Tartalom

Címlap: GEANT – a páneurópai szélessávú kutatói hálózat

A magyar kutatói számítógéphálózat legfrissebb eredményei

szabo@hit.bme.hu

Magyarországon a számítógéphálózati fejlesztések a hetvenes évek első felében kezdődtek el. Több kutató-, fejlesztő intézet foglalkozott különböző csomagkapcsolási eljárásokkal és az ezekhez kapcsolódó alkalmazásokkal. A 80-as évek végére hazai fejlesztésként létrejött az első nagyterületű csomagkapcsolt hálózat, az X.25 és megjelent az első mai értelemben is korszerű hálózati alkalmazás az ELLA elektronikus levelező rendszer. A fejlesztések hátterében alakult meg az Információs Infrastruktúra Fejlesztési Iroda 1986-ban, amely 1992-ben felvette a nemzeti jelzőt. Az NIIF az EU országokhoz hasonlóan a magyarországi kutatóhálózati fejlesztések központi programjává vált. Az NIIF program tevékenységéről a www.niif.hu honlapon lehet részletesebb információt kapni.

1992-ben Miskolcon egy új, hálózati témákkal foglalkozó konferencia mutatkozott be: a Networkshop. A rendezvény – amely azóta is minden évben megrendezésre került – 2006-ban visszatért Miskolcra. A Networkshop, mint konferencia évente körülbelül 400 látogatót vonz és nagyjából 100-110 előadás hangzik el. A szakmai fórum nagyon jól reprezentálja a hazai kutatóhálózati eredményeket, fejlesztéseket, újdonságokat. A konferencia rendelkezik webes archívummal is, amelyet a http://www.iif.hu/rendezvenyek/networkshop/ címen érhetünk el. Sőt az utóbbi pár évben video archívum is készült, azaz a rendezvény előadásait akár utólag is meg lehet nézni.

A Híradástechnika folyóirat szerkesztősége idén úgy döntött, hogy kísérletképpen a 2006. évi Networkshop konferencia néhány előadását cikk formájában is megjelenteti. A cikkeket négy fő területről válogattuk ki, mintegy megfeleltetve a kutatói hálózati tevékenység legfontosabb irányait és a konferencián elhangzó előadásokat.

Az NIIF projektjeiről és a legfontosabb központi fejlesztési eredményekről Fehér Ede és Mohácsi János cikke számol be. A hálózati területen folytatott vizsgálatokat Jákó András, Horváth Gábor, illetve Gál Zoltán és kollégái eredményeiből ismerhetjük meg. A köztes réteg fejlesztéseit, illetve legfontosabb nyitott hazai kérdéseit Sikolya Zsolt, illetve Bajnok Kristóf cikke alapján érthetjük meg. Perlaki Attila illetve Simon András a legaktívabb a könyvtári alkalmazási terület új eredményeiről számolnak be. A kutatási célú alkalmazásokra ad érdekes bepillantást Holl András cikke a csillagászati kutatások összefüggéseinek felvázolásával, a grid terület friss eredményeit pedig Kornafeld Ádám cikkéből ismerhetjük meg.

Szomorú aktualitása is van a júniusi számnak. Róna Péter sokak által tisztelt kollégánk most lenne 75 éves. Egyik oldalunkon Rét András régi kollégaként segít megőrizni emlékét.

Tétényi István,
vendégszerkesztő

Szabó Csaba Attila,
főszerkesztő

A hazai kutatói hálózat infrastruktúrája – a NIIF Program

FEHÉR EDE, MOHÁCSI JÁNOS

Nemzeti Információs Infrastruktúra Fejlesztési Intézet
ede.feher@niif.hu

Kulcsszavak: kutatói hálózat, NIIF, HBONE, információs infrastruktúra

A nemzeti kutatói hálózatok valamennyi európai államban fontos szerepet töltenek be a kutatás-fejlesztés számára nélkülözhetetlen információs infrastruktúra biztosításában, valamint a legújabb hálózati technológiák kipróbálásában, bevezetésében és elterjesztésében. Magyarországon a kutatói hálózati infrastruktúra fejlesztése és üzemeltetése az Nemzeti Információs Infrastruktúra Fejlesztési Program (NIIF Program) keretében valósul meg. A cikk bemutatja az NIIF Program legutóbbi fejlesztéseinek eredményeit, és az élvonalba tartozó infrastruktúra főbb elemeit a fejlesztési program négy stratégia területén.

