BUDAPESTI MŰSZAKI ÉS GAZDASÁGTUDOMÁNYI EGYETEM
VILLAMOSMÉRNÖKI ÉS INFORMATIKAI KAR

Hálózati Rendszerek és Szolgáltatások Tanszék

SPECIÁLIS PROTOKOLLOK ÉS ALGORITMUSOK AZ IP VILÁG KOMPLEX MOBILITÁSI FORGATÓKÖNYVEINEK TÁMOGATÁSÁRA

Bokor László

Ph.D. disszertáció tézisfüzet

Tudományos témavezető:
Dr. Imre Sándor, Sc.D.
Dr. Jeney Gábor, Ph.D.

BUDAPEST, 2014

1. Bevezetés

Napjainkban a telekommunikációs rendszerek különböző vezetékes és vezeték nélküli technológiák szinergikus egységévé formálódnak, melyekben Internet Protocol (IP) alapon futnak az integrált multimédia szolgáltatások [J1], [C7]. Az Internet egy teljesen átlátható és mindenütt jelenlévő multimédia kommunikációs rendszerré válik, melyben a felhasználók a távoli erőforrásokat bárhol és bármikor elérhetik [C8]. Ez az evolúció tette a mobil Internetet a felhasználók és az operátorok számára egyaránt valósággá, javarészt az okostelefonok új generációinak, a 3G/4G modemmel felszerelt hordozható számítógépeknek és a vonzó üzleti modelleknek köszönhetően. Az aktuális trendek és gyártói előrejelzések alapján kijelenthető, hogy a 2020-ig előttünk álló időszak a csomagkapcsolt mobil hálózatok forgalmának robbanásszerű növekedését fogja hozni [1].

A várt forgalmi igények és felhasználói követelmények kielégítéséhez, a speciális használati esetek és komplex forgatókönyvek támogatásához a felhordó (backhaul) és maghálózati technológiáknak is fejlődniük kell. Ezen technológiákon belül kiemelkedő szereppel bírnak a mobilitás-kezelési protokollok és algoritmusok, melyek a jövő mobil Internének kulcsszereplői [J9].

A hagyományos IP mobilitás-kezelés (pl. Mobile IPv6 [2]) képes a mozgás közbeni folyamatos kapcsolat és globális hálózatváltás-kezelés transzparens biztosítására akár heterogén rádiós környezetekben egyaránt, ám különböző teljesítménybeli problémákat (megnövekedett késleltetés, csomagvesztés, jelzésterhelés) is beépít az architektúrába. A hibák kiküszöbölésének igénye vezetett a makro- és mikro-mobilitás forgatókönyveinek megkülönböztetéséhez. A makro-mobilitási protokollok az Internet távoli vezeték nélküli tartományait hivatottak átlátszó módon összekötni [2], [C16], [J4], míg a mikro-mobilitási megoldások (pl. HMIPv6 [3]) helyi, lokalizált körülményekre optimalizáltak, a mozgás okozta jelzési feladatokat nem engedik a tartományon kívülre, így csökkentik a mobilitás-kezelésben érintett csomópontok számát, a jelzésterhelést és a jelzési késleltetést. Skálázhatóságuk és teljesítményük kapóra jön napjaink problémáinak megoldásában, így ezen technikák fejlesztése, optimalizálása, integrálása a reneszánszát éli. A mikro-mobilitási tartományok optimális tervezése szintén fontos kérdéskör, ami főleg ezen protokollok újgenerációs mobil hálózatokban történő telepítésekor jelentkezik.

Az is látható, hogy a közeljövőben az IP alapú mobil és vezeték-nélküli hálózatokban nem csak az önálló végberendezések (táblagépek, okostelefonok, stb.) lesznek résztvevők, hanem a személyi hálózatok (Personal Area Network – PAN), a gépjármű-hálózatok (Vehicle Area Network – VAN), a szenzorhálózatok, valamint az intelligens szállítórendszerek és kooperatív változataik (Intelligent Transportation System – ITS, Cooperative ITS – C-ITS) is egyaránt fontos szerephez jutnak majd [C5], [C10], [C15]. Ez azt jelenti, hogy egész mozgó hálózatok (un. NEMO-k) mobilitás-kezeléséről is gondoskodni kell. A jelenleg szabványosított NEMO Basic Support (BS) protokoll [4] azonban csak alapmegoldás, így a további optimalizáció jelentős feladatot hárít a kutatókra.

A növekvő felhasználószám és forgalom súlyos problémaként nehezedik a jelenlegi IETF és 3GPP szabványokon alapuló mobil Internet architektúrákra. Az erősen centralizált felépítés miatt a vég-vég minőség biztosítása (QoS) már nem oldható meg költséghatékonyan, az operátorok a gyártókkal karöltve keresik a kiutat. A mikro-mobilitási megoldások ígéretesek ugyan, de jellegükből fakadóan nem vezetnek a probléma gyökeréig, ami az architektúra központosított és centralizált természetében keresendő. A skálázhatósági problémákat architektúrális szempontból kell megközelíteni, így az elosztott [J11] és kisimított (flat) [5] mobil architektúrák, proaktív és cross-layer optimalizált technikák (pl. [C23], [C30]) egyre nagyobb figyelmet kapnak.

Bár az IPv6 alapú technológiák az újgenerációs IP protokoll terjedésével fontos szerepet játszanak majd a fent vázolt kérdéskör megoldásában, várható, hogy az IP címek szemantikai túlterheltségét könnyíteni célzó egyéb megközelítések (vagyis a helymeghatározó és állomásazonosító funkciók szétválasztásával foglalkozó „ID/Loc separation” sémák) is egyre jelentősebbé válnak a közeljövőben [6]. A Host Identity Protocol (HIP) család tagjai [7]–[10] jelenleg a legígéretesebbek, így disszertációmban HIP és tisztán IPv6 alapú megoldásokkal egyaránt igyekszem a bemutatott speciális mobilitási forgatókönyvek és használati esetek támogatásához hozzájárulni.

2. Kutatási célkitűzések

A bevezetésben röviden vázolt trendek és komplex felhasználási esetek komoly kihívást jelentenek napjaink mobil Internet architektúrái számára, ha hatékony megoldást kívánunk nyújtani a problémákra. Kutatásaim legfontosabb célja olyan speciális protokollok és sémák kidolgozása volt, melyek a fenti mobilitási forgatókönyvek támogatására szolgálnak megoldásul az IP alapú (all-IP) világban. Új mobilitás-kezelési technikák kifejlesztésével, lokalizált mobilitás-menedzsment megoldások kidolgozásával, mikro-mobilitási tartományok tervezési kérdéseinek tárgyalásával és proaktív, rétegek közti (cross-layer) optimalizálásra támaszkodó hálózatváltási sémák bevezetésével célom volt a skálázhatóság növelése, az IP tartományok közötti észrevehetetlen (seamless) mozgás támogatása, így végső soron a jobb felhasználói minőség (Quality of Service – QoS, Quality of Experience – QoE) támogatása, és a felhasználók privát szférájának erősítése. Munkámat négy nagyobb témakörbe csoportosítottam:

1. A makro-mobilitási protokollok javítását, skálázhatóságuk és teljesítményük növelését két megközelítést használva kívántam elérni. Egyrészről a Mobile IPv6 (MIPv6) kiegészítése volt a célom, egy lehetőleg teljesen transzparens, kizárólag IPv6 alapú, új technikára támaszkodó mikro-mobilitási keretrendszer kidolgozásával, mely nem kíván kiegészítő hálózati elemeket, decentralizáltan működik, és optimális utakat biztosít a tartományon belül is anélkül, hogy extra jelzési terhelést vinne a vezeték nélküli interfészre (I.1 tézis). Ennek a megközelítésnek része volt egy, kifejezetten ehhez a keretrendszerhez kialakított mikro-mobilitási tartomány tervező („subnet forming") algoritmus kidolgozása is (I.2 tézis). Másrészről célul tűztem ki a mikro-mobilitás támogatásának bevezetését a Host Identity Protocol alapú jövő Internet rendszerek számára, egy új, HIP alapú mikro-mobilitási protokoll kidolgozásával és teljesítményelemzésével (I.3 tézis). Ezen munkámban kiemelkedő szerepet kapott a HIP speciális, kriptografikus ID/Loc szeparációs képességeinek a lokalizált mobilitás-kezelés érdekében történő kihasználása.

2. A mobil Internet mindennapjainkba való folyamatos beszűrődésével egyre nagyobb figyelmet kap a felhasználók helyzetinformációnak védelme, a felhasználók privát szférájának biztosítása. Az IP világban történő mobilitás-kezelés során a felhasználó aktuális, és mozgása során sokszor változó IP címe könnyedén átváltható precíz földrajzi pozícióadatokra. A II.1, II.2, II.3, és II.4 téziseimmel célom volt a felhasználók helyzetinformációnak védelmét támogató mikro-mobilitási tartomány tervező algoritmusok kifejlesztése, melyek segítségével a privát szféra védelmének egyre jelentősebb igényét már a hálózat tervezésekor figyelembe tudjuk venni. A létező hálózattervező algoritmusok (pl. [11]–[13]) főleg a regisztrációs és paging költségeket veszik alapul; legjobb tudomásom szerint az én munkám előtt mások nem fordítottak még figyelmet az IP szintű helyzetinformáció-védelem hálózattervezés során történő támogatására.

3. A mozgó hálózatok mobilitás-kezelését alapszinten megvalósító NEMO BS protokoll [4] megoldja a legfontosabb feladatokat, ám a megoldás jelentős jelzési terhelést, szuboptimális útvonalakat és Mobile IPv6 szintű jelzési késleltetést hoz a rendszerbe, nem támogatja a többotthonúságot (multihoming) és a több rádiós hozzáférés egyidejű támogatását (multi-access). Ezen kérdéseket már jó ideje vizsgálja az IETF, de a munka még nem került befejezésre annak ellenére sem, hogy létezik multihoming [14], útvonal-optimalizációs [15], és hálózatváltási teljesítményt javító [17] kiegészítés is NEMO BS-hez. Több valós rendszeren végrehajtott demonstráció [C10] és kialakított tesztrendszer [C5] bizonyítja a NEMO BS és kiegészítéseinek hatékonyságát, ám a további optimalizáció és az új utak keresése (pl. [18]) még mindig lázban tartja a kutatókat. A NEMO sémák továbbfejlesztésekor két megközelítéssel éltem. Egyrészt célom volt a szabványos, IPv6 alapú hálózat-mobilitási protokollok javítása, melyhez egy egyedi, folyamatos hálózatmonitorozást és rétegek közti optimalizálást használó keretrendszert és speciális hálózatváltási sémát alakítottam ki (III.1 és III.2 tézisek). Másrészt célul tűztem ki a mozgó hálózatok Host Identity Protocol rétegében való támogatásának biztosítását, így létrehoztam egy új, HIP-alapú NEMO protokollt melynek szimulációk segítségével végeztem el teljesítményelemzését (III.3 tézis).

4. A jelenlegi erősen centralizált mobil Internet architektúrák nem skálázhatók az előre jelzett forgalmi növekménnyel, nem lesznek képesek kezelni a kihívásokat [19], [J9]. A skálázhatóság javítását célozva az első javaslatok egyikeként hozták létre az Ultra Flat Architecture (UFA) nevű rendszert [5], mely hatékonyan támogatja az elosztott mobilitás-kezelést, és decentralizált, önkonfiguráló és önoptimalizáló sémákat vonultat fel a megoldás érdekében. Az UFA jellemzője, hogy a hálózatváltásokat az alkalmazási rétegben, Session Initiation Protocol (SIP) használatával kezeli. A SIP igen hatékony megközelítés, azonban nem transzparens, nem támogatja a non-SIP (vagyis hagyományos Internet) alkalmazásokat, és a SIP-alapú UFA nem kompatibilis az ITU-T jövő mobil Internet architektúrákra vonatkozó, ID/Loc elkülönítésre tett ajánlásaival sem [6]. Éppen ezért tűztem ki célul egy Host Identity Protocol alapú UFA keretrendszer kidolgozását (IV.1 tézis), valamit az architektúra szerves részét képző, proaktív, elosztott hálózatváltás-kezelő protokoll tervezését és teljesítmény-vizsgálatát. A javasolt keretrendszer előkészíti, és HIP-et használva végre is hajtja a hálózatváltásokat, eltűnteti az architektúrából a központosított IP horgonypontokat (anchor nodes), és a hálózati funkciókat a hozzáférési hálózat szélére tolja ki, a felhasználók közvetlen közelébe (IV.2 és IV.3 tézisek).

3. Kutatási módszertan

Disszertációmban két klasszikus módszertant követtem: analitikus és szimulációs modelleket használtam javaslataim vizsgálatára.

A komplex mobilitási forgatókönyvekben azonosított problémák megoldásához tervezett új protokollok, sémák vagy algoritmusok kialakításakor az analitikus megközelítés nem hagyható figyelmen kívül. Az I. és II. téziscsoportokban dokumentált hálózattervező megoldások gráf-modelleken, speciális költség-struktúrákon és algoritmuselméleti alapokon (pl. szimulált lehűtés) nyugszanak, míg a III. téziscsoportban leírt NEMO optimalizációs keretrendszer vizsgálatához kialakított analitikus modell a valószínűségszámítás elméletének eredményeit használja fel.

Javaslataim vizsgálatához két különböző szimulációs környezetet is felhasználtam. Egyrészt módosítottam és kiegészítettem egy egyedi, Java alapú mobilitás-szimulátort [20], [J3], mely képes valószerű cellaváltások (cella-közti mozgásráta információk) és bejövő hívás-adatbázisok generálására egy adott (mikro)mobilitási rendszerben, és ezen információkat felhasználva különböző hálózattervező mechanizmusokat is le tud futtatni. A szimulátor valószerű mozgásminták kialakítására képes, és felkészítettem az algoritmusaim különböző bemeneti tartomány-struktúrákon történő végrehajtására (I. és II. téziscsoportok).

Másrészről módosítottam és kiegészítettem az OMNeT++ nevű [21], általános célú, nyílt forráskódú, komponens-alapú, diszkrét idejű, eseményvezérelt szimulációs rendszerhez készült, Internet-technológiákat részleteiben modellező INET csomagot, és felkészítettem saját protokolljavaslataim futtatására és széleskörű vizsgálatára. Az I. III. és IV. téziscsoportjaim egyes eredményei ezen a kiterjesztett képességű rendszeren [C17] végrehajtott kiterjedt szimulációs vizsgálatok segítségével születtek.

A matematikai statisztika és a valószínűségszámítás elméletét a szimulációs eredmények analízisekor is használtam, hiszen a nagymennyiségű mérési eredmény feldolgozása igényelte ezt a matematikai hátteret.

4. Új tudományos eredmények

4.1. Mikro-mobilitási protokollok

A különböző rádiós technológiákat heterogén hozzáférési rendszerekbe tömörítő mobil és vezeték nélküli architektúrákban az egyes hozzáférések közti átjárást az Internet Protocol v4 és/vagy v6 változataira épülő sémák egységes all-IP platformon oldják meg [J5], [B6]. A Mobile IPv6 [2] és makro-mobilitási társai kiválóak a globális mobilitás-kezelésre, de rosszul skálázhatók, jelentős jelzésterheléssel és jelzési késleltetéssel járnak, különösen, ha a felhasználó az Internet hozzáférési pontját (Internet Point of Attachment – PoA) gyakran változtatja egy adott, jól körülhatárolható földrajzi területen (un. mikro-mobilitási tartományon) belül. Ezen problémák kiküszöbölésére hozták létre a különböző mikro-mobilitási protokollokat (pl. [3]). A létező mechanizmusok mindegyike szenved valamilyen járulékos hibától: robusztusság hiánya, jelentős komplexitás-növekedés, stb., és gyakran telepítési nehézségekbe ütköznek az operátorok is, mivel nemegyszer új protokollok rendszerét kell integrálni meglévő hálózatokba.

A makro-mobilitási protokollok hálózatváltási teljesítményének javítását célozva egy kizárólag IPv6 alapú (I.1 és I.2 tézisek), valamint egy HIP alapú megközelítést (I.3 tézis) követtem.

A tisztán IPv6 alapú javaslatom fő célja az IPv6 anycasting [22] adástípusával kapcsolatos eredmények kiaknázása, és a mobilitás-kezelésben való részvétele által egy újabb alkalmazási terület bevezetése volt [J10]. Megoldásomban IPv6 anycast címek azonosítják a mikro-mobilitási területben érkező mobil végberendezéseket, és anycast csoportmenedzsment protokollok [23] végzik el a területre belépő csomópontok regisztrációját. A helyzetinformációk frissítése és a hálózatváltás kezelése az anycast alhálózat (anycast subnet) által meghatározott mikro-mobilitási területen belül (intra-domain esetekben) a domain-ben futó anycast routing protokoll (pl. [24]) segítségével történik, ami az optimális intra-domain utakat is biztosítja. Az inter-domain (vagyis makro-mobilitási) eseteket a Mobile IPv6 transzparensen kezeli.

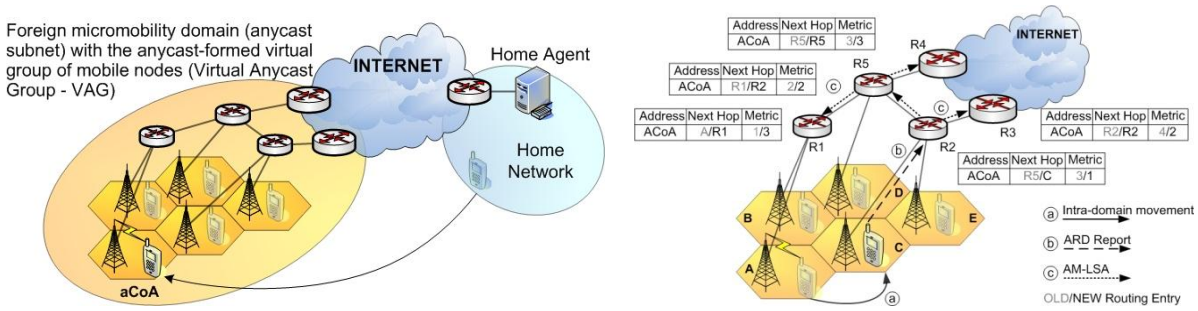
I.1. Tézis [C1],[C2],[C3],[B1] *Kidolgoztam egy anycast alapú mikro-mobilitási keretrendszert (ABMF), mely teljesen decentralizált működésével, valamint a mikro-mobilitási területen belüli optimális útvonalvezetéssel biztosít hatékony lokalizált mobilitás-kezelést anélkül, hogy extra jelzésüzenetekkel terhelné a vezeték nélküli interfészt.*

Az Anycast Based Mobility Framework (ABMF) működésekor, ha egy mobil belép egy mikro-mobilitási tartományba, akkor az ott szerzett ideiglenes címe (Care-of-Address – CoA) egy egyedi anycast cím lesz (aCoA), melyről a mobil automatikusan tájékoztatja MIPv6 otthoni ügynökét, és mely címet a domain-en belül nem kell többé módosítania. A hozzárendelt aCoA cím érvényességi köre (region) az un. Anycast Subnet (AS) nem más, mint a mikro-mobilitási terület, melyet a P prefix és a scope definiál.

A mikro-mobilitási területre lépő mobil csomópont egy virtuális anycast csoport tagjává válik (Virtual Anycast Group – VAG), ahol a VAG a mobil csomópont virtuális (lehetséges) tartományon belüli helyeit jelenti (1. ábra). A tartományban működő anycast routing protokoll feladata megtalálni egy VAG tag aktuális helyét, azaz közvetíteni a tőle származó és felé haladó csomagokat. Ennek eredményeként a tartomány elfedi a belső mozgást, csökkenti a MIPv6 terhelést és a hálózatváltások okozta késleltetést.

Természetesen az ABMF lényeges eleme a használt anycast routing protokoll, mely még nem került szabványosításra, ám ha ez megtörténik, akkor a javasolt módszer csak és kizárólag transzparens IPv6 megoldásokkal biztosítja a hatékony lokális mobilitás-kezelést. Az ABMF kialakítása és működésének definiálása két, még fejlesztés alatt álló anycast routing protokoll esetére is megtörtént (Anycast Extension to OSPFv3 [C9] és ARIP [C3]).

