijaan asiakassolmu ilmoittaa toisessa vaiheessa kotireitittimelle tilapäisosoitteensa. Vaikka ensimmäisen vaiheen tunnisteiden vaihto hoidettaisiin tässä manuaalisesti, tarvittaisiin kuitenkin automaattinen metodi tilapäisosoitteiden päivittämiseksi. Toisaalta, jos avaintenvaihto hoidettaisiin täysin dynaamisesti (IKE-protokollalla), jouduttaisiin suorittamaan turvayhteyden muodostamisen ensimmäinen vaihe aina uudelleen silloin kun asiakassolmu vaeltaa. On lisäksi huomattavaa, että ESP-otsake ei suojaa tilapäisosoitteita, koska tilapäisosoitteet esiintyvät ainoastaan pakettien uloimmissa otsakkeissa.

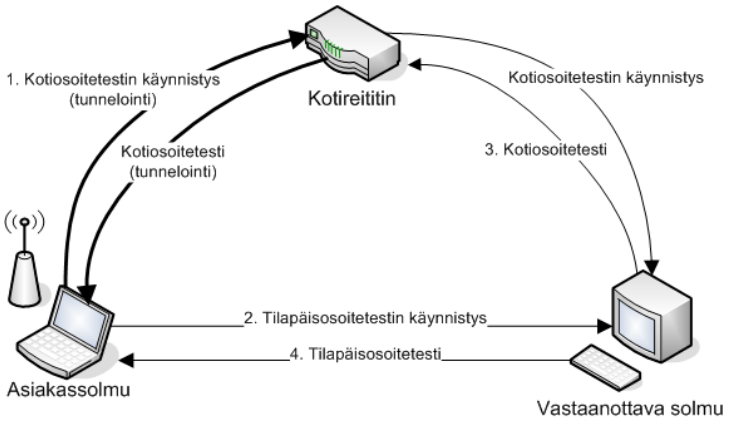
IPsec:n käyttöönotto MIPv6:ssa (ja IPv6:ssa yleensäkin) ei ole ollut aivan mutkatonta. Esimerkiksi turvayhteyttä muodostettaessa hyödynnettävää IKE-protokollaa ei alunperin suunniteltu toimimaan langattomissa verkoissa [KEM04, s. 21]. Lisäksi IPsec:iä alettiin istuttaa MIPv6:een melko myöhäisessä vaiheessa, koska MIPv6:n

standardoineessa IETF:n työryhmässä ei ilmeisesti aluksi kiinnitetty riittävästi huomiota tietoturvaan [KOO07, s. 61-68]. IPsec:n kehitys onkin malliesimerkki siitä, mitä haasteita kansainvälisiin ponnisteluihin yhteisen hyvän aikaansaamiseksi voi liittyä. Sen lisäksi, että työryhmä kehittää omaa tuotettaan, olisi kehityksen pysyttävä myös muiden työryhmien vauhdissa.

