Mobilitás-kezelés az IPv6-ban

előadás jegyzet (VIHIAV07 - IPv6 alapú számítógép-hálózatok)

Írta: Bokor László, Dudás István, Nováczki Szabolcs

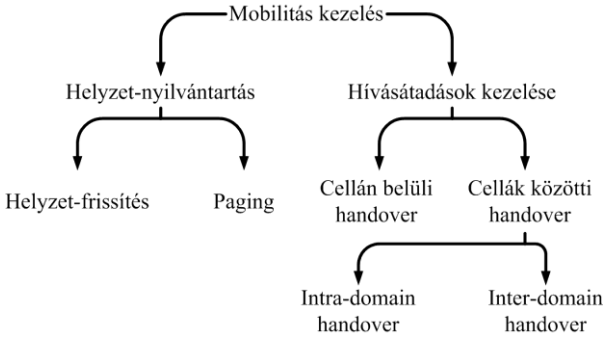
Budapesti Műszaki és Gazdaságtudományi Egyetem, Híradástechnikai Tanszék

Tartalom

Bevezetés

A vezeték nélküli hozzáférést biztosító hálózatok az elmúlt évtizedben olyan széles körben elterjedtek, hogy manapság már a felhasználók egy jelentős hányada e hálózatok szolgáltatásait veszi igénybe. Ezért a szolgáltatók − felismerve a vezeték nélküli kommunikációban rejlő lehetőségeket − arra törekednek, hogy a mobil felhasználók számára is minőségi szolgáltatásokat nyújtsanak. Ennek egyik elengedhetetlen feltétele olyan mobilitás kezelő eljárások kifejlesztése, melyek zavartalan összeköttetést biztosítanak a felhasználók mozgása miatt bekövetkező változások hatásainak kezelése közben is. Sok, egymástól merőben eltérő megközelítést használó megoldás született, mely többé-kevésbé biztosítja a mobilitás transzparens kezelését. Bár ezek a módszerek részleteikben különböznek, mégis találhatunk olyan közös tulajdonságokat, melyeket felismerve meghatározhatók a mobilitás kezelésének alapelvei. Ez a bevezető fejezet ezekről ad összefoglaló képet.

A mobilitás kezelése alapvetően két feladat megvalósítását [1] jelenti (1. ábra). Egyrészt szükség van a folyamatosan mozgó mobil csomópontok helyzetének követésére, másrészt meg kell oldani az ún. hívásátadás (handover) kezelését, azaz a felhasználók kapcsolatainak karbantartását, miközben a hálózat egyik kapcsolódási pontjától egy másikhoz vándorolnak. Az előbbit helyzet-nyilvántartásnak (Location Management), az utóbbit pedig hívásátadás-kezelésnek (Handover Management) hívjuk.

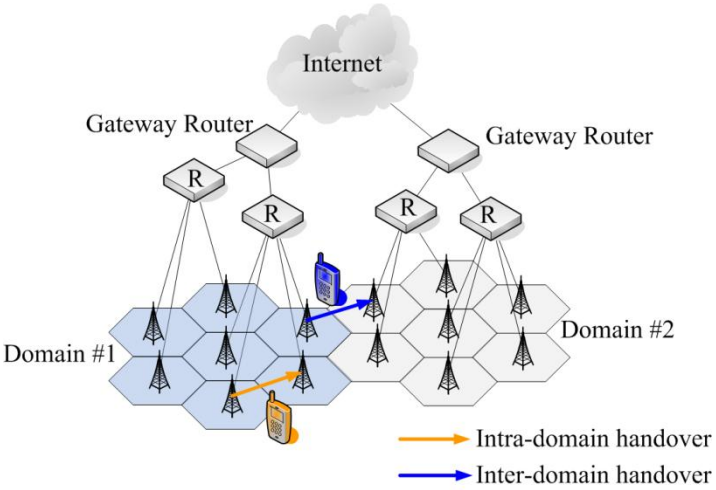


1. ábra. A mobilitás-kezelés feladatai

A helyzet-nyilvántartásnak két feladatot kell megoldania. A mobil csomópontok követését, azaz a helyzet-frissítést (Location Update), valamint ezen mobil egységek megkeresését (paging), amikor nekik címzett adatok átvitelére van szükség. A keresésre azért lehet szükség, mert a helyzet-frissítés nem feltétlenül követi teljesen pontosan a mobilok mozgását, ezért az éppen nem kommunikáló csomópontokat meg kell találni, ha üzeneteket akarunk nekik továbbítani. Erről a későbbiekben részletesen lesz szó.

Egy cellás hálózatban a hívásátadások két típusát különböztetjük meg [1]. Az egyik akkor következik be, amikor a felhasználó nem hagyja el egy adott cella lefedettségi területét, de megváltoztatja az eddig használt rádiós csatornát, ezáltal csökkentve csatornák közötti interferenciát. Ezeket a cellán belüli handovereket valamilyen második (link) réteg béli protokoll kezeli. A másik eset az a szituáció, amikor egy mobil csomópont cellák között vándorol. Bár ebben az esetben is elengedhetetlen a link réteg támogatása, önmagában ez nem mindig elég a probléma megoldásához. Ennek oka, hogy a cellaváltáskor (pl. Wi-Fi hozzáférési pontok közötti mozgás során) megváltozhat a csomópont IP címe. Ez viszont befolyásolja a hálózati réteg működését, amit már nem lehet kizárólag a link rétegben megoldani. Szükség van valamelyik felsőbb réteg támogatására is. Kézenfekvő megoldás, ha a hálózati réteget használjuk az ilyen típusú handoverek kezelésére (erre a feladatra szinte bármelyik felsőbb réteg alkalmas lehet).

Bármelyik rétegben is oldjuk meg a cellák közötti handoverek kezelését egy további fontos tulajdonságra érdemes tekintettel lenni: a vezeték nélküli hálózatok általában földrajzilag nagy területeket fednek le, mely további alhálózatokra, tartományokra (domain) osztható. Ahogy a 2. ábrán is látható, egy ilyen hálózatban a hívásátadás (handover) két alapvető módon valósulhat meg [2].



2. ábra. Handover-típusok

Az egyik az intra-domain handover, ami egy jól definiált területen (ún. mikromobilitási domainen) belüli cellaváltásokra vonatkozik. Ezt kezelik a mikromobilitás protokolljai. Makromobilitásról pedig akkor beszélünk, ha két domain között mozog a mobil csomópont. Ezt inter-domain handovernek nevezünk. Ezt már valamilyen makromobilitási protokoll kezeli. A mikromobilitás algoritmusainak egy fontos célja, hogy minél gyorsabban próbálják lebonyolítani az intra-domain handovereket, ezzel növelve az elérhető teljesítményt, a hálózat kihasználásának hatásfokát, és minimalizálva a felhasználói adatfolyamok megszakításának időtartamát. Ezek azonban általában nem skálázható megoldások, így csak korlátozott számú felhasználó kezelésére képesek. Erre nyújtanak megoldást a makromobilitás kezelő protokollok, melyek a felhasználók számától függő, skálázható megoldást adnak. Ezek azonban nem képesek olyan gyorsan kezelni a cellaváltásokat, mint a mikromobilitási protokollok. Ezért a mobil csomópontok kezelését általában olyan hierarchikus módszerekkel oldják meg, melyekben együtt alkalmazzák a makro-, és a mikromobilitás kezelő protokollokat. Így ezek egymást kiegészítve, hatékony megoldást nyújtanak a felhasználói mobilitásra.

Mindkét mobilitás-kezelési probléma megoldására születtek javaslatok, melyekből egyet-egyet a következő fejezetben fogunk bemutatni. Mielőtt azonban rátérnénk az egyes protokollok ismertetésére, érdemesnek összefoglalni a mikromobilitás kezelő módszerek közös vonásait, és megvilágítani azt, hogy miként javítják a mozgó csomópontok kezelésének hatékonyságát.

A mikromobilitási protokollok gyorsasága a hálózatváltások lokális kezelésében rejlik [3]. A felhasználók domainen belüli mozgását elfedik a makromobilitási protokoll elől, tehát nincs szükség annak bevonására minden cellaváltásnál. A regisztrációs és a jelzési üzenetek − megvalósítástól függően − legfeljebb a domain gyökér routeréig kell eljutniuk, a gyökér router pedig ezeket már gyorsan fel tudja dolgozni. Tehát a gyorsaság a kis terület, a limitált számú felhasználó, és a makromobilitási protokoll kihagyásának következménye.

Bár a fenti alapkoncepciókat mindegyik protokoll figyelembe veszi, azok megoldására azonban eltérő módszereket adnak, ezért a mikromobilitási protokoll tervezeteket működésük és alapgondolatuk szerint néhány nagy csoportba lehet szervezni:

- Proxy Agent Architectures (PAA): Hierarchikus szervezésű, ügynök alapú gyorsítás. Ezek a megoldások az adott makromobilitási protokoll ötletét terjesztik ki többszintű, hierarchikusan szervezett mobil ágensek használatával. A rendszer célja az ágensek működésének gyorsítása. A mobil terminál a hierarchia legalsó szintjén elhelyezkedő helyi ágensnél regisztrálja magát. Minden ágens a felette elhelyezkedő ágensnél regisztrálja a mobil terminált, egészen addig, amíg a regisztráció el nem jut a domain gyökér csomópontjáig. Ebben a rendszerben, a terminál mozgása során bekövetkező IP cím-változásokat kezelő üzenetek nem terhelik az egész hálózatot, hanem lokálisan, az adott

domainen belül történik a kezelésük. Ebbe a csoportba tartozik például a Hierarchical Mobile IPv6 (HMIPv6).

- Locally Enhanced Routing Schemes (LERS): Ezek a megoldások a mikromobilitási domainen belül egy módosított routing algoritmust használnak és tipikusan a hálózati rétegben, az IP (IPv4 vagy IPv6) protokollt kiegészítve működnek. Ezen a csoportot tovább oszthatjuk, az alkalmazott routing protokoll szerint:

    1. Az ún. Per Host Forwarding megoldások egy domainen belül speciális útvonal-nyilvántartási protokollt használnak, hogy létrehozzanak a mobil csomópontokra vonatkozó, adott idő után elévülő (soft-state) bejegyzéseket az útvonalválasztók routing tábláiban. Mivel a bejegyzések idővel elévülnek, periodikus frissítés szükséges. A domain egy gateway router (GW) segítségével kapcsolódik a vezetékes internethez, és kívülről egy alhálózatnak látszik. A GW végzi el a protokoll konverziót az IP, és az alkalmazott mikromobilitás protokoll között. E csoportba tartozik a két legismertebb mikromobilitás protokoll, a Cellular IP (CIP) és a HAWAII.

    2. A Mobile Ad-hoc Network (MANET) alapú rendszerek tipikusan valamilyen mobilitás kezeléssel kiegészített ad-hoc routing protokollt (Ad-hoc On-demand Distance Vector – AODV, Dynamic Source Routing – DSR) használnak a mikromobilitás kezelésére.