1. Bevezetés

A Nemzeti Információs Infrastruktúra Fejlesztési Program (NIIF Program) és ennek szervezeteként alapított NIIF Intézet a hazai kutatási, felsőoktatási és közgyűjteményi számítógép-hálózat létrehozója, fejlesztője és a kiépített országos infrastruktúra üzemeltetője.

A Program elsődleges célja, hogy Magyarországon biztosítsa a tudományos kutatás, az innovatív fejlesztés, valamint a kapcsolódó oktatás területén az EU legfejlettebb országaihoz hasonló infrastrukturális feltételeket. További cél, hogy a nemzetközi élvonalat képviselő K+F információs infrastruktúra – a fejlett világ más országainak kutatói hálózataihoz hasonlóan – húzóerőt gyakoroljon a hazai informatikai és adatkommunikációs ipar fejlődésére, minta- és tesztrendszereket szolgáltasson a széleskörű elterjesztés segítése céljából.

Ez a kutatói hálózati szerep találkozik az EU célkitűzéseivel is, egyebek mellett az eScience, eInfrastructures, Európai Kutatási Övezet (ERA) és i2010 célokkal, illetve áttételesen a lisszaboni célkitűzésekkel. A magyar kutatói hálózat és a szervezeti kereteket biztosító fejlesztési program harmonikusan illeszkedik az európai és tengerentúli törekvésekhez, trendekhez, prioritásokhoz is.

A kutatói hálózatok fejlesztéseiket nem csupán az adathálózati technológiák területén folytatják, hanem minden olyan IKT megoldás elsők közötti bevezetésével illetve fejlesztésével foglalkoznak, amelyek a felhasználói kört munkájukban támogatják. Az NIIF Program keretében a fejlesztési projektek így az adathálózat mellet az internetes alkalmazásokra, kommunikációs megoldásokra és a speciális igényeket kielégítő szuperszámítástechnikai szolgáltatásokra is kiterjednek.

A cikk az NIIF Program keretében végrehajtott fejlesztési projektek főbb eredményeit mutatja be, illetve a szolgáltatások alapját jelentő országos számítógéphálózatot.

2. Az NIIF Program bemutatása

Az NIIF Program különböző szervezeti formában már 1986 óta működik, és – rendkívül költséghatékony módon – biztosítja a kiemelkedő minőségű kutatói hálózati infrastruktúrát hazánkban. Az NIIF Program felhasználói köre a tudományos kutatás, a felsőoktatás, valamint az ugyancsak tudományos igényű és kutatási tevékenységet is ellátó közgyűjtemények (könyvtárak, múzeumok, levéltárak), amely jelenleg több mint 420 intézményt és 600.000 felhasználót jelent. Az NIIF Program hálózatára kapcsolódik többek között valamennyi felsőoktatási intézmény, akadémiai kutatóintézet és országos hatáskörű közgyűjtemény.

A Program kiemelkedő szerepet játszik az internet technológiák és alkalmazások széleskörű hazai elterjesztésében, az információs társadalom magyarországi kialakításában. A legkorszerűbb számítógép-hálózati technológiák és szolgáltatások hagyományosan az NIIF rendszereiben jelennek meg először (pl. DWDM, IPv6, MPLS-VPN, GE, multicasting, szuperszámítástechnika, grid, IP alapú videokonferencia stb.), így a program jelentős húzóerőt gyakorol az egész magyar távközlési és informatikai iparra, valamint kineveli az ország számára a jövő hálózati technológiáinak szakembereit.