4 Reititystesti

Asiakassolmun ja vastaanottavan solmun välisen tietoliikenteen suojaaminen osoittautuu kriittiseksi. IPsec:n käyttö näiden kahden välillä ei suju luontevasti, koska vastaanottava solmu on mielivaltainen IPv6-protokollaa käyttävä solmu. Asiakassolmu ei esimerkiksi yhteyttä muodostaessaan voi tietää, onko vastaanottava solmu langaton vai ei. Lisäksi asiakassolmun ja vastaanottavan solmun välisen yhteyden kesto on yleensä liian lyhyt raskaan IPsec-yhteyden muodostamiseen, koska asiakassolmu vaeltaa usein. Asiakassolmun ja vastaanottavan solmun välisen suoran linkin suojaamiseen käytetään reititystestiä. Reititystesti nojautuu kaikissa tietokoneverkoissa MIPv6:n oletukseen siitä, että verkon reitittimet saavat ”suurella todennäköisyydellä” paketit toimitettua kunnollisina perille [KEM04, s. 20]. Millään linkkikerrosta ylempien protokollapinon kerrosten ratkaisulla ei voida vaikuttaa tähän oletukseen. Reititystestin tavoitteena on asiakassolmun ja vastaanottavan solmun välisen tietoliikenneyhteyden todentaminen siten, että MIPv6:ssa keskeiset sidonnan päivitykset (ja kuittaukset) voidaan hyväksyä tällä yhteydellä. Todentaminen perustuu kryptografisesti suojattuun avaintenvaihtoon, ja siinä hyödynnetään asiakassolmun ja kotireitittimen välisen IPsec-turvayhteyden tunnelimoodia. Aina kun mahdollista, muodostetaan myös *suora linkki* (optimized route) asiakassolmun ja vastaanottavan solmun välille. Suoran linkin käytöllä vältytään asiakassolmun ja kotireitittimen välisen raskaan tunnelin käytöltä, jolloin tiedonsiirto nopeutuu. Reititystesti asettaa siis edellytykset tämän suoran linkin muodostamiseksi turvallisesti. Tämä tutkielma käsittelee reititystestiä MIPv6:n kannalta periaatteellisella tasolla, ja aiheen käsittely keskittyy reititystestin tärkeimpiin viesteihin ja reititystestin käytöstä saataviin etuihin. Huomionarvoista on myös, että tietoliikenneverkosta ja laitteistosta riippuen pienet muunnokset seuraavaksi esiteltävään reititystestin kulkuun yleisellä tasolla ovat mahdollisia, monissa tapauksissa myös tarpeellisia. Joitakin näistä muunnoksista on käsitelty esimerkiksi [KOO07]:n loppupuolella.

4.1 Reititystestin kulku



Kuva 1: Reititystesti

Kuva 1 havainnollistaa reititystestin keskeiset viestienvaihdot. Tämä luku esittelee näistä viesteistä rakenteellisella tasolla ainoastaan *kotiosoitetestin käynnistysviestin* (Home Test Init) ja *kotiosoitetestin* (Home Test), koska näillä kahdella viestillä on erityismerkitys IPsec-turvayhteyden tunnelimoodin kannalta.

Reititystestin aluksi suoritetaan aina asiakassolmun ja kotireitittimen välinen sidonnan päivitys. Tämän jälkeen asiakassolmu lähettää samanaikaisesti kaksi viestiä vastaanottavalle solmulle. Ensimmäinen viesti on kotiosoitetestin käynnistysviesti. Tämä viesti ”tunneloidaan” vastaanottavalle solmulle kotireitittimen kautta kuten kuvassa 1. Asiakassolmulta lähtiessä viestin otsakkeiden järjestys on seuraava [ARK04, s. 6]:

```
IPv6-otsake (lähettäjä = tilapäisosoite,
             vastaanottaja = kotireititin)
tunnelimoodin ESP-otsake
IPv6-otsake (lähettäjä = kotiosoite,
             vastaanottaja = vastaanottava solmu)
langattomuuden ilmaiseva otsake
        kotiosoitetestin käynnistysviesti
```

Huomattavaa on, että tunnelimoodin käyttö suojaa tämän käynnistysviestin kotireitittimelle saakka, mutta viesti kulkee suojaamatta kotireitittimeltä vastaanottavalle solmulle. *Langattomuuden ilmaiseva otsake* (mobility header) sisältyy MIPv6:ssa

kaikkiin paketteihin, joissa joko lähettäjänä tai vastaanottajana on langaton solmu. Toinen asiakassolmun lähettämistä viesteistä on *tilapäisosoitetestin käynnistysviesti* (Care-of Test Init). Tämä viesti lähetetään suoraan vastaanottavalle solmulle, kuten nähdään myös kuvasta 1. Molemmat viestit sisältävät *evästeen* (cookie), joka vastaanottavan solmun on vastausviestissään palautettava. Evästeiden tarkoitus on oleellisesti sama kuin sovelluskerroksella käytettävillä, mutta muuta yhteyttä sovelluskerrokseen näillä evästeillä ei ole. Viestin vastaanottamisen jälkeen vastaanottava solmu luo kaksi *avaimengenerointipolettia* (key generation token), toisen kotiosoitteelle, toisen tilapäisosoitteelle. Vastaanottava solmu ylläpitää myös kokoelmaa *nonsseja* (nonce), joiden suositeltu pituus on vähintään 64 bittiä [KEM04, s. 21]. Nonssit vanhenevat tasaisin väliajoin, jolloin vastaanottava solmu luo kokoelmaan uuden nonssin. Asiakassolmun tulee suoraa linkkiä muodostaessaan osata viitata kullakin hetkellä voimassa olevaan nonssiin, mitä varten jokaisella nonssilla on yksiselitteinen indeksi.