    3. A multicast alapú megoldások valamilyen multicast módszert alkalmazva keresik meg a mobil csomópontokat a hálózatban.

A mikromobilitási protokolloknak, szintén a mikromobilitási domainen belüli működésük alapján, de az előzőektől részben eltérő szempontokat figyelembe véve, további két csoportosítása képzelhető el:

- Proaktív vagy reaktív: Egy proaktív protokoll esetén a hálózat mindig ismeri a mobil csomópont tartózkodási helyét. Ezt folyamatosan küldött, helyzet-frissítő üzenetekkel érik el. Ezzel ellentétben, egy reaktív protokoll esetén a mobil csomópontot meg kell keresni (paging alkalmazása), mikor adatot szeretnénk hozzá eljuttatni. Ezt broadcast (üzenetszórást) vagy multicast üzenetek kiküldésével lehetséges. A proaktív protokoll a sok frissítő üzenet miatt nagy adatforgalommal terheli a hálózatot, de azonnal irányítani tudja a beérkező adatot a megcímzett mobil felhasználó felé. A reaktív protokoll viszont szinte alig, vagy egyáltalán nem terheli a hálózatot jelzési üzenetekkel, amikor nincs adatforgalom, viszont nagyméretű – broadcast vagy multicast – keresést igényel az adatátvitel kezdetekor. Vannak olyan megoldások, amelyek a proaktív és reaktív előnyeit egyesítve, azok hátrányait kiküszöbölve működnek. E protokollok proaktív módon viselkednek az aktív mobil csomópontok kezelését illetően, és a reaktív tulajdonságokat mutatnak, amikor a tétlen készülékek helyzetének nyilvántartásáról van szó.

- Gateway centrikus vagy hop-by-hop. A gateway centrikus tulajdonság azt jelenti, hogy a gateway router pontosan tudja, hol helyezkedik el a mobil felhasználó, és így közvetlenül hozzá küldi a csomagokat. Hop-by-hop esetben mindig csak azt tudják a routerek, hogy a velük kapcsolatban lévő routerek közül melyiknek kell küldeni egy adott mobil csomópontnak címzett csomagot.

Látható, hogy a mobilitás kezelése igencsak összetett probléma. Nagyon sok szempont figyelembevételére van szükség, melyek együttes teljesítése nem is mindig megoldható.

Mobile IPv6

Alapok

Az IP protokoll esetén az adatok csomagokban kerülnek továbbításra, mely csomagok célcím mezői a cél csomópont azonosítóját tartalmazzák. Amennyiben mobil eszköz mozgása során cellát vált, akkor a mobil terminálnak két lehetősége van: vagy megtartja az addig használt IP címét, vagy pedig új IP címet igényel az új alhálózatban. Az IP protokollok esetén a címzés a hálózat fizikai felépítésén alapul, ami viszont ellentmond a mobilitás által támasztott követelményeknek. A mobilitás-kezelés megtervezésénél két egymásnak ellentmondó szempontot kellett figyelembe venni. Egyfelől az IP címzés hierarchiájának megtartása érdekében a mobil terminálnak minden cellaváltás után új, az adott alhálózatnak megfelelő IP címmel kell rendelkeznie. Másfelől az egyértelmű azonosíthatóság miatt a mobil csomópont egy kommunikációs folyam időtartama alatt csak egy IP címmel rendelkezhet, máskülönben a handover során megváltozott cím következtében a mobil terminál régi címére küldött IP csomagok soha sem fogják elérni a felhasználót az új címén.

A tervezők a fenti két követelmény egyidejű teljesítése érdekében bevezették a Care-of-Address (Care-of-Address, CoA – ideiglenes cím) fogalmát. A Care-of-Address egy olyan szimpla IP cím, amely egy adott hálózatban minden megkötés nélkül érvényes, valamint bármikor kiosztásra kerülhet egy éppen csatlakoztatott host számára (amely host természetesen egy mobil eszköz is lehet). Ezzel a megoldással mindkét probléma megoldható, hiszen a mobil csomópont a CoA megszerzése után érvényes IP címmel fog rendelkezni, valamint valamilyen regisztrációs módszer alkalmazása mellett a hálózat többi részét is értesíteni lehet a használt új címről.

Az IPv6 protokoll a címzés és a csomagformátum megújítása mellett számos fontos változtatást tartalmaz a protokoll működése terén. Egyfelől a mobilitás támogatása az IPv6 esetében már szerves részét képezi a protokoll felépítésének, másfelől a biztonsági megoldások is integrálásra kerültek. Mind a mobilitás, mind a biztonsági megoldások a protokollba való beépítése úgy történt, hogy a lehető legjobban felkészüljenek a jövő kihívásaira, és ezáltal egy időtálló protokollt alkossanak meg.

A Mobile IPv6 (MIPv6) [4] sokban támaszkodik az IPv4 protokoll esetén külön megalkotott mobilitás kezelés megoldásaira (MIPv4) [5], azonban orvosolja az ott megjelent hibákat és problémákat. Az MIPv6 protokoll sok tekintetben kihasználja az IPv6 protokoll nyújtotta lehetőségeket, ezáltal egyszerűbbé téve a mobilitás kezelését. A Mobil IPv6 protokoll szinte valamennyi kontroll üzenet esetén az IPv6-ban definiált kiegészítő fejléceket alkalmazza a mobilitás kezeléséhez szükséges információk közléséhez, ezáltal nagyobb rugalmasságot adva a protokoll mobil kiterjesztésének.

A mobilitás kezelő protokollok megfelelő működéséhez feltétlenül szükséges, hogy a mobil eszközök rendelkezzenek egy honos hálózattal (Home Network, HN – honos hálózat). A honos vagy otthoni hálózatra azért van szükség, hogy a mobil terminálnak legyen egy kitüntetett címe a Home Address (Home Address, HAdd – honos cím), amely cím a hálózat többi része felé publikus, és amely címen a mobil eszköz bármikor elérhető. A mobil csomópontok honos hálózatának a mobilitás kezelés szempontjából kitüntetett szerepük van, hiszen amennyiben egy mobil állomás felé a hálózatból kérés érkezik, akkor a kérés az IP protokoll továbbítási mechanizmusainak köszönhetően a mobil eszköz otthoni hálózatába fog eljutni. Abban az esetben, ha mobil terminál a honos hálózatában tartózkodik, akkor megkapja a neki szánt csomagokat és felépül a kommunikáció a két fél között. Amennyiben a mobil állomás nem tartózkodik a honos hálózatában, úgy a mobil készüléknek szánt csomagokat kezelni kell, amely feladatot a honos ügynök (Home Agent, HA – honos ügynök) látja el. A Home Agent legfőbb feladata, hogy regisztrálja és nyilvántartsa a mobil csomópont mozgását és aktuális csatlakozási pontját a hálózatban. Erre annak érdekében van szükség, hogyha kérés érkezik a mobil állomás honos hálózatába, de az éppen egy távoli ponton csatlakozik a hálózathoz, akkor a honos ügynök a beérkezett kérést továbbítani tudja a mobil terminál valós tartózkodási helye felé. A mobil állomás otthoni hálózatában nem csak egy, hanem akár több HA is lehet. Ebből következően a mobil készülék több honos ügynökkel is tarthatja a kapcsolatot.

Annak érdekében, hogy a Home Agent mindig pontos információkkal rendelkezzen a mobil terminál tartózkodási helyéről, a mobil csomópont köteles periodikusan tájékoztatni a honos ügynököt. A mobil állomás miután csatlakozott az idegen hálózathoz (Foreign Network, FN – idegen hálózat) felderíti a kapcsolódási pont új alhálózatát a helyi router által rendszeresen küldött Router Advertisement (Router Advertisement, RA – router hirdetés) üzenetek [6] segítségével. Az új alhálózat felderítése után a mobil eszköz, az IPv6 protokoll által bevezetett automatikus címmegszerzés (Address AutoConfiguration, AAC – automatikus címmegszerzés) mechanizmus segítségével, kétféleképpen juthat érvényes Care-of-Address-hez.

Stateful automatikus címmegszerzés alkalmazása esetén a mobil host a szervertől kér egy CoA-t, amely egyediségét a szervernek kell garantálnia. Ez többnyire azt jelenti, hogy a szerver nyilvántartja a még szabad címeket, amik még használhatóak a domain-en belül, majd ezen címek közül egyet hozzárendel az alhálózathoz csatlakozni kívánó új terminálhoz.

Stateless automatikus címmegszerzést alkalmazva a mobil készülék az új cellába belépve a router hirdetéséből megismeri az érvényes hálózati előtagot. A saját azonosítója elé helyezve a megismert hálózati előtagot elkészíti a javasolt címét (link-local address). Ezt az eljárást a cím hitelesítési folyamat követi (Duplicate Address Detection, DAD – duplikált címfelderítés) annak érdekében, hogy az alhálózatban a cím egyediségét biztosítani lehessen.

A mobil eszköz bármelyik címmegszerzési módot választhatja, hiszen mindkét módszernek megvannak a maga előnyei illetve hátrányai. Stateful esetben a szerver válaszideje lehet nagy, ha a címkérésnek több topológiai szintet kell megjárnia. Míg stateless címszerzés esetén a DAD eljárás tarthat hosszabb ideig, amennyiben sok host csatlakozik az alhálózathoz. Ezáltal a mobil csomópontok a hálózati struktúrának megfelelően váltogathatják az automatikus címmegszerzés módját.

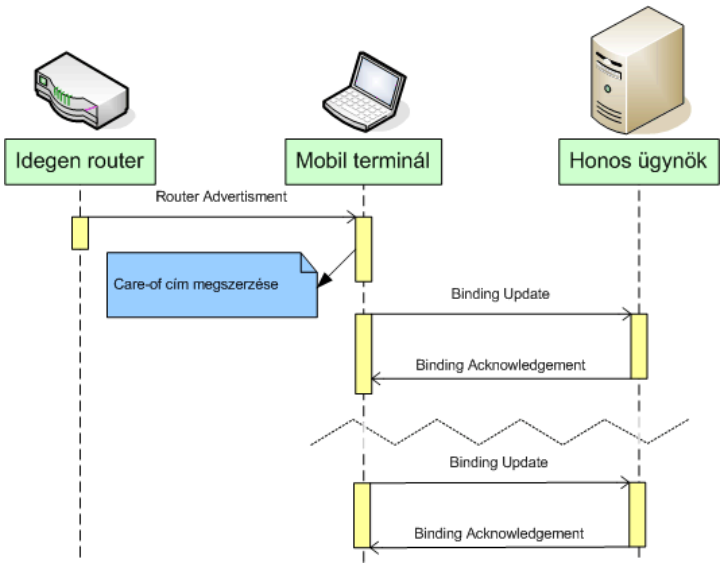
Binding Update

Miután a mobil állomás megszerezte a fent leírt két módszer valamelyikével az új Care-of-Address-ét, értesítenie kell a honos ügynökét az új cím megszerzéséről. Ezt a folyamatot binding-nak (binding - kötés) nevezzük [4].