Az NIIF Program adatkommunikációs hálózata és a kapcsolódó informatikai szolgáltatások minden paramétert tekintve egyenrangúak az EU vezető tagállamainak hasonló hálózataival és szolgáltatásaival. A Program keretében a folyamatos fejlesztő munka eredményeképpen mára elismerten Európa élvonalába tartozó, országos gigabites kutatási és felsőoktatási hálózati infrastruktúra épült ki.

Az NIIF hálózata a legfejlettebb országok kutatói hálózataival egy időben érte el 10Gbit/sec nemzetközi adatforgalmi sebességet, illetve az országon belül harminc vidéki városban teszi lehetővé a nagysebességű, adathálózati csatlakozást a tagintézményi kör számára.

A NIIF számítógép-hálózata integráns része a nagysebességű páneurópai kutatói hálózatnak, a GEANT-nak, amely összekapcsolja Európa 34 országának nemzeti kutatói hálózatait és közvetlen, vagy közvetett kapcsolattal rendelkezik a világ összes jelentős nemzeti, illetve regionális kutatói hálózata felé.

Az NIIF Program számos nemzetközi, az EU által támogatott kutatás-fejlesztési projektben vesz részt (GEANT2, 6NET, SEEREN, EGEE stb.), ami a nemzetközi együttműködés szakmai előnyein túl jelentős mértékű EU-forrás hazai felhasználását is lehetővé teszi. A nemzetközi trendeknek megfelelően az NIIF Program keretében a fejlesztések az alábbi, egymással szoros kapcsolatban lévő stratégiai területeken folynak évek óta:

– adatkommunikációs hálózat,
– köztes rendszerek –
  autentikációs és autorizációs infrastruktúra,
– szuperszámítástechnika, grid,
– kollaboratív alkalmazások.

3. A hazai kutatói hálózat gerinchálózata

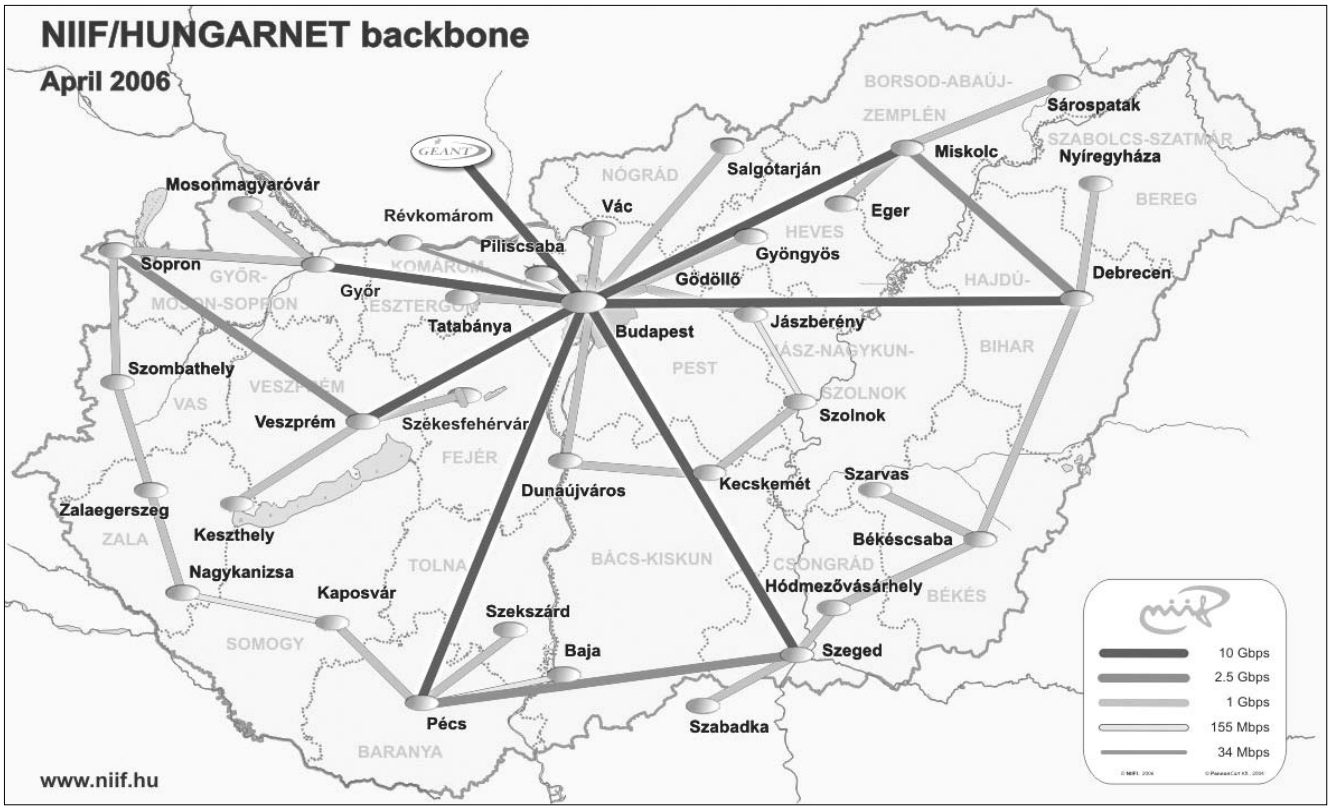
Az NIIF Program gerinchálózata a HBONE, infrastruktúráját tekintve Magyarország egyik legnagyobb és legmodernebb országos hálózata amely összemérhető kapacitásban és tudásban a legfejlettebb nemzetközi kutatói hálózatokkal. Az NIIF infrastruktúra 10 Gbit/sec illetve 1Gbit/sec sebességű gerinchálózattal, 10 Gbit/s IP + 10 Gbit/s optikai nemzetközi kapcsolattal, a magban rendelkezésre álló összesen több mint 150 Gbit/s kapacitással és tartalékoltsággal rendelkezik.