Mint minden hop-by-hop mikro-mobilitási megoldás esetén, úgy az általam javasolt ABMF-ben is probléma a domainen belüli routing táblák méretének felrobbanása, hiszen a mobilok eléréséhez elkülönített, egyedi bejegyzések szükségesek. A routing tartomány méretének kontroll alatt tartása érdekében, és az ABMF skálázhatóságának biztosítását célzandó javasoltam egy speciális anycast subnet tervező algoritmust, mely képes a paging és a regisztrációs költségek figyelembevételére is.



1. ábra: Anycast-based Mobility Framework (balra) és az AOSPFv3 használata ABMF tartományban (jobbra)

I.2. Tézis [C9], [C12], [J3] *Létrehoztam egy kétfázisú anycast subnet (AS) tervező algoritmust, mely először egy mohó csoportosítással hozza létre a vezeték nélküli hozzáférési pontok kiindulási partícióit, amiből szimulált lehűtéssel állnak elő a végleges AS partíciók. Megmutattam, hogy a javasolt kétfázisú Simulated Annealing Based Anycast Subnet Forming (SABAS) algoritmus, mely a SABLAF séma továbbfejlesztése, átlagosan 35%-kal csökkenti a regisztrációs költséget, miközben figyelembe veszi skálázhatóság jelentette korlátokat is.*

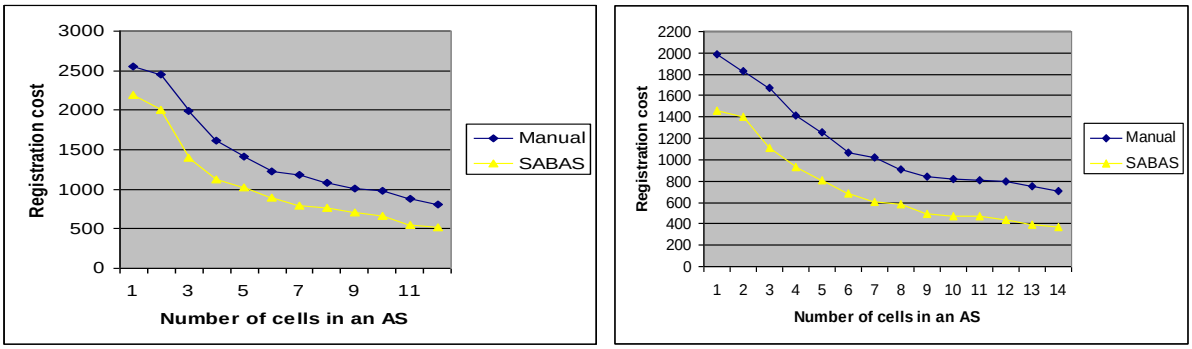
Az ABMF keretrendszerben minden AS határátlépésnél a mobil csomópont MIPv6 üzenetekkel regisztrálja új helyzetét az otthoni ügynökénél. Ez a regisztrációs költség. A paging költség akkor jelentkezik, mikor a mikro-mobilitási területen belül lévő, inaktív mobil terminál pontos helyét kell megtalálni a bejövő csomagok útvonalirányítása érdekében. Érthető módon ez a két költség egymással ellentétes mikro-mobilitási tartomány tervező követelményeket támaszt: a paging költség csökkentéséhez kisméretű tartományokat, míg a regisztrációs költség csökkentéséhez nagyméretű tartományokat kívánna a rendszer. Adott tehát a kérdés: mekkora méretű legyen az anycast subnet, ha a paging és regisztrációs költségeket egyaránt figyelembe kívánjuk venni, és a virtuális anycast csoportokat host bejegyzésekkel kezelő routing táblák maximális mérete is kordában legyen tartva.

Ennek érdekében a paging költséget és a routing táblák maximális méretét korlátként definiáltam, így a regisztrációs költség minimalizálása vált az egyedüli célfüggvénnyé. Az így formalizált probléma tehát az AS-ekbe csoportosítandó PoA-k optimális számának meghatározása úgy, hogy a regisztrációs költség minimális legyen a kényszerparaméterek mellett. A probléma hasonló a Location Area tervezéshez [13], ezért az ott is használt folyadék-modellt használtam a mobil csomópontok (Mobile Node – MN) AS-ek közti mozgásának leírásához, támaszkodtam a [25]-ben használt MIPv6 regisztrációs és paging költségformulákra, valamint a [20]-ban az $N_{\max}$ (az AS-be rakható PoA-k lehetséges maximális száma) kiszámításához bevezetett egyenletre. Mindez, valamint a PoA párok közti MN átmenetek, azaz hálózatváltási ráták (handover rate) adatbázisa nyújtja a SABAS algoritmusom bemenetét.

A SABAS mohó fázisa először kiválasztja a legnagyobb hálózatváltási rátával rendelkező PoA párt a bemenetként kapott adatbázisból ($q_{\max}$) és ezt a két PoA-t berakja az AS_1 halmazba. A következő lépésben a második legnagyobb hálózatváltási rátához tartozó PoA pár azon eleme kerül a halmazba, mely másik eleme már az AS_1 tagja volt. Az algoritmus ellenőrzi, hogy az $N_k < N_{\max}$ egyenlőtlenség teljesül-e (ahol az $N_{\max}$ az N_k maximuma, vagyis az a maximális PoA szám, melyre az AS minimális regisztrációs költséggel bír. Ha az egyenlőtlenség igaz, akkor az új PoA az AS_1 elemévé válik. Ezekkel a lépésekkel eljutunk egy olyan AS struktúrához, mely a mohó megközelítés miatt nem lesz optimális. Ez viszont nem gond, mert ez az AS struktúra képzi a szimulált lehűtéssel operáló második fázis bemenetét: ez a kiindulási partíció (s_0), és ebből, véletlen lépésekkel készül a következő – szomszédos – megoldás (s_1), aminek kiszámoljuk a regisztrációs költségét, és összehasonlítjuk a korábbi megoldáséval ($\Delta C_{Reg}(s_0, s_1)$). Ha javítottunk a helyzeten, akkor s_1 lesz a következő állapotunk, ebből készítjük a következő megoldást. Ha az eredmény romlott, akkor

$e^{\left(-\frac{\Delta C_{Reg}}{T}\right)}$ valószínűséggel fogadjuk el az új, s_1 megoldást a régi helyett (ahol T a hőmérséklet, melyet folyamatosan csökkentünk, így a lehűtés kezdetén (magas hőmérsékletnél) még viszonylag nagy valószínűséggel haladhatunk rossz irányba is). Ha a T eléri a nullát, vagy a ΔC_{Reg} nem változik, megállunk. Egy másik korlátot is bevezettem, ez pedig az AS-be engedhető MN-ek maximális száma ($K_{\max}$), amivel a nem aggregálható anycast routing bejegyzések okozta skálázhatósági problémát igyekszem kezelni. Ha a routing táblák mérete (vagyis a tartományban egyszerre lévő MN-ek átlagos száma) eléri a $K_{\max}$ értékét egy AS-ben, akkor az $N_{\max}$ értékét csökkentenünk kell, vagyis kevesebb PoA-t szabad csak az AS-be építenünk.

A javasolt algoritmust egy valószerű mobilitási környezetet teremtő szimulátor [20], [J3] továbbfejlesztésével vizsgáltam meg. A SABAS eredményeit egy független, intuitív, de nagy valószínűséggel nem optimális AS partícionálást eredményező heurisztika eredményeivel vetettem össze, és megvizsgáltam a regisztrációs költség változását az AS-ben lévő PoA cellák számának függvényében.



2. ábra: A regisztrációs költség alakulása gyéren lakott (balra) és városi (jobbra) környezetekben

A 2. ábrán bemutatott eredményeim bizonyítják, hogy a javasolt SABAS algoritmus mind gyéren lakott, mind városi környezetekben minden $N_{\max}$ értékre jobb megoldást talál a referencia heurisztikánál, és átlagosan 35%-kal csökkenti a regisztrációs költséget adott korlátok mellett.

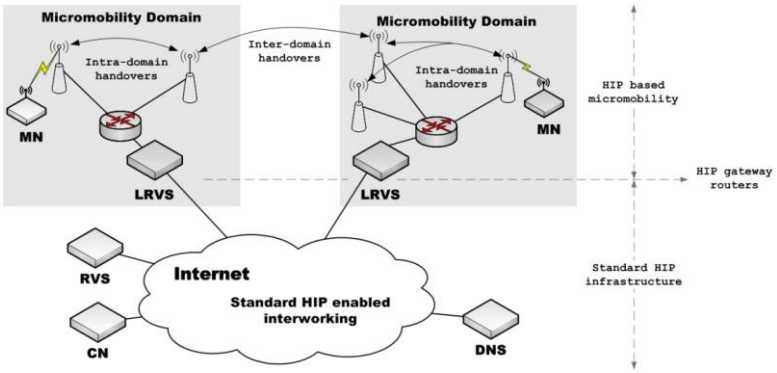
Bár az IPv6 sok újítással bír, az IP alapvető problémáját, vagyis az IP címek szemantikai túlterheltségét nem oldja fel tökéletesen. A jövő Internet egyik ígéretes architektúrális eleme, a Host Identity Protocol (HIP) [7], [8] viszont frappáns megközelítést ad az IP szemantikai túlterheltségének feloldására: egy új réteget definiál a hálózati és a szállítási réteg közé, így választva külön az IP címek topológiai helymeghatározó és állomásazonosító szerepköreit. A protokoll bevezet egy új, globálisan egyedi azonosítókból álló címteret az állomások azonosítására, így az IP használata a továbbiakban kizárólag annak meghatározására szolgál, hogy egy adott csomópont a topológia mely pontján kapcsolódik aktuálisan a hálózathoz. A protokoll ezen alapkoncepciójából adódóan a legkomplexebb mobilitási forgatókönyvek támogatása is hatékonyan oldható meg a Host Identity rétegben. Így létezik biztonságos makro-mobilitás és multihoming támogatás [9], [10], de a mikro-mobilitási esetek nem támogatottak, a protokoll kiegészítését igénylik.

HIP alapú mikro-mobilitás kezelésről először a [26]-ban olvashattunk, ám ez a megoldás nem épített fel egy teljes protokollt a feladatra, kizárólag a biztonsági vonatkozásokat érintette. Ezen kívül a [26] javaslatában a mobil berendezésnek továbbra is frissítenie kell a HIP horgonypontként szolgáló randevú szervert (Rendezvous Server – RVS) a mozgás során, így nem lehet értelmezni teljesértékű mikro-mobilitási sémaként: részleges megoldás a komplex problémára. Ez motivált egy teljesen kidolgozott HIP alapú mikro-mobilitási megoldás tervezésére és teljesítményének elemzésére.

I.3. Tézis [C4], [C11], [C17], [C21], [B3], [J14], [J20] *Kidolgoztam egy Host Identity Protocol alapú mikro-mobilitáskezelési eljárást (µHIP), mely HIP alapú jövő Internet architektúrákban biztosíthatja a gyakran mozgó felhasználók hatékony hálózatváltását a szabványos HIP protokollrendszer valamennyi előnyét kiaknázva. A µHIP protokollhoz terveztem egy HIP alapú speciális paging eljárást*

is. Kiterjedt szimulációs vizsgálatokat komplex protokoll-modelleken végezve megmutattam, hogy a javasolt µHIP séma javítja a szabványos HIP teljesítményét, intra-domain esetekben átlagban 20%-kal jobb TCP teljesítményt mutatva készíti fel a HIP szabványokat a mikro-mobilitási forgatókönyvek támogatására, és 9% körüli teljesítményromlást okoz csak a jóval ritkábban előforduló makro-mobilitási esetekben.

A HIP RVS-ek [10] által játszott horgonypont szerep szétosztása és az egyes mikro-mobilitási tartományok kezelése érdekében bevezettem egy új HIP átjáró entitást. A Local Rendezvous Server (LRVS) nevű speciális hálózati elem kezeli a tartomány összes mobil csomópontját (3. ábra), számukra lokális HIP regisztrációs szolgáltatást nyújt, és fenntart egy IP címfordító funkciót is. Ez utóbbi arra használatos, hogy a µHIP tartományba belépő MN helyi lokátorát (IP_L) az LRVS egy globálisan érvényes lokátorra (IP_G) képezze. IP_L az LRVS-sel való regisztrációra, IP_G a hagyományos RVS-sel való regisztrációra és a domain-en kívülre történő kommunikációra használatos.



3. ábra: A kidolgozott µHIP architektúra

A µHIP működése az inicializációs mechanizmussal kezdődik: az MN fizikailag kapcsolódik az mikro-mobilitási domain egyik hozzáférési routeréhez, majd pl. IPv6 állapotmentes autokonfigurációt használva megkapja IP_L lokátorát. Ezután az MN aktív HIP szolgáltatás felderítéssel [27], vagy passzívan, szolgáltatás hirdetési üzenetre várva észleli a domain-t kezelő LRVS funkció azonosítóit (HIT_{LRVS}, IP_{LRVS}), és egy szabványos Base Exchange (BEX) szekvencia [7] segítségével regisztrál hozzá. Az LRVS a BEX lefuttatásán túl elvégzi az IP_L – IP_G hozzárendelést is. A HIT_{MN}–IP_L–IP_G hármas LRVS-ben történő összeállása után még regisztrálni kell az MN-t a globális RVS-hez is, ami a HIT_{MN}–IP_G párossal tehető meg. Ennek érdekében az MN – támaszkodva a HIP által biztosított önhitelesítő kriptografikus azonosítókra és a [28] [C21] cikkekben bevezetett mechanizmusokra – delegálja jelzési jogait az LRVS számára. Az ehhez szükséges tanúsítványok az MN–LRVS BEX után kerülnek elküldésre, melynek eredményeképpen az LRVS bármilyen jelzési feladatot elvégezhet az MN nevében az adott mikro-mobilitási tartományon belül, így frissítheti az MN RVS-sel és kommunikációs partnereivel (Correspondent Node – CN) fenntartott regisztrációját is, lokátorként az IP_G címet használva.

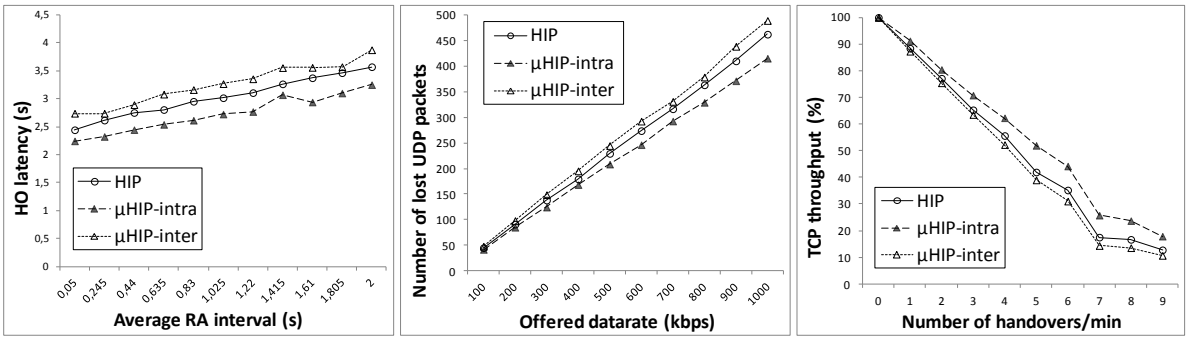
Ezek után az intra-domain hálózatváltások már könnyedén kezelhetőek: az MN egy új IP_L címet kap a tartomány másik hozzáférési routerétől, ezzel frissíti LRVS kötését (szükség esetén a delegáció tanúsítványait is). Fontos, hogy sem az MN RVS-ét, sem CN-jeit nem szükséges frissíteni, mivel a tartományon belüli mozgást az LRVS és az implementált mechanizmusok elfedik, a hálózatváltás helyileg kerül kezelésre a módszerben. Minden gyorsabb váltásokat, kevesebb csomagvesztést, végső soron jobb felhasználói élményt eredményez.

A javasolt HIP alapú mikro-mobilitási architektúra és protokoll teljesítményének vizsgálatához, valamint egy konfigurálható, kiterjeszthető és pontos HIP modell készítéséhez létrehoztam egy IPv6 alapú Host Identity Protocol szimulációs keretrendszert. A HIPSim++ nevű modellgyűjtemény [C17] OMNeT++ 4.2 környezetben fordítható és futtatható [21], GNU GPLv3 licenc alatt szabadon elérhető.

Vizsgálataim során a szabványos HIP működést használtam referenciaként, ahol egy mobil HIP hoszt (MN) váltogat különböző Wi-Fi hozzáférési pontok között (AP). Az AP-k különböző IPv6 prefixeket hirdetnek, így a HIP MN lokátora folyamatosan változik. Ennek kezelésére szabványos HIP UPDATE mechanizmusok futnak le a szimulációban [9] és frissítik a HIP RVS-t és a CN-eket. A

µHIP esetben természetesen megjelennek a mikro-mobilitási tartományok, és az azokat kezelő LRVS-ek. Intra- és inter-domain váltások egyaránt előidézhetők a két tartományt implementáló szimulációs topológiában, kezelésük pedig a µHIP sémát követi.

Az MN mindkét fő forgatókönyvben UDP/TCP kapcsolatot tart fenn CN-jével, és mozgást végez, mely AP váltásokat eredményez. Szimulációs futásonként 100 független hálózatváltási eseményt rögzítettem, és három kulcs teljesítmény indikátort elemeztem három különböző alforgatókönyvet használva. A főbb szimulációs eredményeket összefoglaló grafikonok a 4. ábrán vehetők szemügyre.



a) Hálózatváltási késleltetés b) UDP csomagvesztés c) TCP átvitel

4. ábra: A µHIP séma szimulációs vizsgálatának főbb eredményei

A 4/a ábrán a hálózatváltási késleltetés értékei láthatók, 100 független hálózatváltási esemény átlagaként minden Router Advertisement (RA) intervallum értékre. Megmutattam, hogy a µHIP intra-domain hálózatváltásai átlagosan 10%-kal jobban teljesítenek a szabványos HIP-hez képest. A valóságban sokkal ritkábban előforduló inter-domain váltások kezelése miatti járulékos jelzésterhelés csak kb. 6%-kal terheli jobban a hálózatot az új tartományokba történő váltások során.

A 4/b ábra a hálózatváltások során elveszített UDP csomagok mennyiségét mutatja be. A grafikon egyes pontjai 100 független hálózatváltási esemény eredményének átlagát jelentik minden beállított UDP adási sebességre. A szimulációk tisztán mutatják a µHIP előnyét mikro-mobilitási esetekben, és csak csekély romlás látható intra-domain váltások során. A 4/c ábra a TCP átvitel százalékos arányát mutatja különböző hálózatváltási frekvenciákra a 0 hálózatváltás esetéhez viszonyítva. A µHIP nyeresége intra-domain esetekben átlagban 20%, míg a sokkal ritkábban előforduló tartományok között váltás csak 9% körüli teljesítményromlással jár.

4.2. Felhasználók helyzetinformációinak védelmét fokozó hálózattervező algoritmusok

A mobil Internet használatának, az egyre összetettebb mobilitási forgatókönyveknek és általában a mobil kommunikációnak a terjedése hatással van a felhasználók privát szférájának biztonságára. A technológia fejlődésével párhuzamosan sajnálatos módon szinte folyamatosan nő privát szféránk veszélyeztetettsége: a gyorsan változó alkalmazások, monopolhelyzetben lévő szolgáltatók, személyre szabott reklámozást központba állító üzleti modellek veszélyforrásaival gyakran nem is vagyunk tisztában, ezért különösen fontos szerepe van a mérnöktársadalomnak a problémák megelőzésében és elhárításában.

A mobil terminálok helyzetinformációja fontos szolgáltatások alapja, de rossz kezekben a felhasználók illetéktelen profilozására, a mobil felhasználó követésére is használható. Az IP világban a helyzetinformációk védelme nem könnyű, hiszen minden egyes adatcsomag tartalmazza a forrás IP címet, ami napjainkban könnyedén és igen pontosan konvertálható földrajzi pozícióadatokra [29], [30], így téve lehetővé akár a mobil felhasználók helyzetének folyamatos megfigyelését is [31]. A jövő mobil Internetében előre láthatóan a mainál sokkal gyakrabban változhat a mobil eszközök mozgása közben a forrás IP, hiszen heterogén all-IP rendszerekben való helyzetváltoztatás gyakori IP címváltáshoz vezet, különösen a mai, alapvetően homogén rendszerekhez hasonlítva a viselkedést.