A mobil állomásnak – miután észlelte a cellaváltás tényét és sikeresen lezáródott az új CoA megszerzésének folyamata – értesítést kell küldenie a honos ügynöke irányában, annak érdekében, hogy értesíthesse azt az új Care-of-Address-éről. A mobil terminál egy Binding Update (Binding Update, BU – kötés frissítés) üzenetet küld Home Agent-jének, amely attól függően, hogy a küldő mobil eszköz már szerepelt a nyilvántartásában vagy új regisztrációról van szó, frissíthet, vagy új bejegyzést hozhat létre. A BU üzenetnek tartalmaznia kell a CoA-t a csomag forrás címében, valamit a mobil állomás honos címét a csomag fejléc opciós mezejében. A honos ügynöknek – amennyiben új regisztrációról van szó – meg kell győződnie a honos cím alapján, hogy egyfelől ő felelős-e az adott mobil állomásért, másfelől, hogy a megkapott honos cím egyedi-e az adott alhálózatban. Amennyiben mindkét kérdésre adott válasz pozitív, akkor a honos ügynök létrehozza a mobil csomópontra vonatkozó új bejegyzést az adatbázisában és egy Binding Acknowledgement (Binding Acknowledgement, BA – kötés megerősítés) üzenetet küld a mobil eszköznek, jelezve, hogy az regisztrálásra került.

Amennyiben a mobil állomás már szerepelt a Home Agent adatbázisában, úgy csak a binding élettartamának meghosszabbítására kerül sor, amit ugyancsak egy BA üzenet jelez a mobil terminál számára.

A mobil állomás tehát periodikusan köteles frissíteni a honos ügynök irányában a kötést, máskülönben a kötés időtartamának lejártával megszűnik a binding. Azonban a mobil csomópont nem frissítheti tetszőlegesen gyakran a kötést, mivel a túl gyakori Binding Update üzenetváltás indokolatlanul nagy terhelést jelentene a honos ügynök és a hálózat számára. A Binding Update üzenetváltás folyamatát a 3. ábra mutatja.



3. ábra. A Binding Update menete

A mobil terminál az aktuálisan fenntartott kötésekről nyilvántartást vezet (Binding Update List – kötés frissítési lista) annak érdekében, hogy mindig pontosan ismerje az fenntartott kötések számát, azok még hátralévő élettartamát, illetve a kötésben használt CoA-t. Ez utóbbi paraméter azért fontos, mivel a cellaváltás után mikor új CoA-re tett szert a mobil állomás, a Binding Update lista alapján képes értesíteni a vele kapcsolatban álló csomópontokat a címváltozás tényéről.

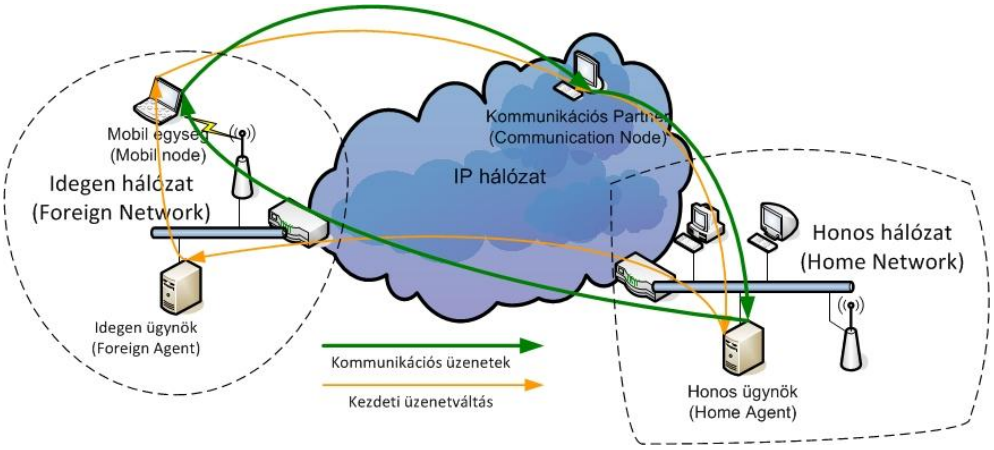
Amikor a mobil eszköz Binding Update üzenetet küld az otthoni hálózata irányába, előfordulhat, hogy nem ismeri az otthoni hálózatában található egyik honos ügynök címét sem. Ilyen szituáció elképzelhető, amennyiben az otthoni hálózat újrakonfigurálásra kerül, mialatt a mobil terminál nem tartózkodik az otthoni hálózatában, hiszen az újrakonfigurálás során például a dinamikus cím kiosztásnak köszönhetően megváltozhat a honos ügynök címe. A mobil csomópontot kiszolgáló Home Agent megváltozhat úgy is, hogy a mobil terminál távolléte alatt az őt kiszolgáló honos ügynökben valamilyen hiba lép fel, és ezáltal kénytelen a honos ügynök átadni a feladatait egy másik, az otthoni hálózatban található Home Agent-nek. Az ilyen típusú váltásokról a honos hálózatba tartozó – de nem ott tartózkodó – mobil eszközök nem kapnak értesítést, ezért a következő kapcsolatfelvétel során nehézségekbe ütközhetnek. Az ilyenkor felmerülő problémák megoldására vezették be a Dynamic Home Agent Address Discovery (Dynamic Home Agent Address Discovery, DHAAD – dinamikus honos ügynök felderítés) mechanizmust.

A DHAAD mechanizmus arra szolgál, hogy a távoli hálózathoz kapcsolódott mobil eszköz képes legyen felkutatni az otthoni hálózatában az aktuálisan működő honos ügynököket. A DHAAD mechanizmus kezdeti lépéseként a mobil állomás egy DHAAD Request üzenetet küld a honos ügynökök anycast címére [7]. Az anycast cím ebben az esetben több honos ügynök interface-éhez van hozzárendelve, amelyek közül a kérés pillanatában legkisebb metrikájú fog válaszolni. Az anycast címek alkalmazására azért kerül sor, mivel a mobil eszköz nem tarthatja nyílván a honos hálózatában található valamennyi honos ügynököt, míg az összes honos ügynök közül legalább az egyik könnyen elérhető az anycast cím segítségével. A DHAAD kérésre adott válaszüzenetben a honos ügynök közli a mobil állomással az aktuálisan aktív honos ügynökök listáját, amely alapján a mobil eszköz kiválasztja a használni kívánt Home Agent-et a megkapott lista szigorú sorrendjében. Amennyiben a mobil eszköz Binding Update listájában található érvényben lévő kötés valamely honos ügynökhöz, akkor a mobil terminálnak először ezen kötést kell megpróbálnia frissíteni, és csak a próbálkozás sikertelensége esetén kezdhet hozzá az otthoni hálózatában található honos ügynökök dinamikus felderítéséhez.

Kötés kialakítása a kommunikációs partner irányában

Eddig a mobil terminál mozgásának következményei illetve a honos ügynökkel fenntartott kapcsolatának részletei kerültek elemzése, azonban a mobilitás kezelés szempontjából legalább ugyanilyen fontos a kommunikációs partnerrel (Correspondent Node, CN – kommunikációs partner) fenntartott kapcsolat bemutatása is.

A kommunikációs partnerrel fenntartott kapcsolatot kétféleképpen csoportosíthatjuk: a kommunikációs fél MIPv6 képes vagy sem. Amennyiben a CN csak az IPv6 protokoll stack-et támogatja, és nincs felkészítve a MIPv6 által küldött vezérlő üzenetek feldolgozására, akkor a kommunikáció a kétirányú alagutazás segítségével történik. A Correspondent Node által küldött csomagok a honos ügynök felé kerülnek továbbításra, amely mobil terminál távollétében elfogja a csomagokat, majd azokat alagutazás segítségével továbbítja a mobil eszköz regisztrált elsődleges Care-of-Address-e irányába. A mobil eszköz egy ellentétes irányú alagút (reverse tunnelling) segítségével a honos ügynöknek küldi a válaszcsomagokat, amely az IPv6 protokollnak megfelelően továbbítja a csomagokat a kommunikációs partnernek.



4. ábra. Háromszögelési probléma a Mobil IPv4 esetén

Abban az esetben, ha a Correspondent Node fel van készítve a MIPv6 protokoll támogatására, akkor a mobil terminál és a kommunikációs partner közötti adatáramlás leegyszerűsödik. Az itt alkalmazott megoldás sokban támaszkodik a MIPv4 [5] protokollban bevezetett megoldásra, azonban további finomításokra került sor. A MIPv4 protokoll esetén a Correspondent Node a mobil eszköz honos hálózata irányába küldi a csomagjait, ahol a honos ügynök továbbítja azokat a mobil terminál aktuális idegen hálózata felé. Az idegen hálózatban az idegen ügynök (Foreign Agent, FA – idegen ügynök) kapja meg a csomagokat, majd irányítja a csomagokat a mobil állomás felé. A mobil eszköz ekkor nem a honos ügynök irányába válaszol, hanem közvetlenül a kommunikációs partnerrel veszi fel a kapcsolatot. Mivel azonban a mobil terminál által küldött csomagokban a forráscím mezőben továbbra is a mobil eszköz otthon címe szerepel, ezért a CN nem értesül a mobil állomás valós helyéről, így csomagjait a honos hálózat felé küldi. Ahogy ez a 4. ábrán jól megfigyelhető az imént vázolt kommunikációs szituációban egy háromszög keletkezik.

A MIPv6 protokoll esetén már sikeresen megoldották ezt a problémát is azáltal, hogy a kommunikációs partnert is képessé tették a kötések (Binding) kezelésére. Akárcsak a honos ügynök esetén, a cellaváltást követően a mobil állomás folyamatban lévő kommunikáció esetén értesíti a kommunikációs partnert a bekövetkezett változásról. Az így létrehozott kötések természetesen bekerülnek a mobil terminál által kezelt Binding Update listába, hiszen ezen kötések regisztrálása és fenntartása ugyanolyan fontos, mint a honos ügynökök esetében.

Return Routability procedúra

A kommunikációs fél irányában történő Binding Update eljárás két jól elkülöníthető részre osztható: elsőként a Return Routability (RR) procedúra zajlik le, amit a tényleges regisztrálás követ. A mobil terminál, miután létrehozta a kötést a honos ügynök felé, csak utána lát hozzá a kommunikációs partnerek értesítéséhez, mivel a Return Routability során szükséges, hogy a honos ügynök már a mobil állomás tényleges Care-of-Address-ével rendelkezzen. A kommunikációs partnerek értesítésekor lezajló üzenetváltás szolgálhatja a kötés megerősítését, valamint törlését egyaránt.