Vastaanottava solmu vastaa kotiosoitetestin käynnistykseen *kotiosoitetestillä* (Home Test). Kotiosoitetesti lähetetään kotireitittimelle, ja kotireititin ”tunneloi” viestin asiakassolmulle (kuva 1). Kotireitittimeltä lähtiessä kotiosoitetestin otsakkeiden järjestyksen tulee olla seuraava [ARK04, s. 6]:

```
IPv6-otsake (lähettäjä = kotireititin,
             vastaanottaja = tilapäisosoite)
tunnelimoodin ESP-otsake
IPv6-otsake (lähettäjä = vastaanottava solmu,
             vastaanottaja = kotiosoite)
langattomuuden ilmaiseva otsake
        kotiosoitetesti
```

Linkki vastaanottavan solmun ja kotireitittimen välillä on edelleen suojaamaton. Kotiosoitetesti sisältää asiakassolmun lähettämän evästeen, kotiosoitteen avaimengenerointipoletin sekä lähetyshetkellä voimassa olevan nonssin indeksin. Vastaanottava solmu vastaa tilapäisosoitetestin käynnistykseen *tilapäisosoitetestillä* (Care-of Test), joka lähetetään suoraan asiakassolmulle. Tilapäisosoitetesti sisältää asiakassolmun lähettämän evästeen, tilapäisosoitteen avaimengenerointipoletin sekä lähetyshetkellä voimassa olevan nonssin indeksin. Kun asiakassolmu on vastaanottanut nämä viestit, varsinaisen reititystestin voidaan katsoa päättyneen.

4.2 Suoran linkin muodostaminen

Mikäli mahdollista, reititystestiä seuraa aina *suoran linkin muodostaminen* (route optimization), jolloin asiakassolmu käyttää vastaanottavalta solmulta saamiansa avainpoletteja lähettääkseen sidonnan päivityksen suoraan vastaanottavalle solmulle. Tämän sidonnan päivityksen lähdeosoitteeksi kirjoitetaan asiakassolmun tilapäisosoite, ja kotiosoite sisällytetään MIPv6:n spesifikaation mukaisesti viestin kotiosoiteoptioon. Sidonnan päivityksen tulee sisältää sekä kotiosoitetestissä että tilapäisosoitetestissä ilmoitetut nonssien indeksit. Nämä indeksit toimivat sidonnan päivityksen tärkeimpänä tunnisteena vastaanottavalle solmulle. Kun vastaanottava solmu on vastaanottanut sidonnan päivityksen hyväksystysti, asiakassolmun kotiosoitteen ja tilapäisosoitteen välinen sidonta lisätään vastaanottavan solmun välimuistiin. Vastaanottava solmu voi myös tarvittaessa lähettää asiakassolmulle *sidonnan kuittauksen* (binding acknowledgement). Mikäli voimassa oleva nonssi olisi sidonnan päivityksen saapuessa ehtinyt vanhentua, vastattaisiin sidonnan päivitykseen *sidonnan virhekoodin* (binding error) sisältävällä kuittauksella. Virhetilannetta seuraisi uusi reititystesti.

4.3 Reititystestin turvallisuus

Reititystestin tuloksena asiakassolmun ja vastaanottavan solmun välille syntyy määrätyksi ajaksi löyhähkö turvayhteys, joka on kuitenkin riittävän voimakas siihen, että suora linkki näiden kahden välille voidaan muodostaa. Reititystestillä suojattu asiakassolmun ja vastaanottavan solmun välinen suora linkki tulee päivittää 7 minuutin välein, ja nonssit saavat olla voimassa korkeintaan 4 minuuttia (suositus 3,5 minuuttia) [KEM04, s. 23]. Reititystesti ei suojaa kotireitittimen ja vastaanottavan solmun välistä linkkiä edellisten lukujen kuvaamilta hyökkäyksiltä, mutta turvaratkaisun laajamittainen ajastus ehkäisee pitempiaikaiset hyökkäykset tätä turva-aukkoa hyödyntäen. Toisaalta reititystestistä aiheutuvat MIPv6:n spesifikaation turva-aukot eivät ole sen vakavampia kuin tavallisessa IPv6-protokollassakaan [KEM04, s. 24]. Tämän perusteella reititystestin voidaan katsoa noudattavan uusien turvaratkaisujen käyttöönotossa suositeltua ”Harm not” -direktiiviä [KOO07, s. 63]. Direktiivin mukaan uudet turvaratkaisut eivät saa luoda uusia hyökkäysmahdollisuuksia ja siten avata uusia ovia hyökkääjille.