A mikro-mobilitási protokolloknak – a mobilitás lokalizációja mellett – az a jó tulajdonsága is megvan, hogy segíthetnek a felhasználók helyzetinformációinak védelmében: a mobilitás-kezelés

külvilágtól való elrejtése megakadályozza, hogy a domainen belüli IP címváltások (IP szintű hálózatváltások) okozta információszivárgás a tartományon kívülre juttasson adatokat [26].

Az IP szintű mobilitás-kezelési protokollok jövő Internet architektúrákban való terjedése egyre inkább előtérbe hozza a felhasználók privát szférájának ilyetén védelmét, akár már a hálózatok tervezése szintjén. A létező hálózattervező mechanizmusok (pl. [11], [25], [32], [J3]) főleg a paging és regisztrációs költségek közti kompromisszum keresésére fókuszálnak. Legjobb tudomásom szerint munkám előtt még senki sem emelte a helyzetinformáció védelmét a mobil hálózatok / mobilitási tartományok tervezésének szintjére, és a mikro-mobilitási protokollok ezirányú képességei is kihasználatlanok voltak. Ez motivált abban, hogy olyan mikro-mobilitási tartomány tervező algoritmusokat hozzak létre, melyek kihasználják a mikro-mobilitási protokollok természetes helyzetinformáció-védelmi képességeit, miközben figyelembe veszik a paging és regisztrációs költségek szokásos megkötéseit is.

II.1. Tézis [J8], [B4] *Kidolgoztam egy egyszerű helyzetinformáció-védelmi modellt olyan mikro-mobilitási domain-tervező algoritmusok számára, melyek már a hálózat tervezésekor figyelembe veszik a mikro-mobilitási protokollok helyzetinformáció védelmi képességeit. A modell alapján javasoltam egy speciális élsúlyozási technikát, mellyel megfelelő gráfreprezentáció állítható elő a tervezőalgoritmusok számára. Az így megalkotott eszközrendszerre támaszkodva kifejlesztettem a PA-SABLAF (Privacy Aware Simulated Annealing based Location Area Forming) nevű algoritmust, ami a SABAS továbbfejlesztéseként képes az inter-domain váltások számának adaptív csökkentésére.*

Az általam javasolt egyszerű helyzetinformáció-védelmi modellben két összetevő biztosítja a PoA átmenetek speciális, "privacy aware" súlyozását. Egyrészt bevezettem a *cellák statikus helyzetinformáció-védelmi szintjét* (*static location privacy significance level of the cells,* $SLP_{[k]}$ a k cella esetén), melynek segítségével az operator (a hálózatot tervező) meghatározhatja, hogy az egyes cellák az ott lévő létesítmények jellege miatt mennyire érzékenyek az IP szintű helyzetinformáció szivárgásra. Másrészt definiáltam a *felhasználók különböző lokáció típusokra vett helyzetinformáció-védelmi érzékenységét* (*user's location privacy profile for different location types* ($ULP_u^{lt_{[k]}}$ ahol u a felhasználó, lt pedig a lokáció típus a k cellában) annak leírására, hogy egy adott mobil felhasználó milyen szintű védelemre tart igényt az adott lokáció típusú cellában. A bejövő dinamikus felhasználói igények és a statikus cellaértékek együttesen hozzák létre a cellára vonatkozó helyzetinformáció-védelmi faktort (*cell's overall location privacy factor,*$OLPF_{[l]}$, *ahol* l *az adott cella*), melyet az élsúlyozási módszerben használok fel. Ezzel a módszerrel a felhasználói és az operátori követelmények egyaránt figyelembe vehetők.

A cellaváltási rátáknak az érintett helyzetinformáció-védelmi faktorral való súlyozásával teszem a tervezőalgoritmust "privacy aware"-ré. Az alkalmazott matematikai reprezentációban a cellák (PoA-k) a gráf csomópontjai, a cellahatár átlépések a gráf irányított élei, a súlyok pedig a cellaváltási ráták (cell border crossing rates) minden irányban. Ezeket a súlyokat módosítom, mikor végrehajtom az alábbi speciális élsúlyozási technikát a célcellára vett helyzetinformáció-védelmi faktort használva:

$$WR_{[k][l]} = CR_{[k][l]} \times OLPF_{[l]} + CR_{[l][k]} \times OLPF_{[k]} \qquad (1)$$

ahol a $WR_{[k][l]}$ a k és l cellák (csomópontok) közti él súlyozott rátája, $CR_{[k][l]}$ a k és l közti cellaváltási ráta értéke, és $OLPF_{[l]}$ az l cella helyzetinformáció-védelmi faktora.

Ezt alapul véve a javasolt PA-SABLAF algoritmus a mohó fázist annak a cella párnak a kiválasztásával kezdi, ahol a legnagyobb a súlyozott ráta, és a két cellát berakja a cellák (PoA-k) D_1 kezdeti tartományába. A következő lépésben a második legnagyobb olyan súlyozott rátát veszi, melyre igaz, a hozzá tartozó PoA pár egyik eleme már része D_1 tartománynak. Ezután ellenőrzi az $N_k < N_{max}$ egyenlőtlenséget, ahol N_k a k -adik tartomány celláinak száma, N_{max} pedig a peremfeltétel, melynél több cella nem lehet egy domainben a paging költség minimalizálása érdekében. Ha az egyenlőtlenség igaz, akkor az új cella hozzávehető D_1 halmazhoz. Ha nem igaz, akkor a cella nem adható ehhez a halmazhoz, és egy új domain kerül létrehozásra, úgy, ahogy azt a SABAS [C9] és SABLAF [12] algoritmusok is teszik. Ennek segítségével a főbb mozgási irányok (autópályák, stb.) és a helyzetinformáció-védelem egyaránt figyelembe vehető. A cellák fenti, mohó partícionálása után az s_0

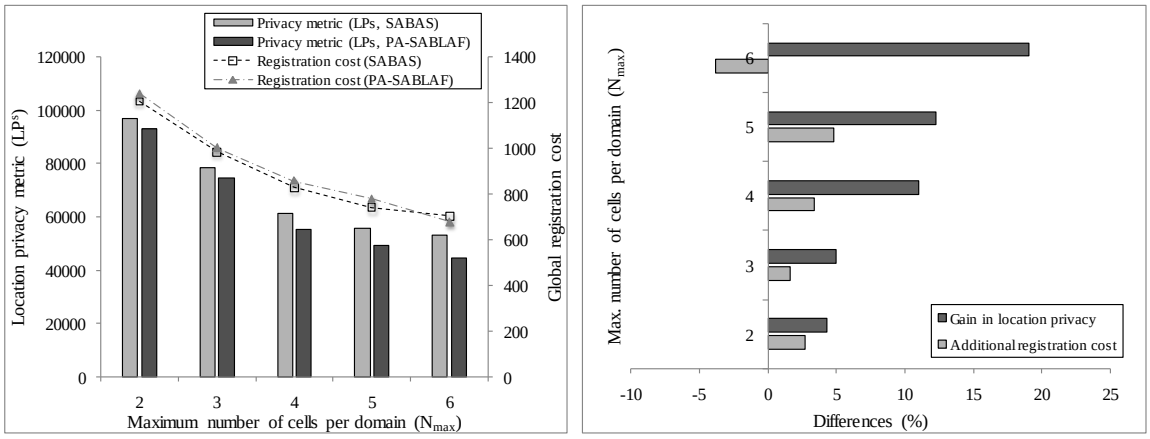
kezdeti, valószínűleg szuboptimális megoldás előáll, és elkezdődik a SABAS-nál már ismertetett szimulált lehűtési fázis.

II.2. Tézis [J8], [B4] *Kidolgoztam egy helyzetinformáció-védelmi metrikát ($\boldsymbol{LP^s_{mic}}$) annak kifejezésére, hogy egy adott mikro-mobilitási domain struktúra milyen hatékonyan veszi figyelembe a cellák statikus helyzetinformáció-védelmi szintjét és a felhasználók által a rendszerbe vitt dinamikus helyzetinformáció-védelmi érzékenységét a működés során. Megmutattam, hogy a PA-SABLAF a regisztrációs költségek maximum 4,8%-os növekedése mellett átlagosan 10%-kal javítja a létrehozott struktúra tulajdonságait.*

Az $\boldsymbol{LP^s_{mic}}$ segítségével mérhetővé teszem, hogy a domain-en kívüli támadók a mobil berendezések követését mennyire nehezen tudják megoldani az IP címváltások figyelésével: kiszámítom a mobil terminálok inter-domain váltásainak súlyozott összegét a teljes hálózatra. Minden mobil minden inter-domain hálózatváltására, és az ilyen hálózatváltások előző és következő celláira összegzem a cellák statikus helyzetinformáció-védelmi szintjét és a mobil csomópontok szóban forgó lokáció típusokra vett helyzetinformáció-védelmi érzékenységének négyzetét, és így állítom elő az egész mikro-mobilitási domain rendszert jellemző helyzetinformáció-védelmi metrikát:

$$\boldsymbol{LP^s_{mic}} = \sum_{u} \sum_{h \in IH_u} (ULP_u^{lt_{[k]}})^2 + (ULP_u^{lt_{[l]}})^2 + SLP_{[k]} + SLP_{[l]} \tag{2}$$

ahol IH_u az u felhasználó valamennyi inter-domain hálózatváltási eseményét jelenti, és $h_{[k][l]} \in IH_u$ egy hálózatváltás forrás (k) és cél (l) celláit azonosítja. Ebből adódik, hogy egy hálózat kisebb $\boldsymbol{LP^s_{mic}}$ értékeknél teljesít jobban a helyzetinformáció-védelem szempontjából.



5. ábra: PA-SABLAF vs. SABAS (balra) és helyzetinformáció-védelem nyereség vs. költségnövekmény PA-SABLAF esetén (jobbra)

A PA-SABLAF algoritmust az I.2. tézisben már bemutatott mobilitás szimulátor egy továbbfejlesztett változatában vizsgáltam. Négy különböző PoA rendszert használtam nagyszámú cellával és mobil csomóponttal, különböző úthálózatokkal. Ebben a környezetben vizsgáltam meg, és a már ismertetett, hagyományos SABAS megoldással hasonlítottam össze a javasolt algoritmust. Az 5. ábrán látható, összes mérésre átlagolt eredmények alapján a PA-SABLAF minden N_{max} értékre jobb $\boldsymbol{LP^s_{mic}}$ értéket adott az eredeti SABAS-nál. A magasabb szintű helyzetinformáció-védelem ára a regisztrációs költségek maximum 4,8%-os növekedése.

Bár a javasolt $\boldsymbol{LP^s_{mic}}$ már képes a mobilhálózatok helyzetinformáció-védelmi képességének numerikus reprezentálására, ez egy egyedi metrika, nem tekinthető általános megközelítésnek. Ezért kezdtem el foglalkozni olyan metrikák átdolgozásával, melyek a helyzetinformáció-védelem irodalma alapján elterjedtnek, más használati esetekben már beváltnak tekinthetők.

II.3. Tézis [J8], [B4] *Kidolgoztam egy bizonytalanság (uncertainty) alapú helyzetinformáció-védelmi metrikát (**$\boldsymbol{LP^{u}_{mic}}$**) annak kifejezésére, hogy egy mikro-mobilitási domain struktúrában milyen hatékony a mikro-mobilitási protokoll miatti beépített helyzetinformáció-védelem. Erre a metrikára alapozva létrehoztam a PA^{u}-SABLAF domain tervező algoritmus-variánst, és megmutattam, hogy a PA^{u}-SABLAF az **$\boldsymbol{LP^{u}_{mic}}$** bizonytalaság alapú metrika értelmében akár 30%-nál is nagyobb relatív nyereséggel javít a domain struktúrán nagyszámú PoA-t tartalmazó domainek esetén, az inter-domain hálózatváltások lehetséges variációinak növelésével.*

A bizonytalanság (uncertainty) alapú helyzetinformáció-védelmi metrikát először a [33]-ban publikálták, ahol a szerzők az mérték, hogy egy mekkora a támadó bizonytalansága a megfigyelt események egy adott felhasználóhoz való rendelésének. Ezt a megközelítést adaptáltam mikro-mobilitási rendszerekben történő használatra.

Egy mikro-mobilitási hálózatban a támadó az általa elfogott felhasználói IP csomagok forrás címmezői alapján az MN mozgása közben végrehajtott inter-domain váltások egy aktuális sorozatát képes megfigyelni. Ezért az MN pályáját domain belépési és kilépési pontokra (vagyis a támadó által megfigyelhető eseményekre) bontom, így ezen pontok határolják a nem megfigyelhető útszakaszokat. Mivel az intra-domain útszakaszok IP címinformációk alapján a domain-en kívüli támadók számára nem követhetők, és feltéve, hogy a domainek legalább kettőnél több cellát tartalmaznak, a támadók csak a belépési és kilépési pontokat azonosíthatják (ezeket nevezzük "felvillanásoknak"). Feltételezzük, hogy a támadó ismeri a domain struktúrát, az átmenetek nem súlyozottak, és megegyező valószínűségűek.

Legyen$Pr_A(d)$ annak a valószínűsége, hogy egy támadó jól tippelt, mikor megpróbálta kitalálni, hogy egy d domainbe váltáskor mi volt a valódi belépési és kilépési pont. A [33] alapján a felhasználó bizonytalanság alapú helyzetinformáció-védelmi metrikája az adott hálózatban a $Pr_A(d)$ entrópiájával számítható ki. Ha ezt az entrópiát az egész hálózat valamennyi felhasználójára kiszámítjuk és összegezzük, akkor megkapjuk az **$\boldsymbol{LP^{u}_{mic}}$** -val jelölt, az egész mikro-mobilitási rendszerre vonatkoztatott metrikát (mivel ez egy entrópia-jellegű mennyiség ezért a nagyobb érték jelenti a jobb helyzetinformáció-védelmet).

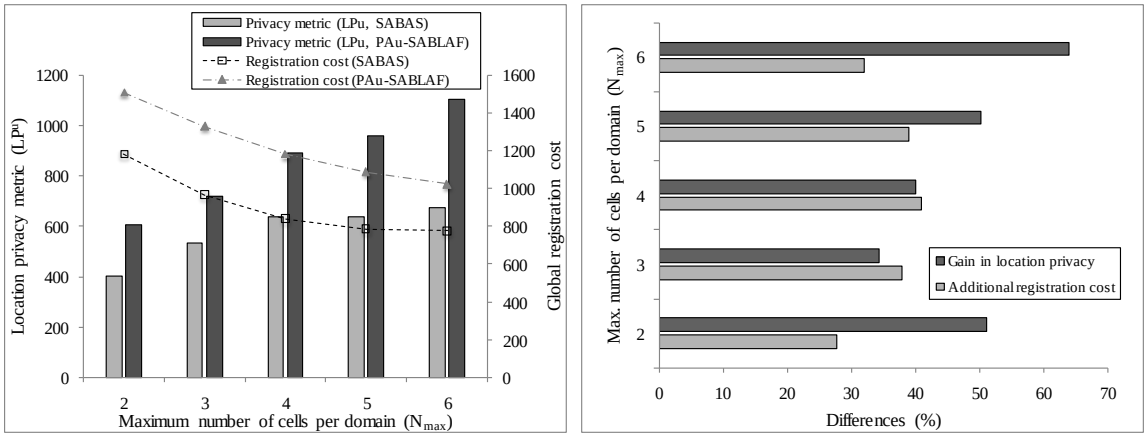
$$\boldsymbol{LP^{u}_{mic}} = -\sum_u \sum_j Pr_A(d_j) \times log_2\left(Pr_A(d_j)\right) \tag{3}$$

Ezen metrikára építő PA^{u}-SABLAF algoritmus-variánsban a mohó fázis az aktuálisan vizsgált átmeneten kívül figyelembe veszi a szomszédos átmeneteket is, hiszen a lehetséges átmenetek minél nagyobb számával igyekszünk ugyanis elbizonytalanítani a támadót. Mivel a mikro-mobilitási domainben lévő cellák (PoA-k) maximális számra N_{max}-ban korlátozott, ezért az algoritmus olyan struktúrát próbál készíteni, ahol a nagy átmeneti rátával bíró cellák hozzák létre a domainek magját úgy, hogy a szomszédos domainekbe is a lehető legtöbb átmenet induljon. A nagy átmenő forgalommal rendelkező cellák forgalmát tehát megpróbáljuk minél több élre/élsorozatra elvezetni, ami azt eredményezi, hogy a többi domainbe kerülő cellák és a nagy forgalmú cellák közt sok helyen lesz lehetséges a váltás. Az ennek megfelelő, PA^{u}-SABLAF variánshoz kifejlesztett élsúlyozási módszer a következő:

$$WR^{u}_{[k][l]} = CR_{[k][l]} + CR_{[l][k]} + TF_{[l]} \tag{4}$$

ahol $CR_{[k][l]}$ a k -ból l-be irányuló átmeneti ráta, és $TF_{[l]}$ az l cellára számított átmeneti faktor (a cella még vár a domainbe való csoportosítására). Az átmeneti faktor definíciója: $TF_{[l]} = \sum_{m \in A_l}(CR_{[l][m]} + CR_{[m][l]})$ ahol A_l az l cella összes szomszédjának halmaza. Ezzel elérhetjük, hogy több él kerül be potenciálisan domain váltást tartalmazó élként egy domain határára kerülő új cella hozzávételével, így a bizonytalanságot jobban növeljük. Ezen kívül a PA^{u}-SABLAF algoritmus megegyezik a II.1. tézisben ismertetett módszerrel.

Szimulációk segítségével megmutattam, hogy a PA^{u}-SABLAF kiemelkedő relatív nyereséget mutat az **$\boldsymbol{LP^{u}_{mic}}$**viszonylatában: az $N_{max} = 6$ esetben a metrika 30%-nál is nagyobb növekménnyel bír (6. ábra). Azonban ebben a variánsban kell a legnagyobb árat is fizetnünk: a legkisebb költségnövekmény is 27%-os.