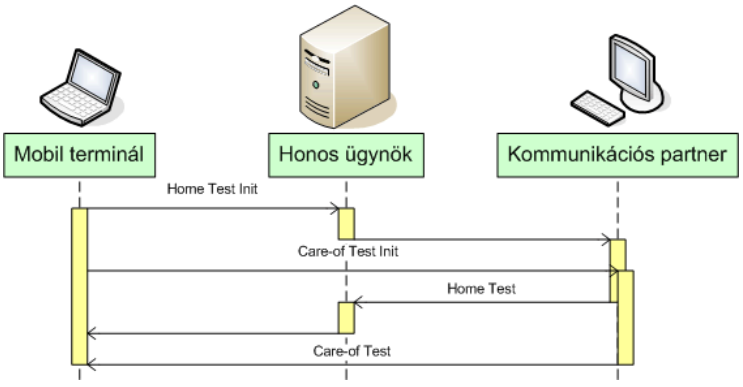
A Return Routability procedúrára azért van szükség, hogy a kommunikációs partner kétséget kizáróan megbizonyodhasson arról, hogy a mobil terminál elérhető az általa használt címek mindegyikén, mind a honos címén, mind pedig az idegen hálózatban szerzett Care-of-Address-én.

A RR eljárást a mobil eszköz kezdeményezi azáltal, hogy elküldi a Home Test Init (HoTI) valamint a Care-of Test Init (CoTI) üzeneteket a kommunikációs fél felé. A két üzenet különböző útvonalon jut el a kommunikációs partnerhez. A HoTI üzenetet a mobil eszköz a Home Agent-en keresztül küldi a Correspondent Node irányába, valamint a csomag forrás cím mezejébe a mobil állomás a honos címét teszi. Míg a CoTI üzenet közvetlenül a mobil eszköz aktuális hálózatából kerül továbbításra a CN felé, továbbá a forrás cím mezőben a mobil terminál aktuális Care-of-Address-e kerül. Mindkét üzenet olyan (egymástól különböző) értéket tartalmaz, amelyet a kommunikációs partnernek vissza kell küldeni, ezáltal biztosítva a válasz üzenetekben, hogy ténylegesen a küldött HoTI és CoTI üzenetekre válaszol.

A megkapott üzenetekre a kommunikációs partner két külön üzenetben válaszol, amelyek azonos útvonalon kerülnek továbbításra a mobil terminál felé, mint azok az üzenetek, amelyek kiváltották a válaszokat.

A Home Test Init üzenetre a Home Test (HT) üzenetet küldi a Correspondent Node. A HT üzenet forrás cím mezejében a kommunikációs partner címe szerepel, míg cél címe a mobil állomás honos címe. Az üzenetben a CN elhelyez egy általa generált tokent, amit a mobil eszköz későbbiekben azonosításra fog felhasználni, továbbá a Home Test üzenetben érkezett érték is belekerül az üzenetbe, végül az üzenetben megtalálható egy, a token egyszerű azonosítására szolgáló index is.

A Care-of Test Init üzenetre a Care-of Test (CT) üzenet kerül elküldésre a mobil eszköz irányában. CT üzenet esetén a cél cím mezőben a mobil állomás aktuális Care-of-Address-e található, így a válasz közvetlenül a mobil eszköz aktuális tartózkodási helye felé kerül továbbításra. A Care-of Test üzenet esetében is elkészít a kommunikációs fél egy tokent, amit ugyancsak a mobil csomópont használ fel azonosítási célokra. A CT üzenet – akárcsak párja a Home Test üzenet – tartalmazza a Care-of Test Init üzentben megkapott értéket, valamit a tokent azonosító indexet.



5. ábra. Return Routability procedúra

A mobil állomás a Return Routability mechanizmus válaszüzeneteit szinte egy időben kapja, amennyiben a különböző linkek nagyjából egyenletesen vannak terhelve. Maga a RR procedúra is elég gyorsan lezajlik, hiszen a válasz üzenetek megalkotásához minimális erőforrás szükséges a kommunikációs partnerben, valamint a HoTI és HT üzenetek továbbítása a honos ügynökben

automatikusan zajlik. A Home Test Init és Care-of Test Init üzenetek és az azokra adott válaszüzenetek továbbításának folyamata az 5. ábrán figyelhető meg.

Amint a mobil terminál megkapta mindkét válasz üzenetet (Home Test és Care-of Test), akkor minden a rendelkezésére áll ahhoz, hogy a megtörténjen a kötés frissítés a kommunikációs partner irányában is. Az üzenetekben kapott tokenek felhasználásával a mobil állomás egy 20 byte hosszúságú kötési kulcsot (binding key, Kbm) generál. Amennyiben egy már létező kötés frissítése történik, akkor a Care-of Test üzenetből nyert token nem kerül felhasználásra, hanem csak a Home Test token vesz részt a kötési kulcs meghatározásában. A Binding Update üzenet felépítése annyiban változik a hagyományos esethez képest, hogy a forrás cím mezőben található Care-of-Address és az opciós fejlécben található Home Address mellett tartalmazza a Kbm kötési kulcsot, valamint a HT és CT üzenetek tokenjeit azonosító indexeket. Az üzenet megérkezését követően a kommunikációs partner feldolgozza a kapott információkat, a kapott indexek alapján a CN könnyen megtalálja a mobil állomás számára elküldött tokeneket, amelyek segítségével ő is képes elvégezni a mobil terminál által alkalmazott átalakításokat, így meg tudja állapítani, hogy tényleg a mobil állomás küldte-e a Binding Update kérelmet. A folyamat végső állomásaként a kommunikációs partner is bejegyzi a mobil eszköz új elérhetési címét a saját Binding Cache-ébe, így a továbbiakban – amíg rendszeresen kapja a kötésfrissítést, vagy egy új cím nem kerül regisztrálásra – a kommunikációs partner ezen a címen próbálja elérni a mobil állomást. A Binding Cache-be a mobil állomások a honos és a Care-of cím párjaikkal kerülnek bejegyzésre, ezért arra is lehetőséget biztosít a Binding Update procedúra, hogy a korábbiakban említetteknek megfelelően a mobil állomás frissítse a honos címét annak megváltozása esetén. Ezt azonban külön jelezni kell a csomagban a megfelelő biztonsági megfontolások betartása mellett. A kötésfrissítési eljárás – akárcsak a honos ügynök esetében – a kommunikációs partner által elküldött Binding Acknowledgement üzenet megérkezésével záródik.

A Return Routability mechanizmus lényege a kommunikációs partner és a mobil állomás közötti biztonságosabb kapcsolat-menedzsment megteremtése. A CN irányába történő kötés létrehozása előtt azért szükséges a Return Routability procedúra végrehajtása, mivel így a kommunikációs partner meggyőződhet arról, hogy ténylegesen azzal a csomóponttal épít ki kapcsolatot, amelyik mind az általa megadott Care-of-Address-en, mind pedig a honos ügynöknél regisztrált honos címén elérhető. Ezáltal kivédhetővé válnak az olyan támadások, amelyekben a támadó a mobil terminált megszemélyesítve egy új CoA-t akar regisztrálni, hogy ezáltal szerezzen meg információkat, hiszen a mobil állomás honos címére küldött tokent csak további támadásokkal lenne képes megszerezni.

A mobilitás kezelés fontos részét képezi a megfelelő szintű biztonság megteremtése a kapcsolatok kiépítésében résztvevő csomópontok számára, mivel a mobilitás tulajdonságaiból adódóan a Mobile IPv6 protokollnak többféle támadással szemben is védelmet kell nyújtania. A támadások legtöbbje hamis kötések létrehozásával próbál meg információhoz jutni a kommunikáló partnerektől. Az ilyen esetekben a támadó általában a mobil terminál megszemélyesítésével próbálja meg hamis kötések létrehozására rábírni mind a honos ügynököt, mind az esetleges kommunikációs partnereket, ezáltal olyan információkhoz jutva, amelyeket eredetileg a mobil állomásnak szántak. Más fajta támadások kivitelezésére is lehetőség lehet, mint a Man-in-the-Middle, ahol a támadó a két kommunikáló fél között lehallgatja az ott zajló információcserét. Az ilyen és ehhez hasonló támadások elleni védekezés igen kritikus, hiszen ilyenkor az adatok megbízhatósága is hitelessége forog veszélyben.

Ahogy azt a mobil eszköz és a kommunikációs partner esetében láttuk, a Return Routability mechanizmus megfelelő biztonságot nyújt, hiszen mindkét fél meggyőződhet arról, hogy a kívánt partnerrel építette ki a kapcsolatot. Azonban fontos látni, hogy a RR procedúra által nyújtott biztonság nagyban támaszkodik arra a feltételezésre, hogy a honos ügynöknél ténylegesen a mobil csomópont regisztráltatta az aktuális Care-of címét. Amennyiben ezt nem képes biztosítani a MIPv6 protokoll, úgy a Return Routability mechanizmus által nyújtott biztonság is megkérdőjelezhetővé válik. A Mobil IPv6 ezért az IPv6 protokollba integrált biztonsági szolgáltatást, az IPSec protokollt veszi igénybe.

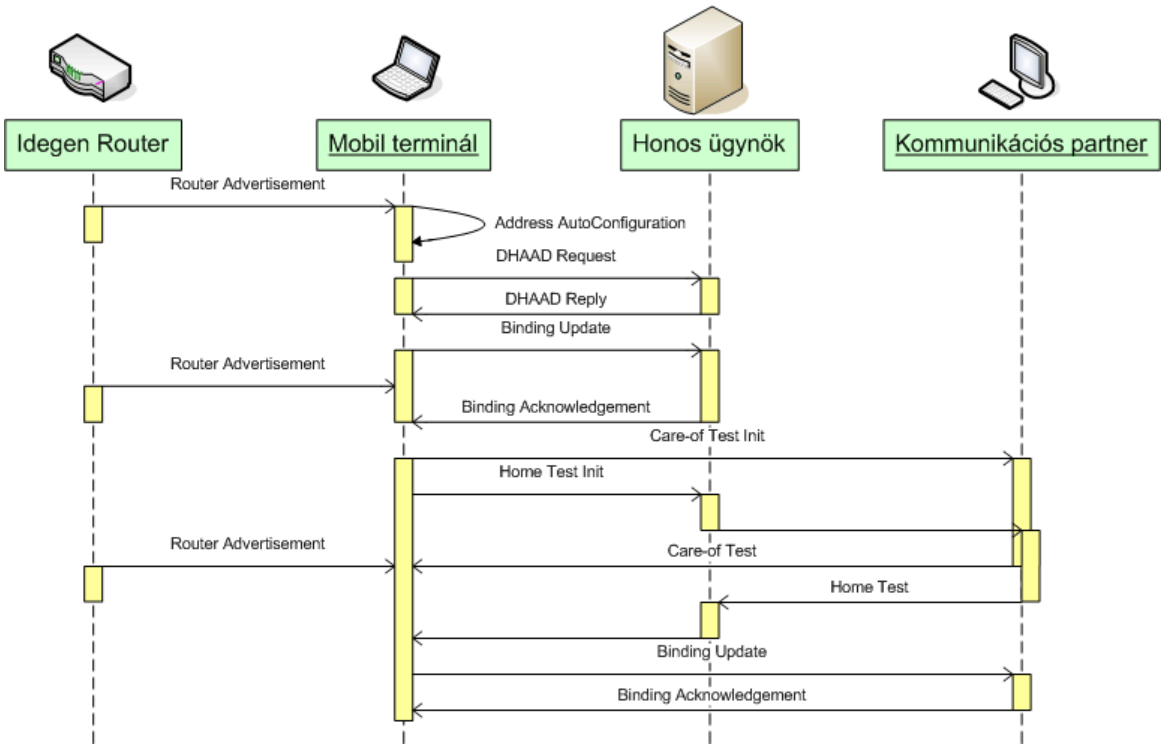
Annak érdekében, hogy a honos ügynök meggyőződhessen a Binding Update üzenet küldőjének kilétéről mind a mobil állomásnak, mind pedig a honos ügynöknek támogatnia kell az Encapsulating