Az NIIF Program országos IP hálózata költségek és rugalmasság szempontjából is hatékony működési modellt valósít meg. A távközlési szolgáltatóktól a mindenkori legmagasabb technológiai szintnek megfelelő adatátviteli szolgáltatást bérel, amelyen az IP és egyéb értéknövelt szolgáltatásokat (pl. IPv6, multicast, MPLS-VPN, videokonferencia, VoIP stb.) a kutatói és felsőoktatási szféra szellemi potenciáljára támaszkodva sokkal magasabb szinten teszi elérhetővé, mintha a távközlési szolgáltatóktól kulcsrakész internet szolgáltatást rendelnének a felhasználók.

Az elmúlt időszak fejlesztéseinek eredményeként egy megfelelő tartalékoltságot biztosító és nagy sávszélesség-kapacitással rendelkező gerinchálózat került kialakításra. A 2005-ben lebonyolított, a vidéki nagysebességű kapcsolatok biztosítására kiírt tender kapcsán alapvető követelmény volt, hogy mind a kapacitások, mind pedig a felügyelt eszközök tekintetében egységes, és a felhasználói igényeket 3-4 éven múlva is kielégítő rendszer alakuljon ki.

A tenderben így a preferált optikai sötétszálak és megvilágított szálak mellett a Gigabit Ethernet, illetve bizonyos összeköttetések esetén 155Mbps-os STM-1 SDH alapú megoldások megajánlását kértük a távközlési szolgáltatóktól. A kapacitás növelése mellett szintén alapelvnek tekintettük az egyes helyszínek megfelelő tartalékolásának megteremtését, így a tender során fontos szempont volt, hogy vonali hibák esetén az egyes HBONE csomópontok lehetőség szerint alternatív útvonalakon is elérhetőek maradjanak. Korábban a nagysebességű vidéki csomópontok tartalékoltsága egy-

1. ábra A HBONE – a hazai kutatói hálózat nagysebességű összeköttetései



általán nem volt megoldott: ha egy vonal meghibásodott, akkor az egyes helyszínekhez kapcsolódó intézmények leszakadtak a hálózatról.