6. ábra: PA^{u}-SABLAF vs. SABAS (balra) és helyzetinformáció-védelem nyereség vs. költségnövekmény PA^{u}-SABLAF esetén (jobbra)

II.4. Tézis [J8], [B4] *Kidolgoztam egy követhetőség (traceability) alapú helyzetinformáció-védelmi metrikát (*$\boldsymbol{LP^{\bar{\bar{t}}}_{mic}}$*) annak kifejezésére, hogy egy mikro-mobilitási domain struktúrában milyen mértékben képtelenek a támadók a mobil csomópontok IP címváltozás alapján történő lokalizálására vagy követésére. Erre a metrikára alapozva létrehoztam a PA^{t}-SABLAF domain tervező algoritmus-variánst, és megmutattam, hogy a PA^{t}-SABLAF az* $\boldsymbol{LP^{\bar{\bar{t}}}_{mic}}$ *követhetőség alapú metrika értelmében 3,9%-os átlagos nyereséggel képes javítani a domain struktúrán úgy, hogy a felhasználókat az egyes tartományok belsejében tartja és a legtöbb esetben a regisztrációs költséget is csökkenti.*

A követhetőség (traceability) alapú metrika annak a mértékét igyekszik megfogni, hogy a támadó nagy bizonyossággal követ egy mobil felhasználót. A [34] szerzői definiálták először az *átlagos távolság a zavarásig* (*mean distance to confusion)* metrikát, mely azt az átlagos távolságot méri, ami során a felhasználót a támadó nagy bizonyossággal képes követni. Az én modellemben – a mikro-mobilitás protokollok helyzetinformáció-védelmi sajátosságait tekintve – az *átlagos távolság zavarásban* (*mean distance in confusion*) metrika definíció megfelelőbb, ezt nevezem $\boldsymbol{LP^{\bar{\bar{t}}}_{u}}$-nek, és azt mérem vele, hogy mekkora az az átlagos, mobil felhasználó által megtett távolság, ami közben a támadó nem tudja követni. Legyen Y_u az összes ilyen követhetetlen periódust tartalmazó halmaz az u felhasználó esetében. Ez alapján egy u felhasználóhoz tartozó, *mean distance in confusion* típusú ($\boldsymbol{LP^{\bar{\bar{t}}}_{u}}$) helyzetinformáció-védelmi metrika

$$\boldsymbol{LP^{\bar{\bar{t}}}_{u}} = \left(\frac{\sum_{(\hat{e}_i, \hat{e}_j \in Y_u)} \left\| loc(\hat{e}_i) - loc(\hat{e}_j) \right\|}{|Y_u|} \right)^{-1} \tag{5}$$

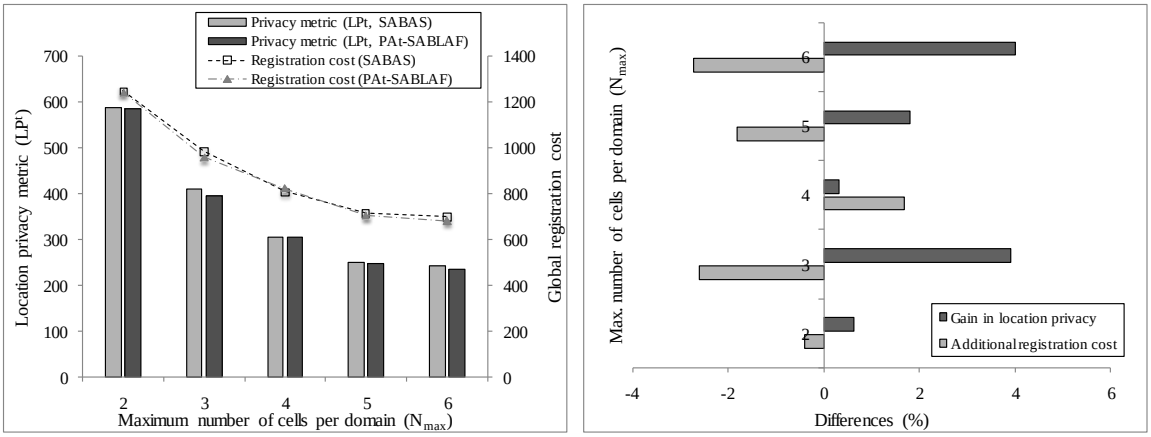
ahol $loc(\hat{e}_i)$ az a lokáció, ahol az $\hat{e}_i$ esemény megtörtént. Egy teljes mikro-mobilitási rendszerre számított követhetőség alapú metrikát ($\boldsymbol{LP^{\bar{\bar{t}}}_{mic}}$) az alábbiként definiáltam (a helyzetinformáció-védelem szintje arányos a zavarásban töltött idővel, így ennél a metrikánál a kitevő értelmében a kisebb értékek a jobbak)

$$\boldsymbol{LP^{\bar{\bar{t}}}_{mic}} = \sum_{u} \left(\frac{\sum_{(\hat{e}_i, \hat{e}_j \in Y_u)} \left\| loc(\hat{e}_i) - loc(\hat{e}_j) \right\|}{|Y_u|} \right)^{-1} \tag{6}$$

A PA^{t}-SABLAF algoritmus-variánsban olyan domain struktúra kialakítására törekszem, melyben a felhasználók nagyobb valószínűséggel végeznek intra-domain mozgásokat. Ez úgy érhető el, ha növeljük a domainekben lévő elvezető (deflector) élek számát. Egy él vagy élek sorozatát elvezetőnek nevezek, ha jelentős átmeneti rátával bír és/vagy nagyobb forgalmú, több irányból érkező forgalmat összefogó élek bemenetét illetve kimenetét adja. Ennek segítségével elérjük, hogy a mobil csomópontok mozgása során egymást gyakran követő cellák és az azokat összekötő élek egy domainbe kerüljenek. Az ennek megfelelően módosított, és a PA^{t}-SABLAF mohó fázisában használatos élsúlyozási módszer:

$$if \quad E_{[k][l]} \in D_{\psi}$$
$$then\ for \quad \forall E_{[i][j]} \in E_{[k][l]} \cup A_{[k][l]} \quad (7)$$
$$do \quad WR^{t}_{[i][j]} = CR_{[i][j]} + CR_{[j][i]} + DF$$

ahol $E_{[k][l]}$ a k és l cellák közti él, D_{ψ} az elvezető élek halmaza, mely azokat az éleket tartalmazza, ahol a hálózat összes átmeneti rátáit tekintve a felső ψ százalék összpontosul, $A_{[k][l]}$ az $E_{[k][l]}$ szomszédjainak halmaza, $CR_{[k][l]}$ a k cellából l cellába tartó átmenet ráta, és DF a deflector faktornak nevezett konstans, mellyel a deflector tulajdonságú éleket jutalmazzuk a súlyozáskor. Ettől a módosított súlyozási módszertől eltekintve a PA^t-SABLAF variáns megegyezik a II.1. tézisben részletezett algoritmussal.



7. ábra: PA^t-SABLAF vs. SABAS (balra) és helyzetinformáció-védelem nyereség vs. költségnövekmény PA^t-SABLAF esetén (jobbra)

A PA^t-SABLAF vizsgálatakor kapott eredményeket a 7. ábra foglalja össze. Ez a variáns mérsékelt átlagos nyereséget (3,9%) mutat az $\boldsymbol{LP^{\bar{t}}_{mic}}$ metrikát tekintve, és az $N_{max} = 4$ esetben negative a relatív nyereség. Azonban ez a módszer a legtöbb esetben képes volt egyszerre javítani a helyzetinformáció-védelmi metrikán és a regisztrációs költségen a legtöbb N_{max} esetben.

Javasolt módszereimmel bebizonyítottam, hogy a felhasználók helyzetinformációjának védelme már a mobil hálózatok tervezésekor növelhető, és a regisztrációs költségnövekmény megfizethető ár.

4.3. Hálózat-mobilitási (NEMO) protokollok optimalizálása

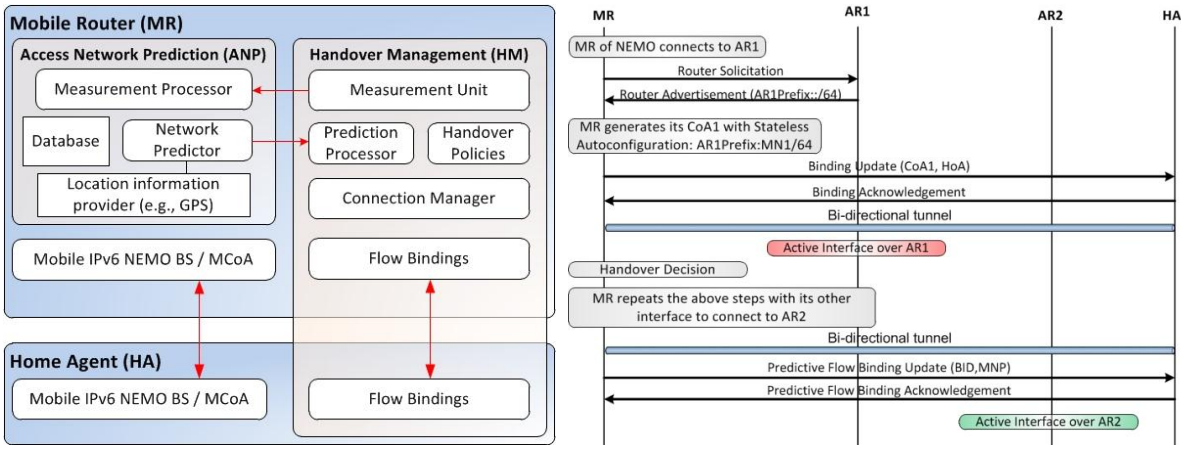
A mobilitás kezelése időigényes, ami a valós idejű (real-time) kommunikációt az okozott csomagvesztés, késleltetés miatt könnyen ellehetetlenítheti. Mindez különösen igaz a mozgó hálózatokra, ahol a NEMO-t vezérlő Mobile Router (MR) entitás nagyszámú belső hálózati csomópont mobilitás-kezeléséért felel [C5], [C10], [C15]. Az IPv6 a terminál mobilitást (MIPv6 [2]) és a hálózat mobilitást (NEMO BS [4]) egyaránt támogatja. Megoldott a multihoming/multi-access problémája (MCoA [35]), és már léteznek a hálózatváltást segítő, azt gyorsító megoldások is ([36], [17], [37], [B7]), de a követelmények változása továbbra is új utak keresésére ösztönzi a kutatókat.

A NEMO megoldások továbbfejlesztését két megközelítésben végeztem. Egyrészt kiterjesztettem a szabványos IPv6 megoldásokat egy speciális keretrendszerrel, ami az MCoA alagutak prediktív és proaktív átkapcsolásával optimalizálja az IPv6 alapú mozgó hálózatok mobilitás-kezelését (III.1 és III.2 tézisek). Másrészt kibővítettem a Host Identity Procotol (HIP) családot és a már bemutatott µHIP sémát annak érdekében, hogy HIP alapokon is lehessen NEMO támogatást nyújtani (III.3 tézis).

III.1. Tézis [C19], [C25], [B7] *Kifejlesztettem egy aktív hálózati mérések földrajzi pozícióadatokhoz való rendelésére támaszkodó, ez alapján a hálózatváltási eseményeket előrejelző és az MCoA alagutak prediktív átkapcsolásával a hálózatváltást optimalizáló keretrendszert és cross-layer vezérelt végrehajtó sémát a multihoming NEMO hálózatok mobilitás-kezelésének átlapolódó rádiós hozzáférési környezetekben történő javítására.*

Kötött pályán vagy rögzített útvonalon mozgó járművek (pl. vonatok) esetén nagy előny, hogy feltérképezhetjük az út során elérhető hálózatokat, ezeket pozícióadatokhoz kötve adatbázist készíthetünk, mely alapján felkészülhetünk a hálózatváltás folyamataira, amivel jócskán csökkenthetjük a hálózatváltás okozta extra késleltetés mértékét. A multihoming konfigurációk által megvalósított hozzáférési redundancia tovább növeli a mobil végberendezések csatlakozási lehetőségeit, vagyis az átlapolódó vezeték nélküli lefedettségeket akár egyszerre is használni képes megoldások nagy előrelépést jelentenek a folyamatos és szakadásmentes mobil kommunikáció felé.

Az általam kidolgozott séma a Flow Bindings protokollra [38] épül, több aktív interfészt használ, és a megfelelő szabályok segítségével az MR minden forgalmát egy interfészre irányítja (aktív interfész). Így elveszítjük ugyan a redundáns átvitel előnyeit (pl. multipath kommunikációra sincs mód), de megnyerjük vele azt, hogy az átvitelre nem használt interfészeken folyamatosan figyelhetjük a környezetünket, és ha úgy döntünk, akkor az inaktív interfészek egyikét felkészíthetjük az átvitel (közel)jövőbeli kezelésére, vagyis a hálózatváltásra. A felkészülés során kiválasztjuk a megfelelő interfészt (hozzáférési hálózatot), csatlakozunk hozzá, IPv6 címet konfigurálunk, és létrehozzuk az MCoA alagutakat, majd egy időzített Flow Bindings frissítéssel az otthoni ügynökön és az MR-en egyszerre átkapcsoljuk az alagutakat és az új interfész válik aktívvá.



8. ábra: A kidolgozott keretrendszer (balra) és a hálózatváltást végrehajtó protokoll (jobbra)

Az új interfész aktivációja és a régi deaktivációja szinkronizált, és az időzített policy-vezérlő jelzési üzenetekkel valósítható meg az HA és MR entitásokon.

A kidolgozott keretrendszer a 8. ábra bal oldalán látható, és három fő komponenst vetít ki: Access Network Predictor (ANP), Handover Manager az MR oldalán (HM-MR) a Home Agent oldalán (HM-HA). Nem az összes részegység belső működésének teljes definíciója az én munkám, de a keretrendszer maga, a részegységek összehangolt működési rendszere és a prediktív hálózatváltási szisztéma az én eredményeim.

Az ANP felel a hozzáférési hálózatok információit tároló adatbázis kezeléséért, és a periodikus előrejelzési üzenetek HM-MR felé való küldéséért. Ez utóbbit az aktuális sebességvektor és pozíció, valamint a mérési eredmények földrajzi koordinátákhoz való rendelése segítségével hajtja végre. Annak érdekében, hogy elkerüljük az adatbázis méretének felrobbanását, a fogadott földrajzi koordinátákat kerekítjük (a hosszúsági és szélességi értékeket megszorozzuk 10000-rel és a legközelebbi egész számra kerekítjük), így folytonos tér helyett korlátos halmazt alkotnak, melynek elemeit raszterpontoknak, a halmazt magát pedig raszterhálónak nevezzük. Ezt az adatbázist folyamatosan frissíti a HM modul hálózati mérésekért felelős Measurement Unit egysége, ami az inaktív interfészeket használva folyamatosan monitorozza a RAN-okat és SNR, IPv6 prefix, sávszélesség, RTT és hasonló értékeket gyűjt és küld az ANP-nek.

Az ANP felől érkező előrejelzéseket a Connection Manager fogadja, ami dönthet, hogy az aktuális aktív interfészt (hozzáférési hálózatot) egy másikra cseréli az előrejelzési időkeretben. Ha a hálózatváltás mellett dönt, akkor az MCoA lehetőségeit kihasználva az alábbi lépéseket végzi el. Az egyik inaktív interfészével a HM csatlakozik az új hozzáférési hálózathoz és létrehozza az MCoA MIPv6 kötéseit (binding). Ebben a fázisban az aktuális és az új hálózathoz való hozzáférés egyaránt MR-HA alagutakkal van megoldva. Maga a hálózatváltás teljes mértékben Flow Bindings alapú, ami esetünkben az összes folyam egyik interfészről a másikra való terelését jelenti. Az aszimmetrikus útválasztás kikerülése érdekében az MR és a HA egyszerre, időzített módon végzi el a folyamokra vonatkozó policy-k és állapotok módosítását. Mindent un. prediktív Flow Binding Update/Acknowledgement üzenetekkel beszéli le az MR és a HA (8. ábra, jobb oldal). Ha a folyamok átváltása sikeres, akkor az új interfész válik aktívvá, míg a többi interfész inaktív állapotban van. A NEMO belső hálózati csomópontjai (Mobile Network Nodes – MNNs) mindebből semmit sem vesznek észre, és átlátszó módon használják a mindenkori aktív interfésszel megvalósított kapcsolatot (8. ábra, jobb oldal). A rendszerben különböző hálózatváltási politikák (Handover Policies), stratégiák és döntési algoritmusok működhetnek, tovább növelve az adaptivitás szintjét.

Látható, hogy a javasolt keretrendszer és hálózatváltási protokoll erősen támaszkodik az előrejelzés pontosságára, ami nagyban függ az ANP modul raszterizációs technikájától, a raszterháló részleteitől. Ezért kezdtem el dolgozni a raszterhálón történő helytelen pozícionálás valószínűségének kiszámításán, és az optimális raszterháló tervezési kérdésein.

III.2. Tézis [C25], [J16] *Kidolgoztam egy valószínűségi modellt az ANP belső működésének leírására, és javasoltam egy alkalmas raszterizációs sémát, melynek használatával a raszteren való hibás pozícionálás valószínűsége 1% alatt marad.*

Legyen raszterpontjaink halmaza $\mathcal{S} = \{\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots \boldsymbol{x}_\infty\}$. $\boldsymbol{x}_i$ azt az i. pontot jelenti, mely egy földrajzi pozíció két koordinátával: egyik a nyugat-keleti koordináta, másik pedig az észak-déli koordináta. $\mathcal{S}$ egy végtelen, de megszámlálható számosságú halmaz. A halmaz elemei konstansok: az aktuális rasztermérettel adottak. Tegyük fel, hogy egy $\boldsymbol{x}_0$ földrajzi pozíción vagyunk ($\boldsymbol{x}_0$ értékét egy istentől kaptuk – pontosan megmérni nem tudjuk). Van egy GNSS alapú mérőberendezésünk, és meg akarjuk mérni $\boldsymbol{x}_0$ értékét. Méréseket végzünk, és $\boldsymbol{\eta}$ -t kapunk, ami természetesen nem lehet 100%-osan pontos, csak egy becslés. Ez a $\boldsymbol{\eta}$ egy véletlen szám (normális eloszlású, mivel értéket sok apró, egymástól független hatás együttesen alakítja ki), várható értéke $\boldsymbol{x}_0$, kovariancia mátrixa pedig $\boldsymbol{C}$:

$$\mathbb{E}\{\boldsymbol{\eta}\} = \boldsymbol{x}_0 \tag{8}$$

$$Pr\{\boldsymbol{\eta} \leq \boldsymbol{y} | \boldsymbol{x}_0, \boldsymbol{C}\} = \Phi(\boldsymbol{y}, \boldsymbol{x}_0, \boldsymbol{C}) = \int_{-\infty}^{y_1} \int_{-\infty}^{y_2} \frac{1}{\sqrt{2\pi}^2 (det\boldsymbol{C})^{1/2}} e^{(\boldsymbol{z}-\boldsymbol{x}_0)^\top \boldsymbol{C}^{-1} (\boldsymbol{z}-\boldsymbol{x}_0)} dz_2 dz_1 \tag{9}$$

Jegyezzük meg, hogy (9)-ben bevezettünk egy új jelölést (Φ). Szintén fontos, hogy $\boldsymbol{\eta} \leq \boldsymbol{y}$ minden olyan $\boldsymbol{\eta}$ pontot jelent, melynek mindkét koordinátája kisebb, a megfelelő $\boldsymbol{y}$ koordinátáknál.

Az ANP adatbázis a III.1. tézisben leírtak miatt csak raszterpontokat használ. Így a mért $\boldsymbol{\eta}$ érték alapján ki kell választanunk a legközelebbi raszterpontot a mérési eredmény tárolásához:

$$\boldsymbol{\xi}(t) = \text{argmin}_{\boldsymbol{x} \in \mathcal{S}} \parallel \boldsymbol{\eta}(t) - \boldsymbol{x} \parallel \tag{10}$$

Itt megjelenik az időtől való függés(t), és a $\|.\|$ operátor, mely az abszolút távolságot méri. Isteni segítséggel (vagyis ismerve $\boldsymbol{x}_0(t)$ értékét), megkaphatjuk a tökéletesen becslést a tároláshoz használandó $\boldsymbol{x}(t)$ raszterpont számára:

$$\boldsymbol{x}(t) = \text{argmin}_{\boldsymbol{x} \in \mathcal{S}} \parallel \boldsymbol{x}_0(t) - \boldsymbol{x} \parallel \tag{11}$$

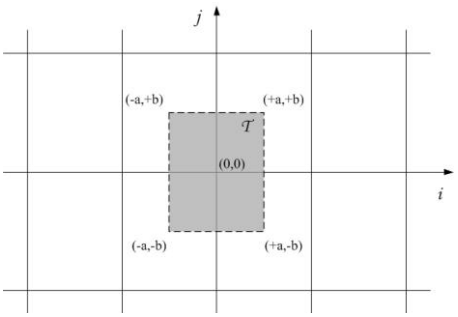
Ezek alapján a formalizált kérdés: mi a valószínűsége annak, hogy rosszul becsüljük a tároláshoz használandó raszterpontot?

$$Pr\{\boldsymbol{\xi}(t) \neq \boldsymbol{x}(t)\} = ? \tag{12}$$

Mivel (10) és (11) egyaránt nemlineáris művelet, így a probléma vizsgálata nehéz. Az alábbiakban megoldást adok ezen valószínűség kiszámításának kérdésére.