Security Payload (EPS) metódust, amely egy minimális hosszúsággal rendelkező authentikációs algoritmussal megfelelően képes azonosítani a két felet egymás számára. Az így történt azonosítást még további IPSec algoritmusok is kiegészíthetik, amelyek azonban már korábban létrehozott (a folyamatban résztvevő) csomópontokra vonatkozó adatbázis-bejegyzéseket igényelnek. Ezáltal megteremthető a kommunikációban résztvevő összes fél számára a biztonságos adattovábbítás lehetősége.

A kötés kialakításának folyamata

Az előző alfejezetekben bemutatásra kerültek azok a részfolyamatok, amelyek a binding procedúra során lezajlanak, a jelen szakasz pedig teljes egészében leírja a binding során az egymást követő lépéseket.

A teljes binding folyamat illusztrálására a legösszetettebb procedúra bemutatásán keresztül kerül sor, mivel így valamennyi lépés jól megfigyelhetővé válik a 6. ábra segítségével. Ennek érdekében feltételezhetjük, hogy a mobil terminál kezdetben a honos hálózatában tartózkodik, ahonnan a handovert követően átlép egy idegen hálózatba, miközben egy távoli MIPv6 képes Correspondent Node-dal kommunikál. Mivel a mobil eszköz eleinte a honos hálózatában található, ezért sem a honos ügynöknek, sem pedig a mobil eszköznek nem kell kötési információt tárolnia a mobil állomásról. A handover bekövetkezte után a mobil csomópontnak az új hálózatban ideiglenes címet kell szereznie, amit az automatikus címkonfigurálás eljárás segítségével tehet meg, miután az új hálózatában megkapott egy Router Advertisement üzenetet.



6. ábra. A kötés kialakításának teljes folyamata

A mobil terminál azt követően, hogy megszerezte az új Care-of címét, elsőként Binding Update üzenetet küld a honos ügynöke számára annak érdekében, hogy továbbra is elérhető legyen a globálisan érvényes honos címén. A binding sikeres létrejöttét a Home Agent egy Binding Acknowledgement üzenet visszaküldésével nyugtázza. Miután a mobil állomás megkapta az értesítést a kötés sikeres regisztrálásáról a honos ügynöknél, azonnal megkezdi a kötés létrehozását a kommunikációs partner irányába is, ehhez azonban szükséges a Home Test Init – Home Test és a Care-of Test Init – Care-of Test üzenetváltást végrehajtása a mobil terminál és a Correspondent Node között, annak érdekében, hogy az esetleges támadások kivédhetőek lehessenek. Az üzenetváltások

sikeres befejezését követően a mobil eszköz nekiláthat a kommunikációs partner irányában ténylegesen a kötés létrehozásának, így sor kerül a Binding Update elküldésére, amire a kommunikációs partner a sikeres regisztrálás esetén – akárcsak a honos ügynök – Binding Acknowledgement üzenettel válaszol. A kötések sikeres létrejöttét követően létrejönnek a bejegyzések a honos ügynök Binding Cache-ében, valamint a kommunikációs partner és a mobil eszköz Binding List-jében. Ezek a bejegyzések addig maradnak a nyilvántartásokban, amíg újabb bejegyzés nem érkezik, vagy az adott kötéshez tartozó időtartam le nem jár. A kötések későbbiekben történő frissítésénél azonban már nem új bejegyzések keletkeznek a cache-ben illetve a listákban, hanem a már meglévő kötések időtartama kerül megnövelésre.

Hierarchical Mobile IPv6

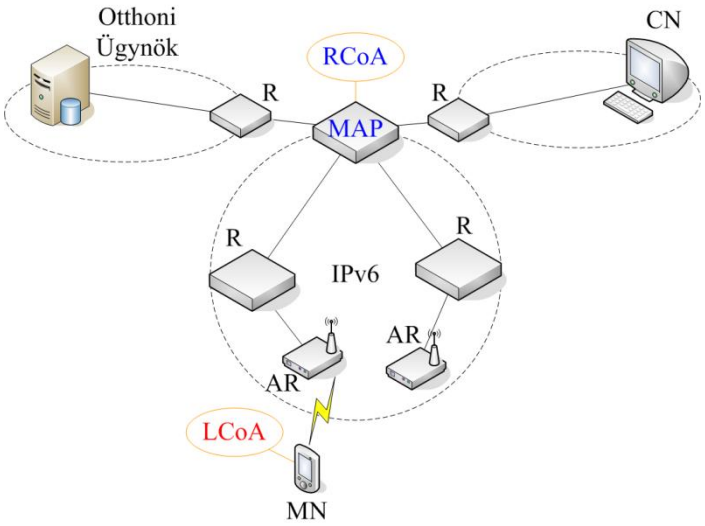
A Mobil IPv6 hasonlóan kezeli egy mobil hoszt helyi (zártabb, adminisztratív domain-en belüli) és globális (domain-ek közötti) mobilitását. Ez a megközelítés nem skálázható, mert nagyszámú mobil hoszt esetén a keletkező jelzésmennyiség túlterhelheti a hálózatot: a már bemutatott mikromobilitás-kezelő protokollokra van szükség. A Hierarchikus Mobil IPv6 [8] a Mobil IPv6 mikromobilitás-kezelést megvalósító kiterjesztése. Célja a domainen belüli jelzésmennyiség csökkentése, továbbá a handover felgyorsítása. Alapötlete a domainek hierarchikus architektúrába szervezése. A helyi handovereket így domainen belül gyorsabban lehet kezelni, elkerülve a felesleges jelzéseket és csökkentve a csomagvesztést.

A HMIPv6 egy új hálózati elemet definiál Mobility Anchor Point-ot (MAP) néven. A MAP feladata a domain-en belüli hálózatváltások kezelése, és ezáltal a domain-en kívüli MIPv6 jelzések mennyiségének a csökkentése, azaz a mikromobilitás biztosítása. A MAP lényegében helyi HA-ként szolgál. A HMIPv6 protokoll bevezetésének a célja a MIPv6 teljesítményének a növelése, úgy, hogy közben a lehető legkevesebb változást kelljen eszközölni a már meglévő MIPv6 (és egyéb IPv6) protokollokon. A HMIPv6 a következő fogalmakat használja:

- Access Router (AR): A mobil eszköz alapbeállítás szerinti routere az adott domainen belül. Az AR gyűjti össze a mobil eszköz kimenő forgalmát.
- Mobility Anchor Point (MAP): A Mobility Anchor Point egy router a mobil eszköz által meglátogatott domainben, mely a nála regisztrált mobilok számára helyi otthoni ügynökként viselkedik.
- HMIPv6-ot támogató mobil eszköz: Egy mobil eszköz, amely képes a HMIPv6 felismerésére és támogatására, azaz képes az access routertől küldött MAP opció kezelésére és regisztráció küldésére.
- On-link care-of address (LCoA): Az on-link care–of address a Mobil IPv6-ban megszabott hagyományos care-of address (közvetett cím), mely a router prefixből és a mobil eszköz azonosítójából tevődik össze. Nem azonos a helyi közvetett címmel.
- Helyi közvetett cím (RCoA): A helyi közvetett cím egy alternatív közvetett cím, amit a mobil eszköz a domainen belül használ. A MAP interfészek egyikéhez tartozik, vagy a MAP prefixéből autokonfigurációval hozza létre a mobil eszköz.
- Helyi Binding Update: A mobil eszköz MAP-nak küldött Helyi Binding Update üzenettel összerendeli a megfelelő RCoA és LCoA címeket.

A HMIPv6-ban a hálózati domain hierarchikus struktúrát alkot. A hierarchia legalján AR-ek (access router, hozzáférési pont) találhatók, felettük HMIPv6 protokollt támogató routerek és a MAP-ok (Mobility Anchor Point) helyezkednek el. A MAP a hierarchia tetszőleges szintjén elhelyezkedhet. A MAP a helyi otthoni ügynök szerepét betöltve lehetővé teszi a jelzések lokalizálását a domainre, ami gyorsabb handovert és kisebb csomagvesztést tesz lehetővé. Így a HMIPv6 képes a MIPv6 teljesítményének növelésére és tökéletesebb handovereket tesz lehetővé.

A MAP megkapja a domainben tartózkodó mobil eszköznek címzett adatcsomagokat, beágyazza őket, majd továbbítja a mobil eszköz aktuális címére. Amennyiben a mobil eszköz címe megváltozik, az új címet csak a helyi MAP-nál kell regisztrálnia. Eközben a globális címe (RCoA, Regional Care-of-Address), amit az otthoni ügynök és a kommunikációs partnerek ismernek, változatlan marad.



7. ábra. A HMIPv6 rendszer

Amikor a mobil eszköz belép egy idegen hálózatba, lekéri a MAP globális címét router advertisement üzenet segítségével és eltárolja az AR-ekbe. Amennyiben a mobil eszköz ugyanazon MAP domainjében mozog, ugyanazt a címet tartalmazó router advertisement üzenetet kapja egy másik alhálózatba belépve. A cím esetleges megváltozása jelzi a mobilnak, hogy belépett egy másik domainbe, ezért Binding Update frissítő üzeneteket küld az otthoni ügynökének és a kommunikációs partnereinek, majd regisztrálja magát az adott MAP-nál. A regisztráció során elküldi otthoni címét és LCoA (On-link CoA) címét. A HMIPv6 a következő funkciókkal bővíti ki a Mobil IPv6-ot:

- Helyi Binding Update (BU): A HMIPv6 a Mobil IPv6 által használt BU üzenetet egy további egybites flaggel bővíti ki, annak jelzésére, hogy a binding-ot a MAP-nál való regisztráláshoz kívánják használni.
- On-link care-of address (LCoA) teszt opció (OCOT): Ez egy nyugtázó üzenet. Használata opcionális és a MAP-ban lehet konfigurálni. Használatát a MAP-nak és a mobil eszköznek is támogatnia kell.
- Neighbour discovery kiterjesztés - MAP opció: A MAP opció a neighbour discovery router üzeneteinek egy kiterjesztése, mely segítségével értesítik a hálózatba érkező mobil eszközöket a MAP jelenlétéről. A MAP globális IP címének prefixe 64. Ezt a prefixet használja a mobil eszköz az RCoA előállításához.