5 MIPv6:n tulevaisuus

MIPv6:n tulevaisuudennäkymät riippuvat voimakkaasti koko IPv6:n tulevaisuudesta. Koska IPv4:n osoiteavaruuden käyttö on etenemässä kriittiseen vaiheeseen [PAL07, s. 17], jossa käyttökelpoiset verkko-osoitteet käyvät vähiin, ovat tietoyhteiskunnat valinnan edessä: Joko IPv4:ää hyödynnetään viimeiseen asti tai sitten siirrytään IPv6:een. Käytännössä vaihtoehtoja on silti enemmänkin. Voidaan esimerkiksi siirtyä käyttämään IPv6:ta vain tilapäisesti tai vain siinä määrin, että osoitteita saadaan riittävä määrä. Tarvittaessa voidaan myös lisätä *NAT*:n (Network Address Translation) käyttöä, jolloin yhdellä verkko-osoitteella tavoitetaan useampia laitteita.

Reititystestin kehittäminen on asettanut perusteet MIPv6:n käytön turvalliselle jatkamiselle ja asteittaiselle lisäämiselle. Protokollan kehityksessä on jatkuvasti pyritty pienentämään asiakassolmun vaeltamisesta ja uuteen verkkoon kiinnittymisestä seuraavia viiveitä asiakassolmun ja vastaanottavan solmun välisessä tietoliikenteessä. Osaksi viivettä pienentää IPv6:n perusominaisuuksiin kuuluva tilaton osoitekonfiguraatio. Mielenkiintoinen esimerkkikokeilu viiveisiin liittyen tehtiin vuonna 2005, jolloin esiteltiin *SHMIPv6* -protokolla (Stealth-time Hierarchical MIPv6), joka kaikissa testitapauksissa pienensi viiveitä ja pakettien hävikkiä normaaliin MIPv6:een verrattuna [LAI05].

IETF jatkaa edelleen kehitystyötä MIPv6:n ja IPsec:n parissa kansainvälisin voimin. Ilahduttavan moni suomalainenkin tutkija kuuluu kehityksestä vastaaviin työryhmiin. Kehitteillä on esimerkiksi langattomaan tietoliikenteeseen paremmin soveltuva IKE-protokollan kakkosversio. Jokainen palveluntarjoaja voi edistää IPv6:n ja siten myös MIPv6:n kehitystä yksinkertaisesti alkamalla tarjota IPv6:ta käyttäviä palveluita. Tietoturvan tärkeys korostuu entisestään tulevaisuudessa, koska on odotettavissa, että pahat tahot kehittävät yhä monimutkaisempia hyökkäyksiä. Samalla pahat tahot ilmeisesti järjestäytyvät yhä suuremmiksi tietoliikenteen turvallisuutta uhkaaviksi voimiksi.

Myös ihmisten käyttämien langattomien tietoverkkoon kytkettävien laitteiden määrän voidaan olettaa kasvavan edelleen. Hyvänä esimerkkinä ovat esimerkiksi kännykkäoperaattorit, jotka tarjoavat nykyään usein asiakkailleen langattomaan Internet-asiointiin tarkoitettuja ”miniläppäreitä” tai ”mokkuloita” liittymäpakettien yhteydessä.