A 9. ábra mutatja a használandó földrajzi raszterháló elrendezést. Mivel a háló önhasonló felépítésű, ezért a koordinátarendszer origójába helyezhetjük. A $\mathcal{T}$ terület definíciója:

$$\mathcal{T} = \{(i,j),\ where\ -a \leq i \leq +a\ \ and\ \ -b \leq j \leq +b\} \tag{13}$$



9. ábra: A modellben használt raszterháló elrendezés

A valódi földrajzi pozíció ($\boldsymbol{x}_0$) bármelyik pontba megegyező valószínűséggel eshet, ezért a rossz becslés valószínűsége ($Pr\{\boldsymbol{\xi}(t) \neq \boldsymbol{x}(t)\}$) megegyezik annak a valószínűségével, hogy a valódi pont a $\mathcal{T}$-vel jelzett szürke részben van ($\boldsymbol{x}_0(t) \in \mathcal{T}$), a mért pont pedig a szürke részen kívül ($\boldsymbol{\eta}(t) \notin \mathcal{T}$):

$$Pr\{\boldsymbol{\xi}(t) \neq \boldsymbol{x}(t)\} = Pr\{\boldsymbol{x}_0(t) \in \mathcal{T} \cap \boldsymbol{\eta}(t) \notin \mathcal{T}\} = 1 - Pr\{\boldsymbol{x}_0(t) \in \mathcal{T} \cap \boldsymbol{\eta}(t) \in \mathcal{T}\} \tag{14}$$

Annak a valószínűsége, hogy $\boldsymbol{\eta}$ a $\mathcal{T}$ területbe esik:

$$Pr\{\boldsymbol{\eta} \in \mathcal{T} | \boldsymbol{x}_0, \boldsymbol{C}\} = \Phi\left(\binom{+a}{+b}, \boldsymbol{x}_0, \boldsymbol{C}\right) - \Phi\left(\binom{+a}{-b}, \boldsymbol{x}_0, \boldsymbol{C}\right) - \Phi\left(\binom{-a}{+b}, \boldsymbol{x}_0, \boldsymbol{C}\right) + \Phi\left(\binom{-a}{-b}, \boldsymbol{x}_0, \boldsymbol{C}\right) \tag{15}$$

Követve a (14)-et, a Bayes törvényét és a raszteren történő hibás pozícionálásra vonatkozó feltételünket, az alábbi egyenlőtlenséget kapuk:

$$0.01 \geq Pr\{\boldsymbol{\xi}(t) \neq \boldsymbol{x}(t)\} = 1 - \frac{1}{4ab}\int_{-a}^{+a}\int_{-b}^{+b} Pr\{\boldsymbol{\eta} \in \mathcal{T} | \boldsymbol{x}_0, \boldsymbol{C}\}_{\boldsymbol{x}_0 = \binom{i}{j}} djdi \tag{16}$$

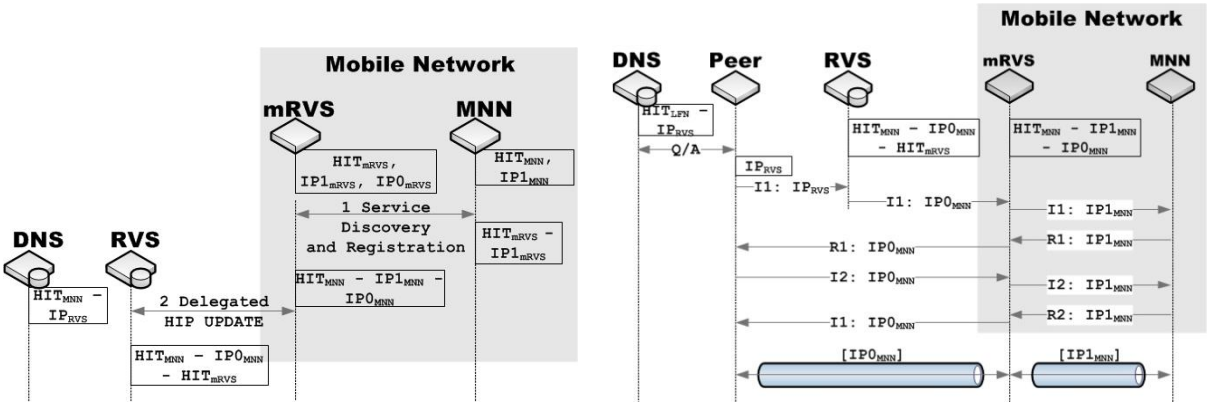
Ha az MR-ben működő mérőberendezés implementációjaként egy GPS eszközt tételezzünk fel $\sigma = 5m$ szórással, figyelembe vesszük, hogy a szélességi körök mentén az egységnyi szöghöz tartozó távolság az adott hely szélességétől is függ (az értékeket a szélesség koszinuszával kell normálni), és Budapest szélességét választjuk működésünk környezetéül (~47.5° N), akkor a megfelelő raszterháló mérete nagyobb, vagy egyenlő mint $18.2m$ x $27m$.

Annak érdekében, hogy az IPv6-ban megoldotthoz hasonló NEMO támogatást lehessen nyújtani a Host Identity Protocol alapú jövő Internet architektúrákban is, és a III.2. tézisben bemutatott fejlett NEMO mobilitási keretrendszer HIP alapokra is átültethető legyen, továbbfejlesztettem az I.3. tézisben bemutatott µHIP sémámat, és ráépítve létrehoztam egy új, HIP-alapú NEMO protokollt. Munkám előtt volt már néhány erre vonatkozó alapszintű megoldás (pl. [39]), de az általam definiált HIP-NEMO tekinthető az első teljes, és kizárólag HIP alapon működő hálózat-mobilitási technikának.

III.3. Tézis [C6], [C17], [B5], [J2], [J14], [J17] *Kifejlesztettem egy Host Identity Protocol alapú hálózat-mobilitási protokollt (HIP-NEMO), mely bevezeti a mobil randevúszerver (Mobile Rendezvous Point – mRVS) új hálózati entitást a HIP-képes mozgó hálózati csomópontok kezelésére. A javasolt rendszer megszünteti a felhasználói sík NEMO BS-ben ismert szuboptimális alagútjait, és hatékony mobilitás-kezelést biztosít a HIP alapú jövő Internet mozgó hálózatai számára. Megmutattam, hogy a*

javasolt HIP-NEMO séma felülmúlja a szabványos NEMO BS megoldást, és a szuboptimális alagutak speciális HIP jelzésrendszerre támaszkodó megszüntetésével akár 19%-kal kisebb csomagvesztés és 211%-os TCP átviteli nyereség is elérhető, melynek jelzésterhelésben megmutatkozó ára a HIP alapú jelzésdelegáció miatt megfizethető.

A HIP-NEMO új hálózati entitása a NEMO BS mobil routeréhez hasonló mRVS végzi el a NEMO hálózat mobilitás-kezelését, idegen hálózatokban való elérhetőségének biztosítását. Az mRVS ezen kívül egy jelzési proxy is az MNN-ek számára: az MNN-ek jelzési jogaikat az mRVS-hez delegálják, így az mRVS hatékonyan tudja kézben tartani az összes mobilitási szituáció kezelését. Kezdő lépésként az MNN-ek regisztrálják magukat az mRVS-hez, majd elvégzik a jelzésdelegációt a [28] [C21] cikkekben használt módszerek alapján (10. ábra, bal oldal). Az mRVS egy táblázatban kezeli az MNN-ek HIT-jét és a NEMO hálózatban érvényes IP címeiket ($IP1_{MNN}$). Ezt a bejegyzést az mRVS összeköti a külső kommunikációhoz általa az MNN-ekhez kirendelt IP címmel ($IP0_{MNN}$). Ennek a címnek a szerepe megegyezik a µHIP-ben már bemutatott hasonló IP cím szerepével: ez érvényes a NEMO-n kívül. Ezen kezdeti lépések és a delegáció sikeres lefuttatása után az mRVS elvégez minden szükséges jelzési feladatot az MNN nevében (CN és RVS regisztrációk, stb.).



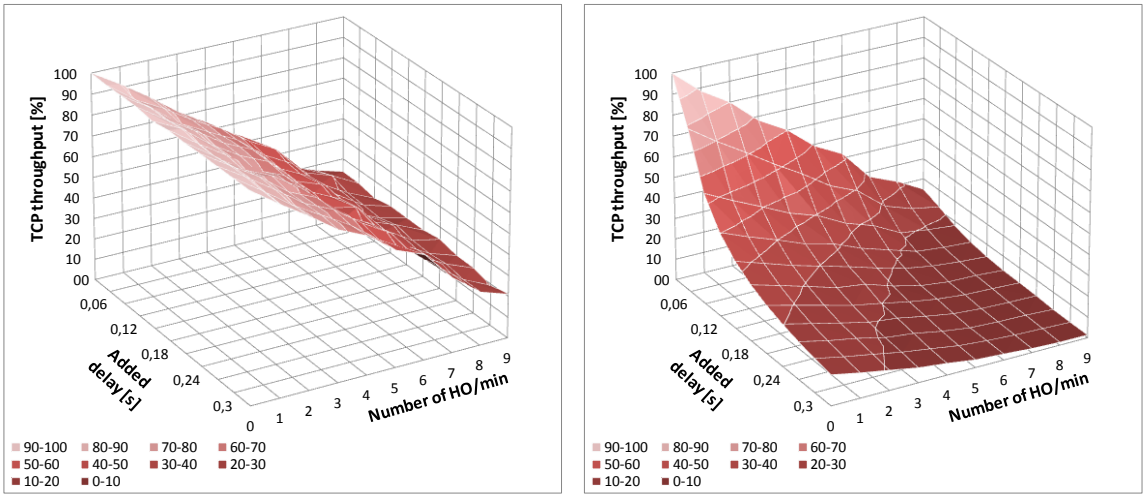
10. ábra: HIP-NEMO hálózat inicializáció (balra) és kapcsolat kialakítás (jobbra)

Az inicializáció megtörténte után az MNN-ek elérhetőek a NEMO-n belül bármely külső CN csomópont számára (10. ábra, jobb oldal). Az CN–MNN BEX folyamat első csomagja az MNN RVS-éhez jut, ami a HIP szabványok alapján az mRVS-hez kerül (hiszen az mRVS saját lokátorával regisztrálta az MNN-t az RVS-nél). Az I1 csomagot [7] az mRVS elfogja, céllokátorát pedig módosítja az MNN NEMO-n belüli IP címére. Végül az MNN megkapja az üzenetet, és válaszol az R1 üzenettel a HIP BEX szabályai alapján [7]. A forráslokátort az mRVS saját, globálisan elérhető címére cseréli, és közvetlenül a CN felé küldi, immár az RVS kihagyásával. A kapcsolatépítés befejeződik, az mRVS mediátor szerepe végig megmarad.

A hálózatváltások kezelése egyszerű a HIP-NEMO rendszerében: mivel az mRVS bírja az MNN csomópontok jelzési jogait, ezért képes a nevükben frissíteni RVS-eiket és CN-jeiket egyaránt. Az UPDATE csomagok a hálózatváltás közben módosult, új mRVS globális IP címet tartalmazzák LOCATOR mezőjükben.

A HIP-NEMO megoldás teljesítményvizsgálatát a NEMO BS szabványos módszerével, mint referenciával összehasonlítva végeztem el. Ennek érdekében az új protokollmodellek implementációjával továbbfejlesztettem a már bemutatott HIPSim++ szimulációs rendszert [C17].

A HIP-NEMO és NEMO-BS mérési forgatókönyvekhez egy-egy MNN-t és mRVS/MR entitásokat tartalmazó mozgó hálózatokat definiáltam. Ez a mozgó hálózat különböző IPv6 hálózatokba kötött Wi-Fi hozzáférési pontok között mozgott. A NEMO-BS esetén Home Agent (HA), míg a HIP-NEMO esetén RVS biztosította a makro-mobilitási ügynökfunkciókat. A szimuláció során a CN indítja az UDP és TCP kapcsolatokat az MNN felé, és egy speciális hálózati csomópont szimulációs paraméterrel szabályozza a HA/RVS-t tartalmazó otthoni hálózat és az idegen hálózatok közti késleltetést 0-300ms között. Az eredményeket a 11. és 12. ábrák foglalják össze, melyek mindegyike 10000 független mérési eredmény átlagát jeleníti meg.

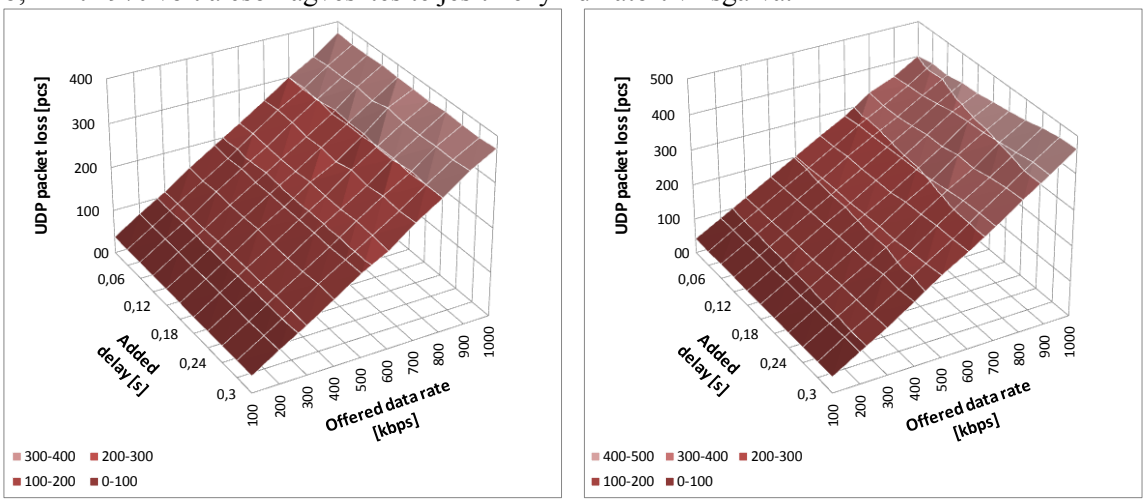


a) HIP-NEMO c) NEMO-BS

11. ábra: A TCP átvitel mérési eredményei

A TCP eredmények (11. ábra) mutatják, hogy a hálózatváltási frekvencia jelentős hatással van mindkét vizsgált protokollra: az átvitel jelentősen romlik, ha nő az átviteli időszakban végrehajtott hálózatváltások száma. Azonban az is látható, hogy a NEMO-BS esetén a teljesítménycsökkenés sokkal jelentősebb, mint a HIP-NEMO esetben. Az általam javasolt HIP alapú megoldásban az MNN és a CN az optimálishoz közeli útvonalon kommunikál, és elhagyja a felhasználói síkban működő alagutakat is. Ennek köszönhetően a HIP-NEMO MNN–CN átvitele számára nem érzékelhető az otthoni és az idegen hálózatok közötti topológiai távolság hatása, ami kb. 211%-os összesített nyereséget jelent a vizsgált körülmények közötti TCP átvitel során.

Az UDP mérések eredményei (12. ábra) tovább erősítik ezt a megfigyelést. A hálózatváltás hatása HIP-NEMO esetében független a mozgó hálózat otthoni hálózattól való távolságától, míg NEMO-BS esetén ez jelentős tényező. A HIP-NEMO átlagos nyeresége magas UDP küldési ráta esetén valamivel több, mint 19% volt a csomagvesztés teljesítményindikátort vizsgálva.



a) HIP-NEMO c) NEMO-BS

12. ábra: Az UDP csomagvesztés mérési eredményei

4.4. Elosztott és flat mobilitás-kezelési sémák

A távközlési ipar széles körben elfogadott előrejelzései alapján állítható, hogy napjaink centralizált mobil Internet architektúrái nem lesznek képesek kielégíteni az egyre növekvő mobil szélessávú forgalom által támasztott követelményeket [1]. Az architektúráknak és a társult protokolloknak is át kell alakulniuk úgy, hogy a felhasználói horgonypontokat a mobil felhasználók közelébe helyezett, hagyományos IP eszközök váltsák fel. Decentralizált, robusztus, önkonfiguráló és

önoptimalizáló sémák megjelenése várható, melyek csökkentik a működési költségeket, javítják a rendszer áteresztőképességét és energiahatékonyságát. A maghálózati skálázhatóság javítása érdekében Khadija Daoud és szerzőtársai bevezették az Ultra Flat Architecture hálózat felépítési paradigmát [5], mely az UFA GW nevű entitással váltja ki a ma ismert különböző hálózati csomópontokat úgy, hogy ebbe a hálózat szélére, a felhasználókhoz közel telepített UFA GW-be osztja szét a felhasználói és vezérlési sík tradicionális funkcióit. Javaslatuk fontos jellemzője, hogy a hálózatváltásokat az IP Multimedia Subsystem (IMS) [C20], [J5] keretrendszerét felhasználva Session Initiation Protocol (SIP) segítségével kezelik. Bár a SIP kiváló megoldás az UFA jelzésrendszeréül, nem transzparens: mivel az alkalmazási rétegben működik, ezért non-SIP alkalmazásokat (vagyis a hagyományos Internet alkalmazásokat) nem támogatja, és nem felel meg teljes mértékben az ITU-T által a jövő mobil Internet architektúráihoz ajánlott ID/Loc szeparációs követelményeknek sem [6].

Ez motiválta kutatócsoportunkat, mikor elkezdtük egy alternatív UFA jelzési séma kidolgozását az ígéretes Host Identity Protocol-ra támaszkodva. A HIP alapú Ultra Flat Architecture (UFA-HIP) kialakításában az én hozzájárulásom három területet ölel át. Egyrészt a nevemhez fűződik a HIP mobilitás-kezelésen, jelzésdelegáción, kontextus-átvitelen és cross-layer együttműködésen alapuló keretrendszer kidolgozása a főbb funkcionális elemek definiálásával, azok struktúrájának kialakításával és jelzési síkban betöltött szerepével. Másrészt én hoztam létre a proaktív, elosztott, 802.21 MIH / HIP alapú hálózatváltást inicializáló, előkészítő, végrehajtó és azt befejező protokollt. Harmadrészt végrehajtottam ennek az UFA-HIP mobilitás-menedzsment sémának a szimulációs teljesítményelemzését. Az általános célokra is használható HIP jelzésdelegációs szolgáltatások, az L2 és L3 kapcsolódási mechanizmusok, a kapcsolat kialakításának (session establishment) vezérlő protokollja, és a SIP-pel kiegészített hálózatváltási alternatíva szerzőtársam, Faigl Zoltán eredményei.

IV.1. Tézis [C21], [C22], [J6], [J9], [J12], [J13] *Kidolgoztam egy Hosti Identity Protocol alapú Ultra Flat Architecture rendszerarchitektúrát (UFA-HIP), mely teljesen megszünteti Point of Access (PoA) és CN entitások közötti központosított IP csomópontokat, a hálózati funkciókat a hálózat szélére (a PoA eszközök topológiai közelségébe) helyezi egy UFA-HIP GW nevű elosztott entitást használva, integrálja a 802.21 MIH és HIP funkciókat a hatékony inter-GW mobilitás-kezelés érdekében, valamint jelzésdelegációt és kontextus-átvitelt használ a HIP BEX folyamatok számának és a rádiós interfész jelzési terhelésének csökkentéséhez.*

A javasolt HIP alapú Ultra Flat Architektúra (UFA-HIP) keretrendszer hét főbb építőelemet definiál (13. ábra): 1) különböző vezetékes és vezeték nélküli hozzáférési hálózatok, 2) IP/MPLS tranzithálózat, 3) a hálózati funkciókat vezérlő és kezelő HIP-képes UFA GW átjárók (UFA-HIP GW), 4) optimalizált kapcsolódási séma és cross-layer hozzáférés-engedélyező protokoll, 5) kapcsolat-kialakító megoldás, 6) IEEE 802.21 Media Independent Handover (MIH) szabványt [40] és kiegészített HIP funkcionalitásokat használó hálózatváltást inicializáló, előkészítő, végrehajtó és azt befejező protokoll, és 7) HIP vezérlő hálózat.

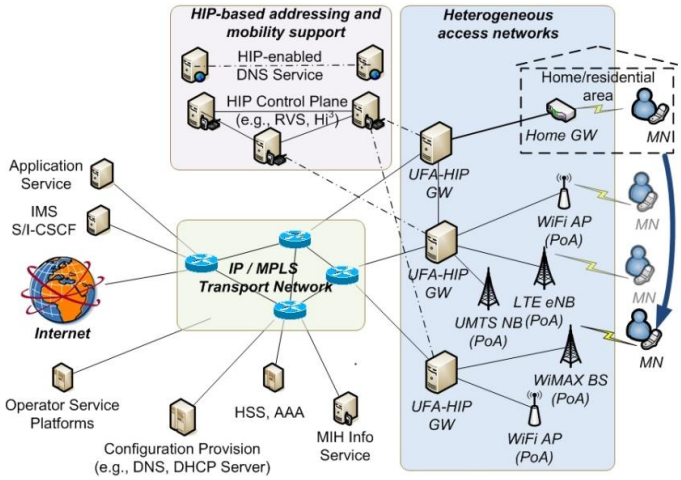
A heterogén hozzáférési hálózatok biztosítják az MN csomópontok csatlakozását. Az IP/MPLS tranzit hálózat az operátor gerinchálózati elemeit, routereit tartalmazza (szolgáltatás és konfiguráció-nyújtás, 802.21 szolgáltatások, stb.), és natív módon csatlakoztatja az UFA hálózatot a globális Internet gerinchálózathoz.