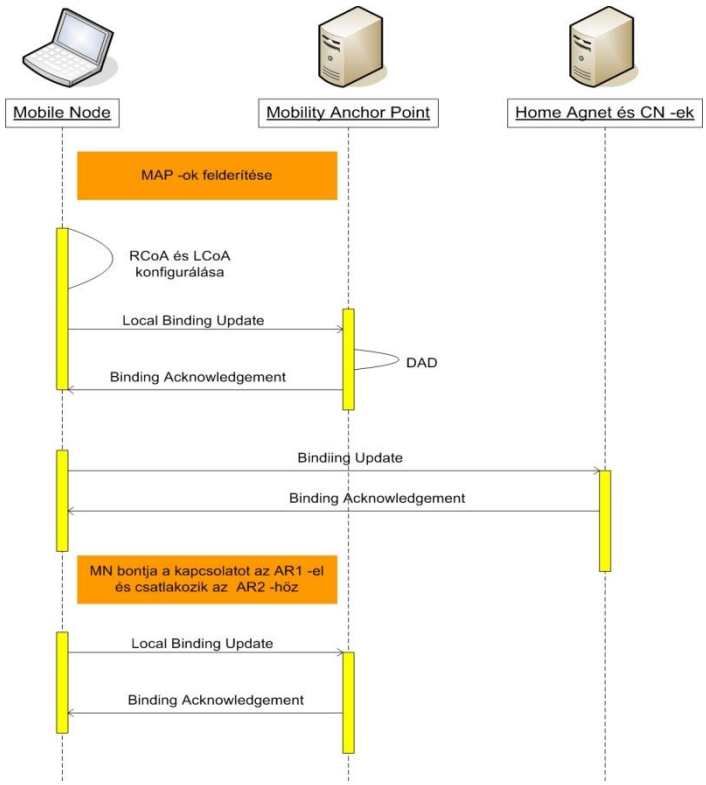
Mivel a MAP domain minden routere ugyanazt a MAP opciót használja, az opciók megváltozása azt jelzi, hogy a mobil hoszt új domainbe lépett be. Ebben az esetben a mobil hosztnak regisztrálnia kell magát az új MAP-nál és értesíteni az otthoni ügynökét és a kommunikációs partnereit az új RCoA céméről.

Az AR-ek is használják a MAP opcióban hordozott információkat. Ennek használatával határozzák meg, hogy melyik MAP-nak küldjenek üzeneteket.

HMIPv6 használata esetén a mobil eszköz két címmel rendelkezik, egy RCoA-val és egy LCoA címmel. Az RCoA-t állapotmentes módon hozza létre a mobil a MAP opcióban kapott interfész-azonosítóból, és az alhálózati prefixből. A protokoll használatához csak a mobil eszköz implementációjának módosítására van szükség a HA és a kommunikáció partnerének beállításai változatlanok.

Amikor a mobil új domainbe érkezik állapotmentes autokonfigurációt használ az új LCoA létrehozásához. Az RCoA-t is létrehozza a MAP prefixéből a már említett módon. Az RCoA létrehozása után Helyi Binding Update üzenetet küld a MAP-hoz LCoA forráscímmel és RCoA otthoni cím opcióval. Ennek hatására a MAP eltárolja az LCoA-RCoA bejegyzést. A MAP, mint otthoni ügynök, Duplicate Address Detection-t (cím egyediség ellenőrzést) hajt végre a mobil eszköz RCoA címén, és nyugtát küld a BU üzenetre (8. ábra). Ez a nyugta a művelet sikerességét mutatja, ellenkező esetben pedig a megfelelő hibakódot tartalmazza.

A MAP használhatja az OCOT opciót is a nyugtában. Ebben az esetben a mobil eszköznek egy OCOT opciót használó nyugtát kell visszaküldenie a MAP-nak, megnövelve az opció sorszámát eggyel. Az opció segítségével a MAP ellenőrizheti, hogy a mobil eszköz tényleg az általa ismert linken tartózkodik.



8. ábra. A HMIPv6 működése intra-domain kommunikáció esetében

A MAP-nál való regisztrációt követően a mobil eszköznek regisztrálnia kell új RCoA címét az otthoni ügynökénél, egy a megfelelő RCoA-otthoni cím párost tartalmazó Binding Update üzenettel. A Home Address opció tartalmazza az otthoni címet, a forráscím mező, vagy az alternatív-CoA opció, pedig az RCoA-t. A mobil eszköz hasonló BU-t küldhet a kommunikáció partnereinek is. A MAP opció I flag-ének használata esetén a mobil eszköz az RCoA-n kívül más forráscímet is megadhat, P flag használatakor a forráscím csak az RCoA lehet. Amennyiben a mobil eszköz az RCoA-t használja forráscímként, az alternatív CoA opció használata nem szükséges. A mobil alagutazással továbbítja kimenő csomagjait a MAP-nak. A forráscím a külső fejrészben a mobil LCoA címe, a célcím pedig a MAP címe. A mobil eszköznek meg kell várnia a MAP nyugtáját az elküldött BU üzenetre, mielőtt regisztrálná magát az otthoni ügynöknél. A Binding Update-ekben az otthoni ügynököknek és a kommunikációs partnereknek küldött élettartam nem lehet nagyobb, mint a MAP-nál történő regisztráció élettartama. A MAP-ok közötti handover felgyorsítása érdekében a mobil eszköz helyi BU-kat küldhet a korábbi MAP-oknak az új LCoA címével. Ezek után a csomagokat a MAP az új LCoA címre továbbítja majd. A MAP a mobil eszköz otthoni ügynökétől és kommunikációs partnerétől a mobil RCoA címére küldött csomagokat a mobil LCoA címére továbbítja alagutazással. Amikor a mobil eszköz domainen belül mozog új LCoA címét csak a MAP-jánál kell regisztrálnia, az RCoA közben

változatlan. A mobil az RCoA helyett az LCoA-t tartalmazó BU üzenetet küldhet a kommunikációs partnerének, amennyiben egyazon linkhez csatlakoznak. Így a csomagok a kommunikációs partnertől közvetlenül juthatnak el a mobil eszközhöz. A MAP opciót a P illetve I flag beállításával használva a mobil eszköz LCoA címét elrejthetjük a MAP domainen kívül tartózkodók elől. Ilyenkor a mobil eszköz a kommunikációs partnernek és otthoni ügynöknek küldött BU üzenetekben az RCoA címét használja forráscímként. Továbbá a kimenő csomagokban szereplő forráscímnek is az RCoA cím fog szerepelni.

Mobile IPv6 Fast Handovers

A Mobile IPv6 Fast Handovers (FMIPv6) protokoll a handover okozta késleltetés csökkentésének céljából hozták létre. A protokoll csak kiterjesztése a MIPv6-nak, és független az alatta lévő rétegektől. Probléma a MIPv6-ban, hogy lassan történik a hálózatváltás. Ennek lényegében 2 oka van, ez első az IP-rétegű késleltetés (pl. Stateless Autoconf során), a másik a Binding Update késleltetés (hálózatba való bejelentkezés után). Az FMIPv6 ezeken javítva próbálja meg leredukálni a handover okozta csomagvesztést [9].

Azalapötlet az, hogy jó lenne, ha tudnánk, hogy hová megyünk, miközben mozgunk. A protokoll kihasználja azt a lehetőséget, hogy az MN bármikor informálódni tud arról, mely hálózatok vannak a közelében, és így egy adott célhálózathoz előre legenerálhat magának egy CoA-t felkészülvén a váltásra.

- Módosított BU üzenetekkel akár már „távolról” is bejelentkezhet az MN az új hálózatba.
- Az új üzenetekkel funkciókat is összevonhatunk (Neigbor Advertisement és bejelentkezés az új hálózatba)

Az FMIPv6 protokoll által bevezetett új fogalmak

A Mobile IPv6 Fast Handovers (FMIPv6) protokoll lehetővé teszi a MN számára, hogy csomagokat küldjön azonnal, amint észleli, hogy új alhálózathoz kapcsolódik, illetve csomagokat fogadjon, amint az új Access Router érzékeli a MN jelenlétét.

- Previous Access Router (PAR): az MN handover előtti hozzáférési pontja.
- Access Point (AP): az adott IP hálózat hozzáférési pontja. AP-ID: L2-es azonosító.
- New Access Router (NAR) az MN handover utáni, új hozzáférési pontja.
- Previous CoA (PCoA) az MN handover előtti CoA-ja.
- New CoA (NCoA) az MN handover utáni, új CoA-ja.
- Router Solicitation for Proxy Advertisement (RtSolPr) üzenet, amelyben a MN információt kér a potenciális új hálózatokról.
- Proxy Router Advertisement (PrRtAdv) válasz az előbbi kérésre, amely tartalmazza a szükséges információkat az új lehetséges hálózatokról.
- Fast Binding Update (FBU) üzenet az MN-tól a PAR-nak, hogy irányítsa át a neki jövő üzeneteket az új hálózatbeli címére (alagutazással).
- Fast Binding Acknowledgment (FBack) nyugta az előző üzenetre, ezek után a tunnel már működik.
- Fast Neighbor Advertisement (FNA) üzenet, amellyel a MN bejelentkezik az új hálózatába és közli a NAR-ral az NCoA-ját.
- Handover Initiate (HI) üzenet, hogy handovert az Access Routerek is kiválthassanak. Ezt az üzenetet a PAR küldi a NAR-nak, és ezzel inicializálja egy MN handoverét.
- Handover Acknowledge (HAck) nyugta az előzőre, a NAR küldi a PAR-nak.
- (AP-ID, AR-Info) kettős: AR-Info: access routerek L2 és IP címei, valamint a prefix azon az interface-én, amihez az AP (azonosítója: AP-ID) csatlakozik.

A mobil hoszt effektív mobilitása a hálózatváltás realizálását követően, egy új CoA címkonfigurálás elvégzése után, az új hálózatból kifele menő sikeres kommunikációval determinálódik. Annak érdekében, hogy a meglévő kapcsolatai fennmaradjanak, frissítenie kell a HA-nál és a CN-eknél az aktuális helyzetinformációját. A Mobile IPv6 protokoll gondoskodik arról, hogy mindez észrevétlen maradjon a hálózati réteg felett.