A HBONE országos topológiáját az *előző oldali ábra* mutatja be. Talán a legszembetűnőbb, hogy egy új gyűrű került kialakításra az ország középső részén és az előző tender kapcsán kialakított 10Gbps sebességű optikai kapcsolatokat felhasználva további gyűrűs kapcsolatok jöttek létre az ország keleti és nyugati felén is.

A legutóbbi bővítés során az SDH technológia helyébe a legtöbb helyen DWDM alapú optikai hálózat lépett a szolgáltatói oldalon. A HBONE magját alkotó optikai rendszer kialakítása katalizátorként hatott a magyarországi szolgáltatói DWDM hálózatok kiépítésére és továbbfejlesztésére.

Minden telekommunikációs szolgáltató felügyelt 10 GE és GE szolgáltatásokat nyújt a kiépített DWDM rendszerén. Egyes helyszíneken, ahol a DWDM nem volt kifizetődő a telekommunikációs szolgáltatók számára, CWDM megoldásokat alkalmaztak, amelyek ugyan nem teszik lehetővé a nagyszámú hullámhosszt, de nagyságrenddel olcsóbb őket kiépíteni. További újdonsága a HBONE optikai gerinchálózatának, hogy elsőként használja a szolgáltatók által elmúlt évben kiépített next generation SDH hálózatok gigabit Ethernet képességeit produkciós környezetben.

A Budapesten belüli összeköttetések esetén a korábbi gyakorlatnak megfelelően a szolgáltatóktól bérelt úgynevezett ,,fekete üvegszálakon" Gigabit Ethernet, illetve 10 Gigabit Ethernet protokollt valósít meg saját eszközeivel az NIIF Intézet.

A gerinchálózat fejlesztése mellett nagy súlyt fektettünk a gerinchálózati eszközök fejlesztésére is. Az elmúlt időszakban az NIIF Intézet több fázisban fejlesztette, illetve redundássá tette a Cisco 6500-as eszközparkját SUP720B és Sup720BXL típusú routing processzorral, valamint a Cisco 7200-as routereket Gigabit Ethernet portokkal és NPE-G1 routing processzorokkal bővítette. A HBONE alapvetően az IP technológiára épít, beleértve az IPv4 és IPv6 technológiát is: Aa gerinchálózati eszközök OSPF, IS-IS és BGP protokollt használnak. Ezekre a technológiákra építenek a különböző értéknövelt szolgáltatások, mint a különböző VPN megoldások, Voice over IP vagy a videokonferencia szolgáltatás is.

A HBONE infrastruktúra monitorozására, konfigurálására professzionális hálózatmenedzsment eszközök és ingyenesen hozzáférhető kisebb segédprogramok egyaránt bevezetésre kerültek. A professzionális termékek közül az Infovista SLA monitorozó terméket érdemes kiemelni. Ez a professzionális termék jól egészíti ki azok szabadon hozzáférhető segédprogramokat, mint például, Cricket, Nagios, Munin, Rancid, és több belső fejlesztésű rendszert, amelyek lehetővé teszik a HBONE infrastruktúra professzionális menedzsmentjét.

A HBONE az alapvető IPv4 szolgáltatáson kívül további szolgáltatásokat is nyújt a felhasználóinak. Az egyik ilyen szolgáltatás az IPv6, amely az IP technológiát elérhetővé teszi egy sokkal nagyobb közönség számára, azáltal, hogy korlátlan címezhetőséget, könnyebb menedzsmentet és biztonságosabb kommunikáció lehetőségét biztosít az internetre csatlakoztatott eszközök számára.