Ebből a rendszerből teljes mértékben hiányoznak a PoA és CN csomópontok közötti centralizált IP horgonypontok, mivel a hálózati funkciók kikerültek a felhasználók közelébe telepítendő UFA-HIP GW entitásokba. A megoldás HIP-et használ az MN és UFA-HIP GW valamint UFA-HIP GW és UFA-HIP GW elemek közti IPsec Security Association (SA) alapú biztonságos kapcsolatok kiépítésére és fenntartására. Az IP-szintű hálózatváltások HIP delegációs szolgáltatások [C21] és CXTP alapú kontextus átvitel [41] segítségével kerülnek kezelésre. Javaslatom az alábbi UFA-HIP GW funkciókat különíti el:

1. Gyors, cross-layer támogatott (L2 és HIP-szintű) hozzáférés-engedélyezés.
2. Aktív interakció az MN-ekkel delegáció alapú HIP és IPsec kapcsolat-menedzsmenttel és kontextus átvitellel optimális üzenettovábbítás, valamint UFA mobilitás- és multihoming-kezelés érdekében. (A javasolt keretrendszer hop-by-hop átvitelt alkalmaz MN–CN viszonylatban, ahol a közbülső csomópontok, az UFA-HIP GW entitások, a peer csomópontok meghatalmazottjai.)

3. Aktuális leképzés/útválasztás kezelése a “külső fejléc” IPsec alagútja és a “belső fejléc” azonosítói között.
4. Erőforrás-kezelés, terheléselosztás és hálózatváltási döntések meghozatala az UFA-HIP cross-layer modulban (MIH taxonómia alapján a MIHU elemben).

Az általam kidolgozott keretrendszerben a HIT-ek azonosítják a folyamokat az UFA-HIP GW átjárókban, a Control Plane Header (CPH) [42]-ben leírt feladataihoz hasonlóan. Delegáció nélkül a végpont-végpont SA-k minden kommunikáló felet érintő kezelésére lenne szükség, ahogy azt a SPINAT rendszer jvasolja [42].



13. ábra: UFA-HIP: A kidolgozott HIP alapú Ultra Flat Architektúra rendszerterve

Vannak olyan kontroll funkciók is, melyek nem kerültek az UFA-HIP GW csomópontokban elosztásra, és a maghálózatban maradtak. Ilyen funkció pl. az IP Multimedia Subsystem (IMS), a Home Subscriber Server (HSS), az Authentication, Authorization, Accounting (AAA) szerver, a szolgáltatás- és konfiguráció-nyújtás (pl. DHCP segítségével), valamint a Media Independent Information Service (MIIS). Ezen funkciók optimális elhelyezése további kutatások témája. A létező szolgáltatási platformok és alkalmazás-szerverek továbbra is központosítottak.

Az IEEE 802.21 MIH menedzsment alrendszer kezeli a hálózatváltás előkészítésének feladatait és a vonatkozó jelzéseket a proaktív HIP hálózatváltás támogatásához és a hálózat vagy mobil vezérelt hálózatváltási döntések meghozatalához. A javasolt keretrendszer hálózat által inicializált 802.21 hálózatváltásokat támogat, melyeket a kiszolgáló UFA-HIP GW triggerel (lásd C.2 függelék [40]-ben.)

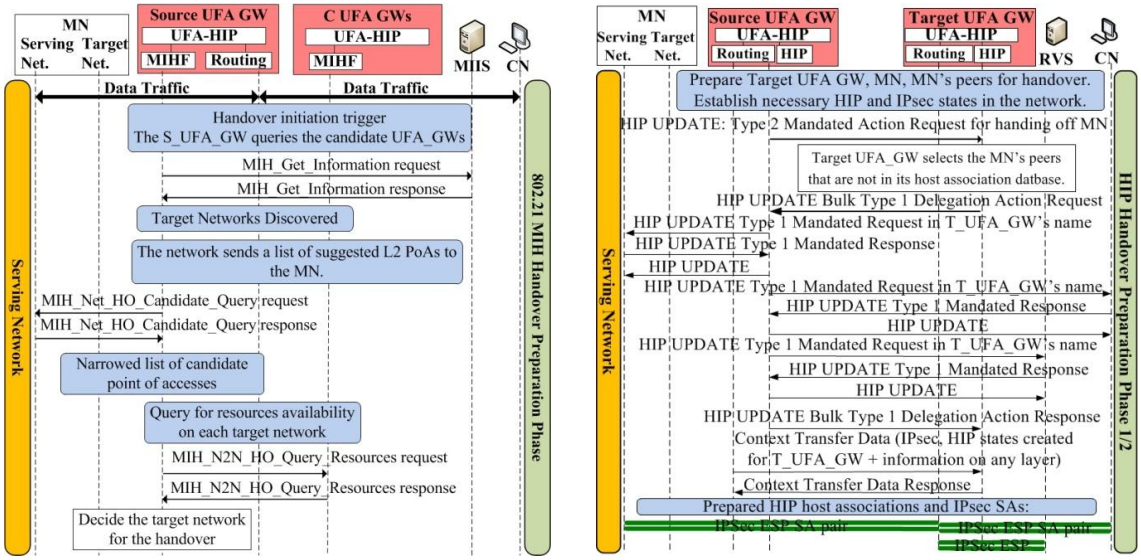
A kontroll hálózat (HIP alapú címzés és mobilitás-kezelés) egy HIP-kompatibilis Domain Name System architektúrát [43] és egy elosztott HIP vezérlési síkot tartalmaz, tárolja és elosztja a gyakran változó ID-Loc kötési információkat az UFA-HIP valamennyi mobil berendezése számára. Ez a vezérlési sík implementálható hagyományos RVS szerverpark segítségével, de a Hi^3 -hoz [44] hasonló elosztott HIP jelzési architektúra is használható.

HIP BEX és UPDATE folyamatok kezelik az IPsec SA-k dinamikus kialakítását az MN és UFA-HIP GW csomópontok között a felhasználói adatok védelme és a kölcsönös MN-hálózat hitelesítés érdekében. A rendszer a hálózatváltás előkészítése, inicializálása során kezeli a proaktív HIP mechanizmusokat és hálózat vagy mobil által vezérelt döntést is támogat. A hálózatváltás végrehajtását a forrás UFA-HIP GW (S UFA GW) kezdi. A HIP és IPsec kontextusok proaktív módon jönnek létre a cél (T UFA GW) átjáró és a mobil levelezőpartnerei között, valamint a T UFA GW és a mobil között, az S UFA GW aktív közbenjárásával. Mindez annak köszönhetően oldható így meg, hogy az MN és a T UFA GW delegálta jelzési jogait az S UFA GW számára. Context Transfer Protocol [41] kerül alkalmazásra a HIP és IPsec kontextusok S UFA GW csomópontról a T UFA GW és MN csomópontokra történő mozgatásához. Mikor a kontextus-adatok megérkeztek rendeltetési helyeikre, a rendszer informálja az MN-t arról, hogy a csatlakozhat az új PoA elemhez, vagyis a sikeres előkészületek után végrehajthatja a fizikai hálózatváltást.

IV.2. Tézis [C21], [C22], [J6], [J9] *Létrehoztam egy proaktív, elosztott, 802.21 MIH és HIP alapú hálózatváltást inicializáló, előkészítő, végrehajtó és azt befejező protokollt az UFA-HIP keretrendszer számára. A javasolt technológia támogatja a flat hálózati architektúrákat, minimalizálja a felhasználói forgalom végpont-végpont távolságát, valamint a felhordó- és maghálózati szegmensekben tartja a mobilitás-kezelés okozta jelzésterhelést.*

A javasolt elosztott mobilitás-menedzsment séma feltételezi, hogy az MN élő regisztrációval bír a hálózat felé, élő regisztráció van a forrás és cél UFA-HIP GW csomópontok között, létezik egy speciális algoritmus, ami dönt és triggereli a hálózatváltást az egyik jelölt UFA-HIP GW felé (C UFA GW) az S UFA GW-hez tartozó PoA kapcsolat elvesztése előtt, valamint már lefutott a beállítási fázis, melyben az UFA GW a MIH funkciókat [40] használva, és azokra támaszkodva beállította a QoS küszöbértékeket az MN számára.

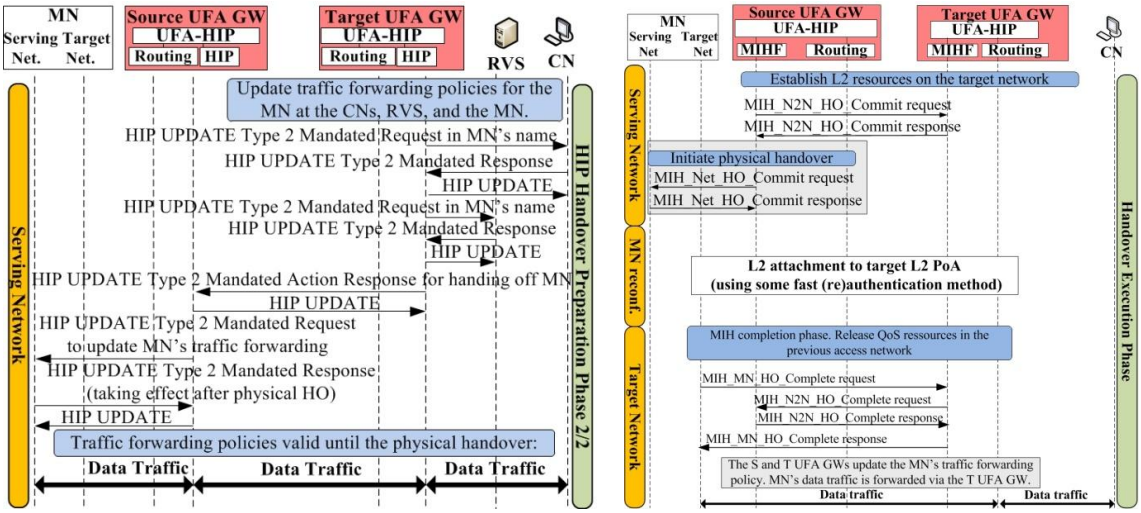
A trigger üzenet fogadása indítja a 802.21 MIH hálózatváltás inicializációt (14. ábra, bal oldal), mely az alábbi rész-fázisokból áll. (1) Felfedezés (Discovery): a C UFA GW-k egy listája kerül beszerzésre a 802.21 Media Independent Information Service (MIIS) [40] entitáson keresztül. (2) Lekérés (Query): a mobilitás-kezelés döntési algoritmusa beszerez minden QoS jellemzőt az elérhető C UFA GW-ről. (3) Kiválasztás (Selection): a mobilitás-kezelés döntési algoritmusa (mely futhat a hálózat vagy a mobil oldalán egyaránt) választ egy T UFA GW-t a C UFA GW-k listájából. Az S UFA GW lekéri a szomszédos hálózatokról szóló információkat a MIIS-től, majd megkéri az MN-t, hogy szűkítse ezt a listát, végül ellenőrzi a rendelkezésre álló erőforrásokat minden C UFA GW-re vonatkozóan. Ezután dönt a T UFA GW csomópontról, ami a hálózatváltás célhálózatát azonosítja.



14. ábra: 802.21 MIH hálózatváltás inicializáció (balra) és HIP hálózatváltás előkészítési fázis 1/2 (jobbra)

A T UFA GW és a hozzá tartozó cél PoA kiválasztása után proaktív módon hozza létre az S UFA GW a szükséges HIP és IPsec kontextusokat a Type 1 és Type 2 típusú HIP jelzésdelegációs szolgáltatásokra támaszkodva [C21], a HIP hálózatváltás előkészítési fázisában. A 14. ábra jobb oldalán látható, hogy az S UFA GW egy Type 2 Mandated Action Request üzenetben inicializálja az MN folyamatainak hálózatváltását az MN nevében. Ez egy bulk Type 1 Delegation Action Request üzenet küldését triggereli, melyben a T UFA GW felhatalmazza az S UFA GW-t, hogy az a T UFA GW nevében létrehozhassa a HIP és IPsec kontextusokat az MN levelező partnerei és a T UFA GW között. Ezután az S UFA GW a CXTP protokollt és IPsec védelmet használva átküldi a létrehozott kontextusokat a T UFA GW-re, így a HIP BEX procedúrák száma csökken és HIP UPDATE-re cserélődik. A sikeres kontextus átvitel után a T UFA GW frissíti az MN-re vonatkozó továbbítási szabályokat a CN csomópontoknál és az RVS rendszerben, majd az MN-en (15. ábra, bal oldal). Először Type 2 Mandated Action Request üzeneteket küld a T UFA GW az MN nevében a CN csomópontok és az RVS rendszer felé. Az MN partnereinek frissítése után a T UFA GW egy Type 2 Mandated Action Response üzenetben tájékoztatja az S UFA GW-t a futó folyamatok átirányítására való felkészülésről. A T UFA GW frissíti a HIT alapú forgalom-továbbítási táblákat [J6], hogy

fogadni tudja az MN felé irányuló csomagokat, és azokat az S UFA GW felé továbbítja. Az S UFA GW szintén frissíti az MN és a saját HIT alapú forgalom-továbbítási tábláit: az MN felől érkező forgalmat át kell rakni abba az IPsec alagútba, melynek a T UFA GW van a másik felén. Az MN késlelteti saját továbbítási táblájának frissítését: az MN forgalma csak akkor fog közvetlenül a T UFA GW csomóponton áthaladni, ha a fizikai hálózatváltás is befejeződött.



15. ábra: HIP hálózatváltás előkészítési fázis 2/2 (balra) és Hálózatváltás végrehajtási/befejezési fázis (jobbra)

A 15. ábra jobb oldalán látható a javasolt UFA-HIP hálózatváltási séma végrehajtási/befejezési fázisa. Miután befejeződött a HIP hálózatváltás előkészítési fázis, a MIH_N2N_HO_Commit és MIH_Net_HO_Commit request 802.21 MIH üzenetek [40] inicializálják az L2 hálózatváltás végrehajtási folyamatát a T UFA GW és az MN irányában. Ezután az MN L2 eszköze csatlakozik a cél PoA entitáshoz. Az utolsó fázist az MN inicializálja, mikor fizikailag is sikeresen csatlakozott a cél L2 PoA és T UFA GW csomópontokhoz: az MN közli a T UFA GW elemmel, hogy a hálózatváltás sikeres volt és az S UFA GW és forrás L2 PoA felszabadíthatja az MN folyamjaihoz rendelt erőforrásokat. Ez az utolsó lépés a 802.21 MIH protokoll MIH_MN_HO_complete folyamatával kerül végrehajtásra. Végezetül frissíteni kell az MN-ben lévő továbbítási szabályokat, valamint a forrás és cél UFA GW elemek továbbítási tábláit annak érdekében, hogy az S UFA GW kikerüljön a továbbítási útvonalból.

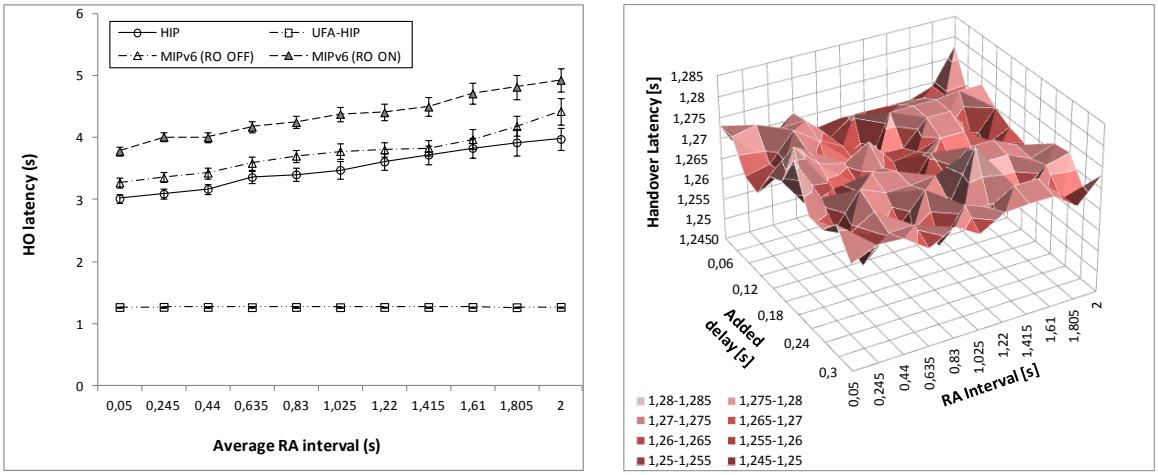
A javasolt séma teljesítményvizsgálata az INET/OMNeT++ alapú, nyílt forráskódú HIPSim++ HIP szimulációs modell [C17] kiegészített változatában történt.

IV.3. Tézis [C17], [J14], [J17] *Megmutattam, hogy a javasolt proaktív HIP-UFA mobilitás-kezelési séma átlagban 67%-kal csökkenti a hálózatváltási késleltetést, és így majdnem teljesen kiküszöböli az elosztott és flat mobil hálózati architektúrákban gyakori inter-GW hálózatváltások negatív hatásait. Szimulációs vizsgálataimmal megvilágítottam módszerem felsőbb rétegbeli (UDP és TCP) alkalmazások teljesítményére gyakorolt pozitív hatásait is. Az elosztott megoldás átlagban 55%-kal kevesebb csomagvesztést okoz az UDP szintjén, és a TCP átvitelben mért átlagos nyereség eléri a 60%-ot.*

Referenciaként a szabványos HIP és MIPv6 mobilitás-kezelési megoldásokat használtam: az MN Wi-Fi hozzáférési pontjait változtatva módosítja PoA-ját mozgása közben, és az így bekövetkező lokátorváltozásokat a HIP és a MIPv6 megoldásai kezelik le. HIP esetben az RFC 5206 szabványban rögzített HIP UPDATE procedúra [9], míg MIPv6 esetben a szabványos Binding folyamat [2] végzi ezt a feladatot. Az utóbbi esetben a routing optimalizáció (return routeability) bekapcsolt (RO ON) és kikapcsolt (RO OFF) állapota két alesetet eredményez.

Az UFA-HIP forgatókönyv UFA-HIP GW csomópontokra cseréli a hagyományos hozzáférési útválasztókat és ezek vezérlik a PoA-kat. Ebben az esetben az MN jel/zaj arány (SNR) méréseket végez, és egy küszöbérték átlépésekor triggereli a hálózatváltás inicializációját. A HIP funkciók

(jelzésdelegáció és kontextus átvitel) a HIPSim++ rendszerben kerültek implementálásra, míg a 802.21 MIH keretrendszer modellje az INET/OMNeT++ Notification Board eszköztárára épül [45].