6 Yhteenveto

Tämä tutkielma käsitteli MIPv6:ta, protokollan turvallisuusuhkia ja turvaratkaisuja, erityisesti reititystestiä. Aiheiden käsittely kohdistui jonkin verran myös tulevaisuuden visiointiin tutkielmassa todetun pohjalta. Tutkielma käsitteli tietoturva-asioita ja reititystestiä melko yksityiskohtaisesti tinkien kenties samalla muiden mielenkiintoisten aiheiden yksityiskohtaisesta käsittelystä. IKE-protokollan tarkempi toimintalogiikka ja reititystestin mahdolliset variantit ovat kuitenkin selkeästi tutkielman aihealueiden ulkopuolella. Lisätietoa näistä löytyy tutkielman lähteistä, erityisesti [KOO07]:stä.

IPv6-protokollan ohella MIPv6:n kehittäminen on ollut välttämätöntä, koska langaton tietoliikenne on yhä yleisempää nykyaikaisissa tietoliikenneverkoissa. MIPv6:n kehitys on sellaisella tasolla, että protokollaa voidaan pitää IPv4:n langatonta tietoliikennettä tukevien protokollien luonnollisena seuraajana. IPsec:n ja reititystestin avulla MIPv6:ta käytettäessä voidaan tyydyttävästi suojautua samanlaisilta turvallisuusuhilta kuin MIPv6:ta edeltävissäkin langattoman tietoliikenteen protokollissa. Reititystesti ei ole täysin vedenpitävä ratkaisu, mutta tarjoaa edes jonkinlaista turvaa asiakassolmun ja vastaanottavan solmun väliselle yhteydelle, joka muutoin olisi täysin suojaamaton. Reititystestissä olevat turva-aukot liittyvät kuitenkin läheisesti tietoliikenteessä jo havaittuihin tietoturva-aukkoihin eikä testin käyttö avaa mitään uusia ovia hyökkääjille. Tutkimustyö asiakassolmun vaeltamiseen liittyvien viiveiden pienentämiseksi on myös tuottanut konkreettisia tuloksia. Langattomien laitteiden määrän lisääntyessä MIPv6:n käytön voidaan olettaa lisääntyvän entisestään. Käytön lisääntyminen tietoyhteiskunnissa on hyvä haaste protokollalle ja sen nykyisille tietoturvaratkaisuille. Tällaisen tosielämässä, erityisesti kaupallisessa käytössä suoritetun testauksen voidaan myös olettaa asettavan selkeät suuntaviivat MIPv6:n tulevalle kehitykselle.

Lähteet

ARK04 Arkko, J., Devarapalli, V. ja Dupont, F., Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents (RFC 3776), 2004. `http://www.ietf.org/rfc/rfc3776.txt`. [24.4.2009]

AUR02 Aura, T., Roe, M. ja Arkko, J., Security of Internet Location Manage-

ment. *Computer Security Applications Conference, 2002. Proceedings. 18th Annual*, sivut 78–87.

HAM09 Hamilton, D., IPv6 Support At Meager Four Percent, 2009. `http://www.thewhir.com/web-hosting-news/030909_IPv6_Support_At_Meager_Four_Percent`. [23.3.2009]

KEM04 Kempf, J., Arkko, J. ja Nikander, P., Mobile IPv6 Security. *Wireless Personal Communications*, 29,2(2004), sivut 389–414.

KOO07 Koodli, R. S. ja Perkins, C. E., *Mobile Inter-networking with IPv6*. Wiley-Interscience. Hoboken, New Jersey (USA), 2007.

LAI05 Lai, W. K. ja Chiu, J. C., Improving Handoff Performance in Wireless Overlay Networks by Switching Between Two-Layer IPv6 and One-Layer IPv6 Addressing. *IEEE Journal on Selected Areas in Communications*, 23,11(2005), sivut 2129–2137.

NIK03 Nikander, P., Arkko, J., Aura, T. ja Montenegro, G., Mobile IP version 6 (MIPv6) Route Optimization Security Design. *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*, 3, sivut 2004–2008.

OSH01 O'Shea, G. ja Roe, M., Child-proof Authentication for MIPv6 (CAM). *ACM SIGCOMM Computer Communication Review*, 31,2(2001), sivut 4–8.

PAL07 Palet, J., The Choice: IPv4 Exhaustion or Transition to IPv6, 2007. `http://www.6journal.org/archive/00000285/01/the_choice_ipv4_exhaustion_or_transition_to_ipv6_v4.4.pdf`. [15.3.2009]