Az FMIPv6, ahogy a nevéből is kiderül, a handover gyorsítását célozza meg azáltal, hogy adatkapcsolati szinten segít olyan információkhoz jutni, majd ennek következtében bizonyos akciókat végrehajtani, amik a hálózatváltás idejét csökkentik. A mobil az elérhető alhálózatok felderítésekor az aktuálisan csatlakozott AP-jának információira támaszkodik. Az RtSolPr - PrRtAdv üzenetváltás következtében jut a környező hozzáférési pontok listájának birtokába. A szomszédos hálózatok adatai alapján az MN kiválaszt egyet, és létrehoz magának egy új care-of címet, az NCoA-t. Ezután csatlakozik a NAR linkjére, és a kiküldött FBU-ra kapott FBack válasz megérkezését követően válik képessé ismét csomagfogadásra, illetve csomagküldésre immár az új hálózatban.

A BU késleltetés csökkentését a PCoA és az NCoA közti alagút kiépítése célozza. Küld egy FBU-t a mobil a PAR-nak (lehetőleg az ő linkjéről, vagy a NAR-hoz kapcsolódva egyből). Ez triggereli a korábbi útvonalválasztót a pufferelés elkezdésére és a tunnel létrehozására. Az FBack válasz jelzi, hogy a PAR elkészült az alagúttal, és útnak indítja a mobil eltárolt csomagjait. (Attól függően, hogy melyik linken kapja meg az FBack választ, a protokoll kétféleképpen működik, amit a későbbiek során részletezek.) Az eredmény egy alagút lesz a PAR-tól (PCoA) az MN-ig (NCoA), ami aktív marad mindaddig, míg a CN-ekkel le nem zajlik a BU-váltás. Fordított irányban is működik, tehát az MN-től érkező üzeneteket a PAR forward-olja a kommunikációs partnereinek.

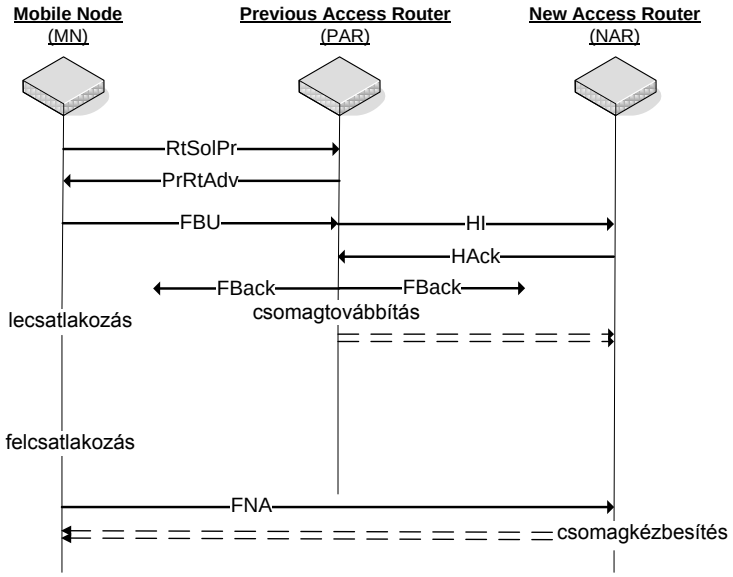
Az új hálózaton a mobil egy FNA üzenettel kezdi hirdetni az NCoA címét. Az üzenet vétele után létrejön egy bejegyzés a NAR-nál az MN-re vonatkozóan. A címütközés elkerülését a protokoll 2 különböző működésű forgatókönyve, más-más fázisban kezeli le, de amennyiben nincs probléma a használni kívánt címmel, a mobil teljes értékű csomóponttá válik az új hálózatában.

Itt természetesen a Neighbor Solicitation és Neighbor Advertisement üzenetváltások alatti késleltetéssel is számolni kellene, de a protokoll az FNA-val küszöböli ki a fontos másodpercek elvesztését.

A handover menete

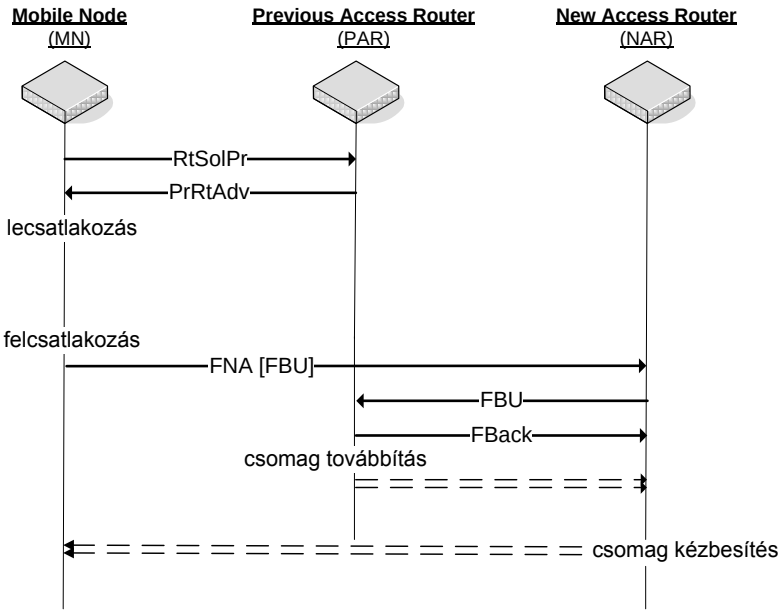
A mobil küld egy RtSolPr kérést a PAR-nak. Válaszul visszakap egy PrRtAdv üzenetet, amelyben a szomszédos hálózatok részletes információi vannak. Ez a válasz tartalmaz egy vagy több [AP-ID, AR-Info] párost. Az MN azután választ egy, a mozgásának, sebességének, stb. megfelelő cél hálózatot. Ehhez a hálózathoz elkészít magának egy NCoA címet, így már készen áll arra, hogy az új hálózatba lépve azonnal kommunikálhasson. A handover megkezdéseként küld egy FBU-t a PAR-nak, aki összeköti a PCoA-t az NCoA-val. A PAR ezek után az NCoA-ra továbbítja a MN csomagjait, és küld egy FBAck nyugtát az MN-nek. Attól függően, hogy melyik linken kapja meg az FBack választ, a protokoll kétféleképp működik [9].

1. "Predictive" Fast Handover, amikor a PAR-nál kap FBack-et (9. ábra)
   - Ebben az esetben az MN megvárja az FBAck-et a PAR-nál.
   - Küld egy FBU-t, ami a címütközéseket megelőzendően tartalmazza az NCoA címet.
   - A hálózatváltást a HI üzenettel inicializálják.
   - A PAR továbbítja az NCoA-t a HI üzenetben a NAR-nak, aki felülvizsgálja azt.
   - Amennyiben a cím ütközik, vagy csak valamilyen policy alapján kapnak a csomópontok címet az új hálózatban, a HAck üzenetben visszaküldésre kerül a használandó cím.
   - A PAR ezt szolgáltatja vissza az FBack-ben a mobilnak.
   - Az MN ezután köteles a javasolt címet felvenni, ha a NAR-hoz át kíván lépni.
   - A tunnelezés ilyenkor folyamatban van a NAR felé történő hívásátadáskor.
   - Végül az FNA üzenettel bejelenti magát a mobil a NAR-nál, és a pufferelt csomagok azonnal érkeznek is hozzá.



9. ábra. Prediktív handover

2. "Reactive" Fast Handover, amikor a NAR-nál kap FBack-et (10. ábra)
   - Ilyenkor az MN rögtön elhagyja a PAR-t a PrRtAdv vétele után, és átmegy NAR-hoz.
   - Ott rögtön FNA üzenettel bejelentkezik.
   - Nem tudhatja, hogy a PAR sikeresen feldolgozta-e azt, ezért az FNA-ban egy FBU is utazik.
   - Ha az NCoA már használatban van, a NAR elveti a belső FBU-t, és olyan Router Advertisement-et küld, amiben elhelyezi a másik címet, elkerülve a duplikációt.
   - Ha már megfelelő az NCoA, akkor a NAR továbbítja a FBU-t a PAR-nak.
   - A PAR végül FBAck üzenettel nyugtázza a hálózatváltást.



10. ábra. Reaktív handover

Network Mobility (NEMO) Basic Support Protocol

Mobil hálózat (Mobile Network, MNet) egy olyan hálózati szegmens vagy alhálózat, amely képes mozogni és változtatni a hálózathoz való kapcsolódási pontját. A mozgó hálózat egy meghatározott gateway-en (átjárón) keresztül érhető el. Ezt az átjárót Mobile Router-nek (MR) nevezzük (11. ábra). A MR kezeli le tulajdonképpen a MNet mozgását. A mobil hálózatokkal és a hozzájuk kapcsolódó problémákkal többek között az IETF NEMO (NEtwork MObility) csoportja foglalkozik 2002 óta. Az általuk kidolgozott NEMO Basic Support megoldás [10] hasonló elveken alapul, mint a Mobile IPv6, vagyis amikor csak egyedülálló hosztok mozognak a (nem mozgó) hálózaton belül. A NEMO BS azonban nem az egyes hosztok mozgásával kapcsolatos megoldásokra, hanem hálózatok, mint hosztok halmazának mobilitására dolgozta ki a NEMO Basic Support-ot.

Az alapgondolat az, hogy minden egyes MR-hez tartozik egy Home Agent és köztük kétirányú (bidirectional) tunneling épül ki annak érdekében, hogy a folyamatban lévő kapcsolatok szakadatlanságát biztosítani lehessen. Ez a kétirányú alagút a mozgó hálózat egységei számára transzparens. A MR a MIPv6-nál megismert MN-hez hasonlóan viselkedik. Van egy otthoni címe (Home Address), illetve egy ideiglenes címe (abban az esetben, ha nem az otthoni hálózatban van).