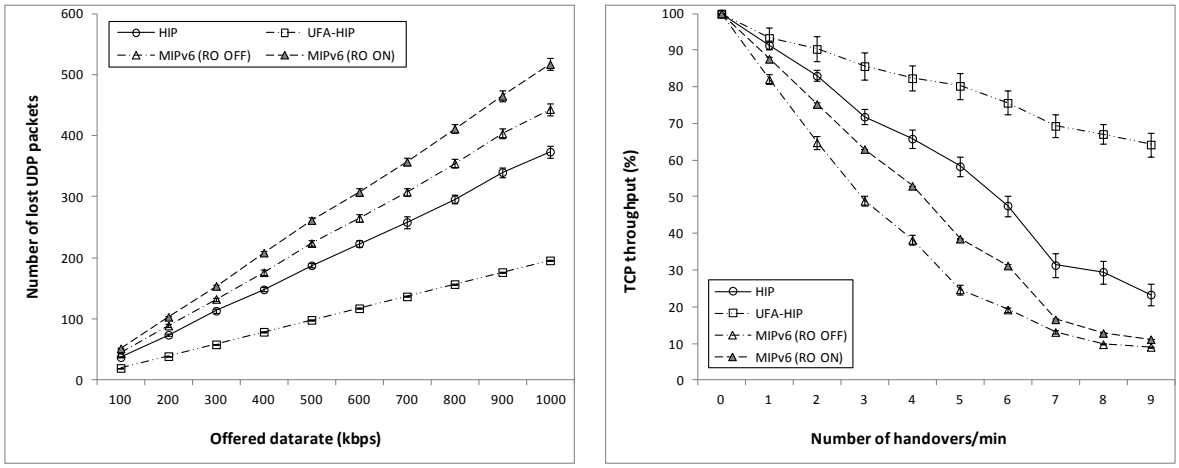


a) HO késleltetés vs. RA intervallum b) HO késleltetés vs. S és T UFA GW közti távolság

16. ábra: Hálózatváltási késleltetés az UFA-HIP sémában

Szimulációs futásonként 100 független hálózatváltási eseményt generáltam az MN mozgásával, és három kulcs teljesítmény-indikátort mértem három különböző alesetben. A 16/a ábra 99%-os konfidencia intervallumban ábrázolja a hálózatváltási késleltetést úgy, hogy minden RA intervallumra 100 hálózatváltási sorozat került feldolgozásra protokollonként. A mérési eredmények bizonyítják, hogy az UFA-HIP hálózatváltási séma független az IP réteg mechanizmusaitól (vagyis az új hálózaton történő IP címszerzéstől, DAD ellenőrzéstől, stb.), és 1 másodperc körül tartja a hálózatváltás miatti szolgáltatás megszakadás hosszát. Az eredmények azt mutatják, hogy az UFA-HIP hálózatváltási késleltetés független a célhálózaton tapasztalható konfigurációs folyamatok időigényétől (RA intervallum ebben az esetben), és a fejlett, proaktív működésnek köszönhetően átlagban 67%-kal kevesebb, mint a referenciaprotokollok esetében.

A 16/b ábrán a hálózatváltási késleltetés az RA intervallum és az S és T UFA GW csomópontok topológiai távolságának függvényében került megjelenítésre. Látható, hogy a javasolt proaktív séma független a forrás- és célhálózatok közötti késleltetés értékétől, ami lényeges protokolljellemző.



a) UDP csomagvesztés egyetlen HO alatt b) TCP átvitel vs. HO/perc

17. ábra: UDP és TCP alkalmazások teljesítménye az UFA-HIP hálózatváltási protokoll használatakor

A 17/a ábra mutatja a HIP, MIPv6 RO ON, MIPv6 RO OFF, és UFA-HIP technológiák által végrehajtott hálózatváltások okozta UDP csomagvesztés nagyságát, 99%-os konfidencia intervallumban, minden UDP küldési rátára végzett 100 független hálózatváltási eseményt alapul véve. A vizsgált protokollok hálózatváltási teljesítménye kiválóan megfigyelhető az UDP szintjén is. A

javasolt proaktív, kontextus átvitelre építő, elosztott megoldás átlagban 55%-kal kevesebb csomagvesztést okoz az UDP szintjén, mint a hagyományos HIP és MIPv6 mobilitás-kezelési technológiák.

A TCP-re végzett mérések a 17/b ábrán vehetők szemügyre: a grafikon azt ábrázolja, hogy egy egyperces kommunikációs folyamatban mekkora a TCP átvitel nagyságának egymáshoz viszonyított aránya különböző hálózatváltási frekvenciák (0-9 HO/perc) esetén. A javasolt UFA-HIP megoldás nyeresége szembetűnő, főleg a nagy HO frekvenciák esetén: 9 HO/perc esetben 175%-os a TCP átvitelben mért nyereség, míg az összes HO frekvencia esetre vett átlagos nyereség is eléri a 60%-ot.

Kiterjedt szimulációs vizsgálataimmal bizonyítottam, hogy a javasolt UFA-HIP hálózatváltási protokoll jelentősen csökkenti a hálózatváltás okozta szolgáltatás-kimaradás idejét és így az UDP csomagvesztés mértékét, valamint növeli a TCP átviteli teljesítményt. Mindez azt jelenti, hogy az elosztott UFA-HIP GW csomópontok által biztosított kiterjesztett skálázhatóság releváns növekményt jelent a hálózatváltások kezelésében is.

5. Az eredmények alkalmazása és továbbfejlesztési lehetőségek

A lokalizált vagy mikro-mobilitás bevezetése, a felhasználók helyzetinformáció-védelme, a hálózat-mobilitás és az elosztott mobilitás-kezelés támogatása fontos kérdések és egyben megoldandó mobilitási forgatókönyvek napjaink IP alapú modern távközlési rendszereiben. Doktori értekezésemben ezen forgatókönyvekhez javasoltam új sémákat, protokollokat és algoritmusokat azért, hogy a hagyományos megoldások teljesítménye és a mobil alkalmazások minősége egyaránt javuljon.

A kidolgozott anycast alapú mikro-mobilitási keretrendszer és a hozzá fejlesztett anycast subnet tervező algoritmus könnyen telepíthető, transzparens, hop-by-hop útválasztáson alapuló, de mégis skálázható opció mikro-mobilitás megoldására. Azonban módszerem gyakorlati használatához szükség lenne az IPv6 anycasting routing és csoportmendzsment protokolljainak szabványosítására, amit egyelőre még nem végeztek el a szabványosító szervezetek. Ezen protokollok szabványosítása mellett fontos előrelépés lehetne a szabványosítás során felmerülő tervezési kérdések (pl. az ABMF módszer esetében lényeges konvergenciaidőt befolyásoló technikák használati módjainak) tudományos vizsgálata, körüljárása.

A felhasználók helyzetinformációinak védelmét fokozó hálózattervező algoritmusok bemutatott variánsai kiváló eszköznek bizonyulhatnak az operátorok kezében a mikro-mobilitási tartományok tervezési és elosztott/flat rendszerek GW elhelyezési kérdéseinek felhasználói privátszférát is erősítő megválaszolásában. A domain tervezés különösen izgalmas kérdés a jövő elosztott és flat mobil hálózataiban, hiszen az IP címváltások előfordulása igen gyakori lehet ezekben a heterogén architektúrákban. Az IP címektől függő helyzetinformáció szivárgás és az emiatti fenyegetettség így a jövőben nagyobb figyelmet kaphat, ám ehhez szükség van a felhasználói nyitottságra, magasabb fokú privátszféra-tudatosságra, és nem utolsó sorban operátori és szabályozói akaratra is, hiszen ez a PET technológia a hálózattervezési fázisban alkalmazható leginkább. Továbbfejlesztési lehetőségként adódik a piko- és femtocellás rendszerekre történő optimalizálás, és az egyes algoritmus variánsok integrációja egy komplex, általánosabb felhasználású tervezősémába.

A javasolt helyzetinformációval segített, proaktív, multihoming környezetekhez tervezett NEMO MCoA keretrendszer és hálózatváltási módszer kiegészíti a szabványos NEMO BS megoldást és egyesíti az MCoA előnyeit a predikció alapú, cross-layer optimalizált menedzsmentben rejlő lehetőségekkel. Megmutattam, hogy megfelelő elrendezés esetén az előrejelzési motor mentes lesz mérési eredmények hibás tárolásának problémájától, ami így a javasolt sémát egy megbízható és praktikus, átlapolódó rádiós lefedettségekben különösen hatékony NEMO BS kiterjesztéssé teszi. A séma az EUREKA Celtic BOSS projektben [46] fő mobilitás-kezelési megoldásként szolgált, és a konzorcium által kialakított, vonatok vezeték nélküli videós távfelügyeletét ellátó rendszer központi eleme volt és ott implementációra is került. Továbbfejlesztési lehetőség az ITS/C-ITS rendszerekbe valló illesztése, szabványosítása. A kooperatív járműkommunikációs rendszerekben szabványosítás alatt álló Local Dynamic Map (LDM) koncepció kiváló felület lehet a GNSS alapú predikciókhoz, a szabványosítás pedig megoldaná a gyakorlati bevezetés nehézségeit.

Az állomásazonosító és helymeghatározó (ID/Loc) funkciók különválasztása a jövő Internetének egyik fontos evolúciós útja. A Host Identity Protocol egy olyan biztonsági megoldás, mely valós,

kriptografikus ID/Loc elkülönítést, IP mobilitás-kezelést és multihoming támogatást nyújt. A HIP-képes csomópontok és alkalmazások állandó vagy ideiglenes azonosítókat kapnak, IP címüket pedig csak valódi címzési célokra használják. A mobilitás-kezelés így rejtve maradhat a transzport és az alkalmazási rétegek elől. A jelenlegi 3GPP hálózatokban a non-3GPP hozzáférés IKEv2 és IPsec protokollokkal védett. A HIP kiváló alternatívája lehet az IKEv2-nek, ha L3 szintű újra-hitelesítési és IPsec SA kiépítési teljesítménye meghaladja elődjéét. Az észrevétlen hálózatváltás non-3GPP hozzáférések között nem megoldott a jelenlegi 3GPP szabványokban, holott a HIP segítségével ez hatékonyan támogatható lenne. Decentralizált és flat architektúrákban, melyek nagyszámú elosztott PGW jellegű hálózati elemet tartalmaznak, az intra-3GPP mobilitási esetek gyakori inter-PGW mobilitást jelentenek. Éppen emiatt jelentős az UFA-HIP elosztott mobilitás-kezelési módszere, és ezért játszhat minden HIP rétegben működő mobilitás-kezelési kiegészítés (pl. μHIP, HIP-NEMO) jelentős szerepet a jövő mobil Internet architektúráiban. Mindazonáltal a HIP technológiák bevezetése a jelenlegi és a jövőbeli mobil architektúrákba nem triviális feladat: a TCP/IP protokoll stack strukturális felépítését érintő változtatás komoly telepítési problémákat okoz, melyet meg kell oldani a HIP alapú hálózati megoldások bevezetéséhez. Léteznek persze áthidaló megoldások: a HIP delegációs szolgáltatások esetén a HIP-et nem használó csomópontok támogatása például HIP proxy entitások rendszerbe integrálásával [47] megoldható. Zöldmezős architektúráknál azonban nincs ilyesmire szükség, és ezt használta ki az EUREKA Celtic-Plus MEVICO projekt [48], mely alapvető építőkövei közé emelte az UFA-HIP technológiát, így képezve egy alternatív megoldást a mobil hálózati forgalom robbanásszerű növekedésének kezelésére és az egyéni felhasználói élmény fokozására. Fontos továbbfejlesztési irányt jelent HIP alapú javaslataim számára a virtuális, programozható mobilhálózatokba (Software Defined Mobile Network – SDMN) történő integráció vizsgálata, az OpenFlow protokollal való együttműködés kérdéseinek tárgyalása. Ehhez szorosan kapcsolódik a mobilitás-kezelési protokollok szerepének és funkcióinak általános átértékelése az SDMN hálózatok terjedésével: a programozhatóság és a forgalomkezelési irányelvek valós idejű optimalizálásának lehetősége a mobilitás-kezelési paradigmákat is alapvetően befolyásol(hatja) majd a jövőben.

Hivatkozások

[1] CISCO, “Global mobile data traffic forecast update, 2013–2018.” Tech. rep., Cisco VNI White Paper, Feb-2014.

[2] C. Perkins, D. Johnson, and J. Arkko, *Mobility Support in IPv6*. IETF, 2011.

[3] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier, *Hierarchical Mobile IPv6 (HMIPv6) Mobility Management*. IETF, 2008.

[4] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, *Network Mobility (NEMO) Basic Support Protocol*. IETF, 2005.

[5] K. Daoud, P. Herbelin, and N. Crespi, “UFA: Ultra Flat Architecture for high bitrate services in mobile networks,” in *Personal, Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on*, 2008, pp. 1–6.

[6] ITU-T, “General requirements for ID/locator separation in NGN, ITU-T Y.2015 (Y.ipsplit).” ITU-T Draft Recommendation, 06-Feb-2009.

[7] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, *Host Identity Protocol*. IETF, 2008.

[8] R. Moskowitz and P. Nikander, *Host Identity Protocol (HIP) Architecture*. IETF, 2006.

[9] P. Nikander, T. Henderson, C. Vogt, and J. Arkko, *End-Host Mobility and Multihoming with the Host Identity Protocol*. IETF, 2008.

[10] J. Laganier and L. Eggert, *Host Identity Protocol (HIP) Rendezvous Extension*. IETF, 2008.

[11] X. He, D. Funato, and T. Kawahara, “A dynamic micromobility domain construction scheme,” in *Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE Proceedings on*, 2003, vol. 3, pp. 2495–2499 vol.3.

[12] V. Simon and S. Imre, “A Simulated Annealing Based Location Area Optimization in Next Generation Mobile Networks,” *Mob. Inf. Syst.*, vol. 3, no. 3,4, pp. 221–232, Dec. 2007.

[13] E. Cayirci and I. F. Akyildiz, “Optimal location area design to minimize registration signaling traffic in wireless systems,” *Mobile Computing, IEEE Transactions on*, vol. 2, no. 1, pp. 76–85, Jan. 2003.

[14] N. Montavont, T. Noel, and T. Ernst, “Multihoming in nested mobile networking,” in *Applications and the Internet Workshops, 2004. SAINT 2004 Workshops. 2004 International Symposium on*, 2004, pp. 184–189.

[15] V. P. Kafle, E. Kamioka, and S. Yamada, “MoRaRo: Mobile Router-Assisted Route Optimization for Network Mobility (NEMO) Support,” *IEICE - Trans. Inf. Syst.*, vol. E89-D, no. 1, pp. 158–170, Jan. 2006.
[16] T. K. Tan and A. Samsudin, “Efficient NEMO security management via CAP-KI,” in *Telecommunications and Malaysia International Conference on Communications, 2007. ICT-MICC 2007. IEEE International Conference on*, 2007, pp. 140–144.
[17] Y.-H. Wang, K.-F. Huang, and H.-Y. Ho, “A Seamless Handover Scheme with Pre-registration in NEMO,” in *Advanced Information Networking and Applications Workshops, 2009. WAINA ’09. International Conference on*, 2009, pp. 338–344.
[18] C.-M. Huang, C.-H. Lee, and J.-R. Zheng, “A Novel SIP-Based Route Optimization for Network Mobility,” *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 9, pp. 1682–1691, Sep. 2006.
[19] P. Bertin, S. Bonjour, and J.-M. Bonnin, “Distributed or Centralized Mobility?,” in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 2009, pp. 1 –6.
[20] V. Simon and S. Imre, “Location Area Design Algorithms for Reducing Signalling Overhead in Mobile Networks,” in *3rd Inter. Conf. On Advances in Mobile Multimedia, MoMM’05*, Kuala Lumpur, Malaysia, 2005, pp. 365–375.
[21] A. Varga and R. Hornig, “An Overview of the OMNeT++ Simulation Environment,” in *Proceedings of the 1st International Conference on Simulation Tools and Techniques for Communications, Networks and Systems & Workshops*, ICST, Brussels, Belgium, Belgium, 2008, pp. 60:1–60:10.
[22] S. Doi, S. Ata, H. Kitamura, and M. Murata, “IPv6 anycast for simple and effective service-oriented communications,” *Communications Magazine, IEEE*, vol. 42, no. 5, pp. 163–171, May 2004.
[23] Z. Zhou, G. Xu, J. He, J. Jiang, and C. Deng, “Research of Secure Anycast Group Management,” in *Networked Computing and Advanced Information Management, 2008. NCM ’08. Fourth International Conference on*, 2008, vol. 1, pp. 604–608.
[24] Y. Wang, L. Zhang, Z. Han, and W. Yan, “Anycast extensions to OSPFv3,” in *Parallel and Distributed Systems, 2005. Proceedings. 11th International Conference on*, 2005, vol. 1, pp. 223–229 Vol. 1.
[25] P. S. Bhattacharjee, D. Saha, and A. Mukherjee, “Heuristics for assignment of cells to switches in a PCSN: a comparative study,” in *Personal Wireless Communication, 1999 IEEE International Conference on*, 1999, pp. 331–334.
[26] J. Ylitalo, J. Melén, P. Nikander, and V. Torvinen, “Re-thinking Security in IP Based Micro-Mobility,” in *Information Security*, vol. 3225, K. Zhang and Y. Zheng, Eds. Springer Berlin Heidelberg, 2004, pp. 318–329.
[27] P. Jokela, J. Melen, and J. Ylitalo, “HIP Service Discovery.” IETF Internet Draft, Jun-2006.
[28] P. Nikander and J. Arkko, “Delegation of Signalling Rights,” in *Security Protocols*, vol. 2845, B. Christianson, B. Crispo, J. Malcolm, and M. Roe, Eds. Springer Berlin Heidelberg, 2004, pp. 203–214.
[29] A. Lakhina, J. W. Byers, M. Crovella, and I. Matta, “On the geographic location of Internet resources,” *Selected Areas in Communications, IEEE Journal on*, vol. 21, no. 6, pp. 934–948, Aug. 2003.
[30] A. R. Beresford and F. Stajano, “Location privacy in pervasive computing,” *Pervasive Computing, IEEE*, vol. 2, no. 1, pp. 46–55, Jan. 2003.
[31] R. Koodli, *IP Address Location Privacy and Mobile IPv6: Problem Statement*. IETF, 2007.
[32] S. Pack, M. Nam, and Y. Choi, “A study on optimal hierarchy in multi-level hierarchical mobile IPv6 networks,” in *Global Telecommunications Conference, 2004. GLOBECOM ’04. IEEE*, 2004, vol. 2, pp. 1290–1294 Vol.2.
[33] R. Shokri, J. Freudiger, M. Jadliwala, and J.-P. Hubaux, “A Distortion-based Metric for Location Privacy,” in *Proceedings of the 8th ACM Workshop on Privacy in the Electronic Society*, New York, NY, USA, 2009, pp. 21–30.
[34] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.-C. Herrera, A. M. Bayen, M. Annavaram, and Q. Jacobson, “Virtual Trip Lines for Distributed Privacy-preserving Traffic Monitoring,” in *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services*, New York, NY, USA, 2008, pp. 15–28.
[35] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami, *Multiple Care-of Addresses Registration*. IETF, 2009.
[36] R. Koodli, *Fast Handovers for Mobile IPv6*. IETF, 2005.
[37] A. Dutta, S. Chakravarty, K. Taniuchi, V. Fajardo, Y. Ohba, D. Famolari, and H. Schulzrinne, “An Experimental Study of Location Assisted Proactive Handover,” in *Global Telecommunications Conference, 2007. GLOBECOM ’07. IEEE*, 2007, pp. 2037–2042.
[38] G. Tsirtsis, H. Soliman, N. Montavont, G. Giaretta, and K. Kuladinithi, *Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support*. IETF, 2011.
[39] J. Ylitalo, “Re-thinking Security in Network Mobility,” in *NDSS Wireless and Security Workshop*, San Diego, CA, USA, 2005.

[40] IEEE, “IEEE Standard for Local and metropolitan area networks- Part 21: Media Independent Handover.” IEEE Std 802.21-2008, 2009.
[41] J. Loughney, M. Nakhjiri, C. Perkins, and R. Koodli, *Context Transfer Protocol (CXTP)*. IETF, 2005.
[42] J. Ylitalo, P. Salmela, and H. Tschofenig, “SPINAT: Integrating IPsec into Overlay Routing,” in *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*, 2005, pp. 315–326.
[43] P. Nikander and J. Laganier, *Host Identity Protocol (HIP) Domain Name System (DNS) Extensions*. IETF, 2008.
[44] A. Gurtov, D. Korzun, A. Lukyanenko, and P. Nikander, “Hi3: An Efficient and Secure Networking Architecture for Mobile Hosts,” *Comput. Commun.*, vol. 31, no. 10, pp. 2457–2467, Jun. 2008.
[45] “The INET Framework for OMNeT++,” Mar-2014. [Online]. Available: http://inet.omnetpp.org/.
[46] “EUREKA Celtic-BOSS : On Board Wireless Secured Video Surveillance,” Mar-2014. [Online]. Available: http://celtic-boss.mik.bme.hu.
[47] J. Melen, J. Ylitalo, and H. Salmela, “Host Identity Protocol-based Mobile Proxy.” IETF Internet Draft, Aug-2009.
[48] “EUREKA-Celtic Plus MEVICO project: Mobile Networks Evolution for Individual Communications Experience,” Mar-2014. [Online]. Available: http://www.mevico.org/.

Publikációk

Folyóirat cikkek

[J1] L. Bokor, L. Lois, Cs. A. Szabó, S. Szabó: „A Novel Vertical Handover Mechanism for Media Streaming in Heterogeneous Wireless Architectures”, Híradástechnika, English Issue of Selected Papers, Volume LXII. 2007/7. pp. 52-59. 2007.
[J2] Sz. Nováczki, L. Bokor, G. Jeney, S. Imre: „Design and Evaluation of a Novel HIP-Based Network Mobility Protocol”, Journal of Networks, Academy Publisher, ISSN: 1796-2056, Volume 3, Issue 1, pp. 10-24, January 2008.
[J3] V. Simon, L. Bokor, S. Imre: „A Hierarchical Network Design Solution for Mobile IPv6”, Journal of Mobile Multimedia (JMM), ISSN: 1550-4646, Vol. 5, No.4 (December 2009) pp. 317-332, 2009.
[J4] L. Bokor, Á. Huszák, G. Jeney: „Novel Results on SCTP Multihoming Performance in Native IPv6 UMTS–WLAN Environments”, International Journal of Communication Networks and Distributed Systems (IJCNDS), 2010 - Vol. 5, No.1/2 pp. 25 – 45. ISSN (Online/Print): 1754-3924/1754-3916, DOI: 10.1504/IJCNDS.2010.033966, 2010.
[J5] L. Bokor, Z. Kanizsai, G. Jeney: „IMS-centric Evaluation of IPv4/IPv6 Transition Methods in 3G UMTS Systems”, International Journal on Advances in Networks and Services, ISSN: 1942-2644, vol. 3, no. 3 & 4, pp. 402 – 416, 2010.
[J6] Z. Faigl, L. Bokor, P. M. Neves, K. Daoud, P. Herbelin: „Evaluation of two integrated signalling schemes for the Ultra Flat Architecture using SIP, IEEE 802.21, and HIP/PMIP protocols”, Computer Networks, Elsevier B.V., ISSN: 1389-1286, DOI: doi:10.1016/j.comnet.2011.02.005, 2011.
[J7] L. Bokor, Z. Faigl, J. Eisl, G. Windisch, Components for Integrated Traffic Management – The MEVICO Approach, Infocommunications Journal 3:(4) pp. 38-49. 2011.
[J8] L. Bokor, V. Simon, S. Imre, Evaluation of the Location Privacy Aware Micromobility Domain Planning Scheme, Infocommunications Journal III:(3) pp. 38-49. 2011.
[J9] L. Bokor, Z. Faigl, S. Imre, Flat Architectures: Towards Scalable Future Internet Mobility, Lecture Notes in Computer Science 6656: pp. 35-50. 2011.
[J10] Z. Kanizsai, L. Bokor, G. Jeney: „An Anycast based Feedback Aggregation Scheme for Efficient Network Transparency in Cross-layer Design”, Periodica Polytechnica-EE 55:(1-2) pp. 45-52. 2011.
[J11] A. Takács, L. Bokor: „A Distributed Dynamic Mobility Architecture with Integral Cross-Layered and Context-Aware Interface for Reliable Provision of High Bitrate mHealth Services”, Lecture Notes of the Institute for Comp. Sciences Social-Informatics and Telecomm. Engineering 61: pp. 369-379. 2013.
[J12] Z. Faigl, L. Bokor, J. Pellikka, A. Gurtov: „Suitability analysis of existing and new authentication methods for future 3GPP Evolved Packet Core”, Computer Networks 57:(17) pp. 3370-3388. 2013.
[J13] Z. Faigl, J. Pellikka, L. Bokor, A. Gurtov: „Performance evaluation of current and emerging authentication schemes for future 3GPP network architectures”, Computer Networks 60: pp. 60-74. Paper COMPNW_5170. 2014.
[J14] L. Bokor, Z. Faigl, S. Imre: „Survey and Evaluation of Advanced Mobility Management Schemes in the Host Identity Layer”, International Journal of Wireless Networks and Broadband Technologies (IJWNBT), ISSN 2155-6261, 3(1), 34-59, January-March 2014.

[J15] L. Bokor, J. Kovács, Sz. Cs. Attila: „A Home Agent Initiated Handover Solution for Fine-grained Offloading in Future Mobile Internet Architectures: A Survey and Experimental Evaluation”, under press, 2014.

[J16] L. Bokor, G. Jeney, J. Kovács: „A study on the performance of an advanced framework for prediction-based NEMO handovers in multihomed scenarios”, submitted, 2014.

[J17] L. Bokor, Z. Faigl, S. Imre: „An extensive analysis of the Host Identity Protocol based Ultra Flat Architecture”,submitted, 2014.

Magyar nyelvű folyóirat cikkek

[J18] Bokor L., Szabó S.: „Multimédia szolgáltatás a következő generációs (NGN) hálózatokban”, Magyar Távközlés (XVI), Budapest, 2005/4. szám. pp. 14-19., 2005.

[J19] Bokor L., Szabó S.: „Az IMS megjelenése és alkalmazása cellás mobil hálózatokban”, Híradástechnika, LXI. Évfolyam, pp. 11-19., 2006/10. szám.

[J20] Nováczki Sz., Bokor L., Imre S.: „A Host Identity Protocol, avagy egy új internetarchitektúra alapjai”, Magyar Távközlés (XVII), ISSN: 0865-9648, pp. 20-25. Budapest, 2006/4.

[J21] Kara P. A., Bokor L., Imre S., A mérőalanyok prekoncepciói által okozott torzítások hatása 3G videotelefonálás QoE kiértékelési eredményeire, Híradástechnika LXVI.:(2011/4) pp. 22-28. 2011.

Könyvfejezetek

[B1] I. Dudás, L. Bokor, S. Imre: „Survey and Extension of Applications and Services in IPv6 Anycasting”, Encyclopedia of Mobile Computing & Commerce, Idea Group Inc., ISBN: 978-1-59904-002-8 (hardcover), 978-1-59904-003-5 (ebook), New York, NY, USA. 2007.

[B2] L. Bokor, Z. Németh, I. Dudás, S. Imre: „Novel Results on MBMS Service Provisioning in UTMS/WLAN Heterogeneous Architectures”, Handbook of Research in Mobile Multimedia, 2nd edition, Section IV: Mobile Networks, Chapter XXVIII, IGI Global, ISBN: 978-1-60566-046-2 (hardcover), Ismail Khalil Ibrahim (ed.), USA. Released on September 25. 2008.

[B3] Sz. Nováczki, L. Bokor, G. Jeney, S. Imre: „Emerging Mobility Applications of Host Identity Protocol”, Next Generation Mobile Networks and Ubiquitous Computing, IGI Global, ISBN: 9781605662503 (ISBN13), 160566250X (ISBN10), 9781605662510 (EISBN13), DOI: 10.4018/978-1-60566-250-3.ch019, Samuel Pierre (ed.), USA. 2010.

[B4] L. Bokor, V. Simon, S. Imre: „A Location Privacy Aware Network Planning Algorithm for Micromobility Protocols”, in Simulated Annealing, Theory with Applications, Book edited by: Rui Chibante, ISBN: 978-953-307-134-3, pp.: 75-98, Publisher: Sciyo 2010.

[B5] L. Bokor, Sz. Nováczki, S. Imre, Host Identity Protocol: „The Enabler of Advanced Mobility Management Schemes”, In: Katalin Tarnay, Gusztáv Adamis, Tibor Dulai (ed.) Advanced Communication Protocol Technologies: Solutions, Methods, and Applications. Hershey; New York: IGI Global, Information Science Reference, (ISBN: ISBN 978-1-60960-732-6) pp. 247-272., 2011.

[B6] L. Bokor, G. Jeney : „IPv4 / IPv6 Coexistence and Transition: Concepts, Mechanisms and Trends”, In: Katalin Tarnay, Gusztáv Adamis, Tibor Dulai (ed.), Advanced Communication Protocol Technologies: Solutions, Methods, and Applications., Hershey ; New York: IGI Global, Information Science Reference, (ISBN: ISBN 978-1-60960-732-6), pp. 156-177. 2011.

[B7] J. Kovács, L. Bokor, Z. Kanizsai, S. Imre: „Review of Advanced Mobility Solutions for Multimedia Networking in IPv6”, In: Dimitris Kanellopoulos (ed.) Intelligent Multimedia Technologies for Networking Applications: Techniques and Tools., Hershey: IGI Global, Information Science Reference, pp. 25-47. ISBN: 9781466628335, 2013.

Konferencia cikkek

[C1] I. Dudás, L. Bokor, G. Bilek, G. Jeney, S. Imre: „Examining anycast address supported mobility management using Mobile IPv6 testbed”, MELECON 2004 (2004.05.11-15.), INSPEC: 8180353, ISBN: 0-7803-8271-4, pp.555 – 558, Vol.2. Dubrovnik, Croatia. 2004.

[C2] L. Bokor, I. Dudás, S. Imre, „Anycast-based Micromobility”, SoftCOM 2005, (2005.09.15-17), Split, Marina-Frapa, Croatia, pp.125-130.

[C3] L. Bokor, I. Dudás, S. Szabó, S. Imre: „Anycast-based Micromobility: A New Solution for Micromobility Management in IPv6”, MoMM 2005 (2005.09.17-21), ISBN: 3-85403-195-5, pp.68-75, Malaysia, Kuala Lumpur, 2005.

[C4] Sz. Nováczki, L. Bokor, S. Imre: „Micromobility Support in HIP: Survey and Extension of Host Identity Protocol”, DOI: 10.1109/MELECON.2006.1653184, ISBN: 1-4244-0087-2, MELECON 2006 (2006.05.16-19.), Málaga, Spain, pp.651-654, Vol.1.

[C5] L. Bokor, N. Montavont, P. D. Francesco, T. Ernst, T. Hof, J. Korva: „ANEMONE: A Pan-European Testbed to Validate IPv6 Mobility Technologies”, SAINT-WONEMO 2007 (2007. 01.15-19.), DOI: 10.1109/SAINT-W.2007.25, ISBN: 0-7695-2757-4, Hiroshima, Japan, pp.44-48.

[C6] Sz. Nováczki, L. Bokor, S. Imre: „A HIP based Network Mobility Protocol”, SAINT-WONEMO 2007 (2007. 01.15-19.), DOI: 10.1109/SAINT-W.2007.8, ISBN: 0-7695-2757-4, INSPEC: 9352994, Hiroshima, Japan, pp.48-52.

[C7] Cs. A. Szabó, S. Szabó, L. Bokor: „Design considerations of a novel media streaming architecture for heterogeneous access environment”, BWAN 2006, (2006. 09.20) Alghero, Sardinia, Italy, ACM ICP Series; ISBN:1-59593-532-0, Vol. 196, Article No. 3.

[C8] L. Bokor, L. Lois, Cs. A. Szabó, S. Szabó: „Testbed of a Novel Media Streaming Architecture for Heterogeneous Wireless Environment”, Tridentcom2007, (2007.05.21-23), ISBN: 1-4244-0739-7 , pp. 220-230. Orlando, Florida, USA.

[C9] L. Bokor, V. Simon, I. Dudás, S. Imre: „Anycast Subnet Optimization for Efficient IPv6 Mobility Management”, IEEE GIIS 2007, DOI: 10.1109/GIIS.2007.4404188, ISBN 978-1-4244-1376-8, pp. 187-190, Marrakesh, Morocco, 2-6. July, 2007.

[C10] T. Ernst, L. Bokor, A. Boutet, Y. Lopez: „An Open Network for Testing, Verification and Validation of IPv6-based ITS Components”, ITST 2007, (2007.07.6-8), DOI: 10.1109/ITST.2007.4295901, ISBN: 1-4244-1178-5, pp. 1-6. Sophia Antipolis, France 2007.

[C11] L. Bokor, Sz. Nováczki, S. Imre: „A Complete HIP based Framework for Secure Micromobility”, 5th @WAS International Conference on Advances in Mobile Computing and Multimedia, MoMM2007, ISBN 978-3-85403-230-4, pp. 111-122., Jakarta, Indonesia, 3-5 December 2007.

[C12] V. Simon, L. Bokor, S. Imre: „Novel Network Design Algorithm for Optimizing Hierarchical Mobile IPv6”, 5th @WAS International Conference on Advances in Mobile Computing and Multimedia, MoMM2007, ISBN 978-3-85403-230-4, pp. 123-133., Jakarta, Indonesia, 3-5 December 2007.

[C13] L. Bokor, Z. Németh, I. Dudás, S. Imre: „MBMS Service Provisioning in UTMS/WLAN Heterogeneous Architectures”, 5th @WAS International Conference on Advances in Mobile Computing and Multimedia, MoMM2007, ISBN 978-3-85403-230-4, pp. 41-52., Jakarta, Indonesia, 3-5 December 2007.

[C14] L. Bokor, Z. Kanizsai, S. Imre: „Simple QoS Provisioning Framework for MBMS in all-IP UMTS Networks”, IEEE CN: CFP08MEL-CDR, ISBN: 978-1-4244-1633-2, MELECON 2008 (2008.05.5-7.), Ajaccio, France, pp. 286-292.

[C15] N. Montavont, A. Boutet, T. Ropitault, M. Tsukada, T. Ernst, J. Korva, C. Viho, L. Bokor: „Anemone: A ready-to-go testbed for IPv6 compliant Intelligent Transport Systems”, 8th International Conference on Intelligent Transport System Telecommunicaitons (ITST 2008), Print ISBN: 978-1-4244-2857-1, DOI: 10.1109/ITST.2008.4740262, pp. 228-233, Phuket, Thailand, October 22-24, 2008.

[C16] L. Bokor, Á. Huszák, G. Jeney: „On SCTP Multihoming Performance in Native IPv6 UMTS-WLAN Environments”, In the proceedings of the Fifth International ICST Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCom2009), ISBN: 978-1-4244-2847-2, Print ISBN: 978-1-4244-2846-5 DOI: 10.1109/TRIDENTCOM.2009.4976216 , Washington D.C., USA, April 06-08, 2009.

[C17] L. Bokor, Sz. Nováczki, L. T. Zeke, G. Jeney: „Design and Evaluation of Host Identity Protocol (HIP) Simulation Framework for INET/OMNeT++”, in the proceedings of the 12-th ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWIM 2009), ISBN:978-1-60558-616-8, DOI: 10.1145/1641804.1641827, pp. 124-133, Tenerife, Canary Islands, Spain, 26-30 October 2009.

[C18] L. Bokor, L. T. Zeke, Sz. Nováczki, G. Jeney: „Protocol Design and Analysis of a HIP-based Per-Application Mobility Management Platform”, in the proceedings of the 7-th ACM International Symposium on Mobility Management and Wireless Access (MobiWAC 2009), ISBN:978-1-60558-617-5 , DOI: 10.1145/1641776.1641779, pp. 7-16, Tenerife, Canary Islands, Spain, 26-27 October 2009.

[C19] G. Jeney, L. Bokor, Zs. Mihály: „GPS Aided Predictive Handover Management for Multihomed NEMO Configurations”, in the proceedings of the 9-th IEEE International Conference on ITS Telecommunications (ITST’09), E-ISBN: 978-1-4244-5347-4, Print ISBN: 978-1-4244-5346-7, DOI: 10.1109/ITST.2009.5399380, pp. 69 – 73, Lille, France, 20-22 October 2009.

[C20] L. Bokor, Z. Kanizsai, G. Jeney: „Performance Evaluation of Key IMS Operations over IPv6-capable 3G UMTS Networks”, In Proceedings of 2010 Ninth International Conference on Networks, ICN’10, ISBN: 978-0-7695-3979-9, Print ISBN: 978-1-4244-6083-0, DOI:10.1109/ICN.2010.49, pp. 262 - 271,Menuires, France April 11-16, 2010. (Received Best Paper Award)

[C21] L. Bokor, Z. Faigl, S. Imre, „A Delegation-based HIP Signaling Scheme for the Ultra Flat Architecture”, Proceedings of the 2nd International Workshop on Security and Communication Networks (IWSCN 2010), ISBN: 978-91-7063-303-4, pp. 9-16, Karlstad, Sweden, May 26-28, 2010.

[C22] Z. Faigl, L. Bokor, P. M. Neves, R. A. Pereira, K. Daoud, P. Herbelin, „Evaluation and Comparison of Signaling Protocol Alternatives for the Ultra Flat Architecture”, Proceedings of The Fifth International Conference on Systems and Networks Communications (ICSNC 2010), ISBN: 978-0-7695-4145-7, Nice, France, Aug. 22-27, 2010.

[C23] R. Fracchia, C. Lamy-Bergot, G. Panza, J. Vehkaperä, E. Piri, T. Sutinen, M. Mazzotti, M. Chiani, S. Moretti, G. Jeney, L. Bokor, Z. Kanizsai and M. G. Martini, „System architecture for multimedia streaming optimisation”, in Proc. of Future Network and MobileSummit 2010, Florence, June 2010.

[C24] Sz. Kustos, L. Bokor, G. Jeney, „Testbed Evaluation of Dynamic GGSN Load Balancing for High Bitrate 3G/UMTS Networks“, Proceedings of the IEEE 73rd Vehicular Technology Conference (VTC2011-Spring), pp. 1-5., ISBN: 978-1-4244-8332-7, DOI: 10.1109/VETECS.2011.5956406 , Budapest, Hungary, 05.15-05.18., 2011.

[C25] J. Kovács, L. Bokor, G. Jeney: „Performance Evaluation of GNSS Aided Predictive Multihomed NEMO Configurations”, In: ITST-2011: 11th International Conference on ITS Telecommunications. Szentpétervár, Oroszország, Institute of Electrical & Electronics Engineers (IEEE), pp. 293-298.(ISBN: 978-1-61284-670-5), 2011.

[C26] Z. Faigl, J. Pellikka, L. Bokor, S. Imre, A. Gurtov: „HIP in 3GPP EPC”, In: IETF 82 Proceedings. Taipei, Tajvan, 2011.11.13-2011.11.18. pp. 1-54. Paper HIPRG-4. , 2011.

[C27] P. A. Kara, L. Bokor, S. Imre: „Distortions in QoE measurements of ubiquitous mobile video services caused by the preconceptions of test subjects”, In: IEEE/IPSJ International Symposium on Applications and the Internet SAINT2012. Izmir, Turkey, 2012.07.16-2012.07.20. IEEE, pp. 409-413. ISBN: 978-0-7695-4737-4 , 2012.

[C28] I. Kulik, P. A. Kara, T. A. Trinh, L. Bokor, Analysis of the Relationship between Quality of Experience and Service Attributes for 3D Future Internet Multimedia, In: IEEE 4th International Conference on Cognitive Infocommunications. Budapest, Magyarország, 2013.12.02-2013.12.05. Budapest: pp. 641-646. ISBN: 978-1-4799-1544-6 , 2013.

[C29] I. Kulik, P. A. Kara, T. A. Trinh, L. Bokor, Attributes Unmasked: Investigation of Service Aspects in Subjective Evaluation of Wireless 3D Multimedia, In: The Second International Conference on Informatics & Applications (ICIA2013), Lodz, Lengyelország, 2013.09.23-2013.09.25. pp. 270-275. Paper 150. ISBN: 978-1-4673-5255-0, 2013.

[C30] L. Bokor, G. Panza, J. Vehkaperä, L. Iacobelli, E. Piri, M. Mazzotti, B. Lecroart, M. Martini, Cross-layer Optimized Delivery for Interactive Multimedia Healthcare Services: The CONCERTO Architecture, In: Future Network and MobileSummit 2013, Funems 2013. Lisboa, Portugália, 2013.07.09-2013.07.13. pp. 1-4. , 2013.

[C31] P. A. Kara, L. Bokor, S. Imre, Distortions in QoE Assessment of 3D Multimedia Services on Multi-access Mobile Devices, In: 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). Lyon, Franciaország, 2013.10.07-2013.10.09. (IEEE) pp. 311-318., 2013.