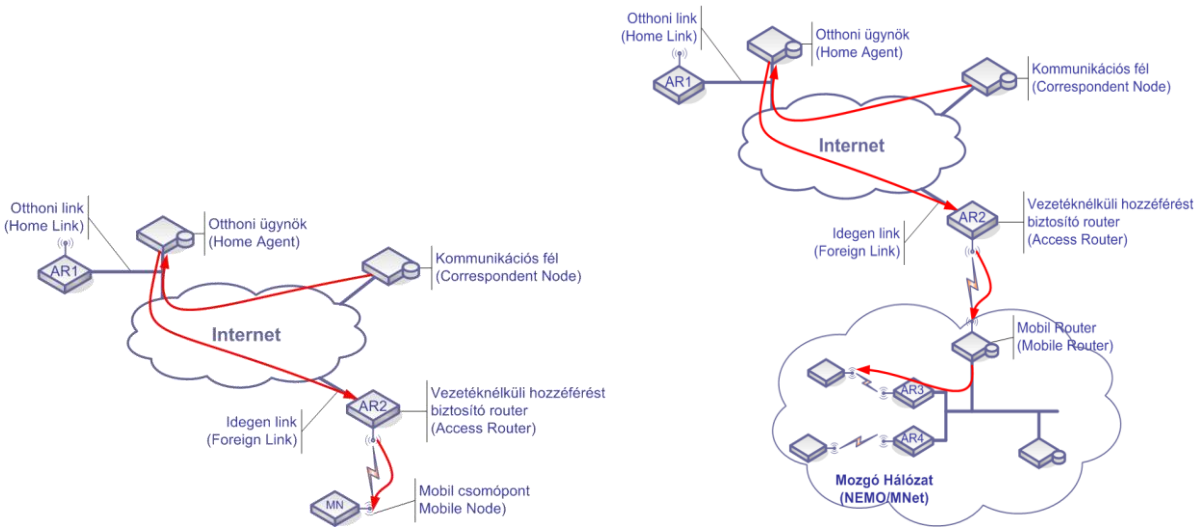
A protokoll lehetővé teszi egymásba ágyazott mobil hálózatok kialakulását (Nested MNet). Ebben az esetben a mobil hálózat valamely eleméhez egy másik MR csatlakozik. Ilyen egymásba ágyazott hálózatokból több szint is kialakulhat. Ez azonban nem túl előnyös, mivel minden egyes újabb szint megnöveli az overheadet, ugyanis a csomagok minden szinten újra becsomagolásra kerülnek.

Különbségek a MIPv6-hoz képest

A MR viselkedhet normál Mobile Node-ként vagy Mobile Router-ként. Ha úgy dönt, hogy MR-ként fog viselkedni, akkor a HA-nak küldött BU üzenetben ezt jeleznie kell. Azzal tudja ezt megtenni, hogy az R flaget beállítja a BU üzenetben. A MR által a MNet-ben hirdetett prefixet Mobile Node Prefixnek (MNP) nevezzük. Egy MR természetesen több MNP-t is hirdethet ugyanazon MNet-ben. A BU üzenetben a MR-nek az MNP-re vonatkozó információkat is közölnie kell a HA-val, azért hogy a HA továbbítani tudja a csomagokat a mozgó hálózatba. A MNP információt egy új Mobility Header Option-ben kell elhelyezni. Ha a MR nem csak egy, hanem több MNP-t is hirdet a mozgó hálózatban, és szeretné, ha a HA minden prefixről tudna, akkor mindegyik prefixet el kell helyeznie a BU üzenetben. Egy BU üzenetben több MNP is elhelyezhető. A HA, amikor olyan csomagot kap, amelyiknek a célja a MNet-ben van, a csomagot a MR felé fogja továbbítani.

A HA, mint mindig, BA üzenettel fogadja el a BU üzenetet. Pozitív BA esetén a BA üzenetben be kell állítani a R flaget. A pozitív visszajelzés azt jelenti, hogy a HA beállította a továbbítást a MNet felé. A kötés befejezéseként kiépül a kétirányú alagút a MR és a HA között. A mobil hálózatból érkező csomagokat a MR becsomagolja, majd a HA felé továbbítja. A saját maga által küldött csomagokat a MR küldheti az alagúton keresztül vagy közvetlenül a kommunikációs partnernek, ha az képes a routing optimalizációra. A mobil hálózatba irányuló csomagokat a HA elfogja, becsomagolja és az alagúton keresztül továbbítja a MR aktuális CoA-jára, vagy az otthoni címére, ha a MR az otthoni hálózatában van. A MR kicsomagolja a csomagot, majd továbbítja a MNet-be. Ha a csomagok nincsenek védve egyéb mechanizmussal (pl. IPsec), akkor a MR a kicsomagolás előtt ellenőrzi, hogy a csomag forrás cím mezőjében a HA címe található-e, illetve azt is ellenőrzi a MR, hogy a csomag cél címe a mobil hálózatban van-e, amennyiben nem úgy a csomagot a MR eldobja.

A mobil hálózatban lévő csomópontok szintén lehetnek mobilak, vagy lehetnek fixek, és persze egy MNet-ben lévő mozgó egység lehet akár Mobile Router is.



11. ábra. Hoszt mobilitás és hálózat mobilitás

A MR működése

Tulajdonképpen a MR funkcionalitását tekintve nem más, mint egy mozgó egység és egy router ötvözése. Egy MR kétféleképpen működhet. Egyrészt viselkedhet mozgó hosztként (mobile host): a HA ekkor nem tárol semmilyen, az MR-hez tartozó, prefixszel kapcsolatos információt, viszont tárol egy - a MR Home Address-éhez rendelt - Binding Cache-t. Másrészt MR-ként viselkedhet. A HA ez utóbbi esetben is kezel Binding Cache-t, azonban ezen felül tárolja az üzenettovábbításhoz szükséges hálózati prefix-információkat is. A kétféle működés megkülönböztetésére szolgál a korábbiakban már ismertetett R jelzőbit a BU üzenetben.

Az MR-ben megtalálható a Binding Update List, ami a Binding Update üzenetekkel kapcsolatos információkat tartalmazza. Néhány új bejegyzéssel is ki van egészítve a MIPv6-hoz képest a lista. Az egyik a „Prefix információs mező”, ami a MNP opcióval kapcsolatos információkat tartalmazza; a másik új bejegyzésben az „R” jelzőbit értékét is tárolja a MR valamennyi Binding Update-hez.

A BU üzenet küldésének két módja van. Az egyiknek kötelezően implementálva kell lennie. A két módszer az implicit, illetve az explicit módszer. Implicit esetben a MR nem egészíti ki a BU üzenetet MNP opcióval. A HA ekkor tetszőleges módszert alkalmazhat a MR-hez tartozó MNP-k meghatározásához (pl.: kézi konfigurálás). Explicit esetben a BU üzenetben a MR elhelyezi a MNP-kre vonatkozó információkat.

A MR az általa küldött BU üzenetekre válaszként BA üzenetet kap a HA-tól. Ha a kapott BA üzenetben a HA azt jelzi, hogy elfogadta a BU üzenetet, és az R jelzőbit értéke 1, akkor az MR úgy vélekedik, hogy a HA készen áll az üzenetek továbbítására az adott MNet felé. Ha az R bit értéke 0, akkor viszont a MR újabb, olyan HA-k után fog keresni, amelyek támogatják a MR-eket. Természetesen a MR-nek először egy de-regisztrálási folyamatot kell végrehajtania az aktuális HA-val, mielőtt egy újjal venné fel a kapcsolatot. A sikeres BU folyamat után kialakul a kétirányú alagút a MR és a HA között.

A HA működése

A HA binding cache-e a MIPv6-hoz képest ki van egészítve a MNP-kre vonatkozó információkkal, valamint az R bit értékét feldolgozó algoritmussal. A HA emellett tárol még egy úgynevezett Prefix táblázatot. Ez elsősorban biztonsági funkciót lát el. Abban az esetben, ha egy MR illetéktelenül, vagy meghibásodás végett másik MR-hez tartozó hálózati prefixet küld a Binding Update-ben. A HA – megnézve a bejegyzéseket – detektálhatja a hibát, vagy a támadást. A táblázat két mezőből áll, a MR otthoni címéből, amely a MR-t azonosítja, illetve egy MNP mezőből.

A HA, amikor BU üzenetet kap, először megvizsgálja, majd ha nem utasítja el a BU üzenetet, akkor feldolgozza azt és a benne található MNP opciókat. A BU üzenetben található MNP-ket eltárolja a binding cache-ében és a Prefix táblázatban. Ha egynél több MNP van a BU üzenetben,

akkor a HA-nak minden prefixre ki kell alakítania a csomagtovábbítási mechanizmust. Amennyiben akár csak egy prefixre nem sikerül ez, a HA-nak el kell utasítania a BU üzenetet.

A HA a mozgó hálózatba irányuló csomagokat a kétirányú alagút segítségével továbbítja a MR-hez. Amikor egy MR de-regisztrálja a MNP-ket a HA-nál, akkor a HA kitörli a kérdéses MR-re vonatkozó információkat a binding cache-ből, majd lebontja az adott MR-rel kiépült alagutat és abbahagyja a csomagok továbbítását a MR felé.

DHAAD módosítások

A DHAAD mechanizmus kiterjesztése szükséges azért, hogy a MR-ek csak olyan HA-nál próbálják meg a regisztrációt, akik támogatják azt, hogy egy hoszt MR-ként viselkedjen. A DHAAD request üzenetben szintén elhelyezhető az R flag. A MR akkor állítja be ezt a bitet, ha jelezni akarja, hogy csak olyan HA-kat keres, akik támogatják a Mobile Routereket. A DHAAD reply üzenetben szintén elhelyezhető az R flag. Ha a HA olyan DHAAD kérést kap, amelyben az R flag be van állítva, akkor a válaszban el kell küldenie azoknak a HA-knak a listáját, amelyek támogatják a MR-eket. Amennyiben legalább egy ilyen HA van, akkor a DHAAD reply-ban be kell állítani az R flaget. Előfordulhat az is, hogy nincs olyan HA, amely támogatja a MR-eket, akkor azon HA-knak a listáját kell visszaküldeni a válaszban, akik a normál MIPv6-ot támogatják. Ez utóbbi esetben az R bitet nem kell beállítani.

Hivatkozások

[1] D. Saha, A. Mukherjee, I. S. Misra és M. Chakraborty, „Mobility Support in IP: A Survey of Related Protocols,” in *IEEE Network*, 2004.

[2] I. F. Akyildiz, J. Xie és S. Mohanty, „A Survey of Mobility Management in Next-Generation All-IP-Based Wireless Systems,” *IEEE Wireless Communications*, pp. 16-28, 2004.

[3] P. Reinbold és O. Bonaventure, „IP Micro-Mobility Protocols,” *IEEE Communications Surveys & Tutorials*, pp. 40-57, 2003.

[4] C. Perkins, D. Johnson és J. Arkko, „Mobility Support in IPv6,” IETF RFC 6275, 2011.

[5] C. Perkins, „IP Mobility Support for IPv4, Revised,” IETF RFC 5944, 2010.

[6] T. Narten, E. Nordmark, W. Simpson és H. Soliman, „Neighbor Discovery for IP version 6 (IPv6),” IETF RFC 4861, 2007.

[7] D. Johnson és S. Deering, „Reserved IPv6 Subnet Anycast Addresses,” IETF RFC 2526, 1999.

[8] H. Soliman, C. Castelluccia, K. E. Elmalki és L. Bellier, „Hierarchical Mobile IPv6 Mobility Management (HMIPv6),” IETF RFC 5380, 2008.

[9] R. Koodli, „Mobile IPv6 Fast Handovers,” IETF RFC 5568, 2009.

[10] V. Devarapalli, R. Wakikawa, A. Petrescu és P. Thubert, „Network Mobility (NEMO) Basic Support Protocol,” 2005.