Másik ilyen szolgáltatás a különböző VPN-ek (Virtuális Privát Hálózatok) kialakításának lehetősége, melynek segítségével felhasználói csoportok úgy kommunikálhatnak egymással a HBONE szolgáltatásait igénybe véve, mintha közvetlenül védett csatornán volnának összekötve. A jelenlegi IP VPN (L3 VPN) technológiát az igények és lehetőségek függvényében Ethernet VPN (L2 VPN) technológiával is kiegészítjük.

További fontos szolgáltatása a HBONE-nak az alkalmazások és szolgáltatások osztályba sorolása és bizonyos osztályú alkalmazások priorizált kezelése (QoS). Tipikus felhasználója ennek a szolgáltatásnak az IP alapú hangtovábbítás és IP alapú videokonferencia szolgáltatások, mely alkalmazások esetén a késleltetésnek, késleltetés ingadozásának és a csomagvesztésnek az alacsony szintre szorítása elengedhetetlen akár a többi forgalom terhére is.

HBONE fejlesztése folyamatosan történik annak érdekében, hogy a felhasználói kör igényeit kielégítő innovatív szolgáltatások a vezető kutatói hálózatokkal egyidőben és megegyező minőségben jelenjenek meg. A páneurópai GEANT2 hálózatban, az end-to-end szolgáltatások bevezetésére helyeződik át a hangsúly, amely garantált minőségű és sávszélességű hozzáférési lehetőséget biztosít az osztott távoli e-Science erőforrásokhoz.

4. Köztes rendszerek – AAI

Az NIIF Intézet autentikációs és autorizációs infrastruktúrájának alapját az elosztott, országos névtár-rendszer képezi, amelyet az NIIF szolgáltatásainak jelentős része használ a felhasználó azonosítás és jogosultságkezelés során (például behívás, e-mail, webtárhely). Erre épül az NIIF CA szolgáltatása is, amely nemzetközileg elismert, az EU K+F projektjeiben is felhasználható és az EUGridPMA által elismert tanúsítványokat bocsát ki.

Az alapinfrastruktúrát biztosító névtár rendszerre építve indult el 2005-ben az AAI projekt keretében egy olyan egységes azonosítási, jogosultság-kezelési és naplózó rendszer kifejlesztése is, pilot keretében történő validálása, amely a hazai kutatói hálózatra csatlakozó szervezetek számára biztosítja a védett webes erőforrások (alkalmazások, adatbázisok stb.) biztonságos és rugalmas megosztását egymás illetve harmadik fél számára – hazai és nemzetközi viszonylatban egyaránt.

A fejlesztés alatt álló rendszer az NIIF Program infrastruktúráján belül egy olyan központi szolgáltatásnak teremtené meg az alapját, amely segítségével megvalósítható a hallgatók és a kutatók „egykapus" elektronikus kiszolgálása, illetve az adatok szabályozott és ellenőrzött áramlása az intézmények között az alábbi kritériumok teljesülése mellett:

- Rugalmas, könnyen használható a felhasználók számára: egyedi programok telepítését nem igényli a kliens oldalon, használata egyszerű és könnyen megtanulható;
- Szövetségi (föderatív) modellt követi: a központosított rendszerekkel ellentétben a szolgáltatást igénybe vevő intézmények bizalmi kapcsolataira épül, amely támogatja a heterogén rendszerek együttműködését, miközben nem sérti az egyes intézmények autonómiáját. A központi kiszolgálás csak az egyes intézményektől független funkciók megvalósításához szükséges. Az NIIF Program a megbízható „harmadik fél" szerepét tölti be, aki egyben biztosítja a kapcsolódási pontot az összeurópai, hasonló elven működő AAI rendszerekhez.

5. Szuperszámítástechnika

Az NIIF Program szuperszámítástechnikai infrastruktúrája két egymást kiegészítő és egymással összekapcsolt rendszerből áll: a központi szuperszámítógépekfürt illetve az országos ClusterGrid infrastruktúrából.

Az NIIF Szuperszámítógép Központ SUN E15K, illetve E10K szuperszámítógépei 2001 februárjától állnak a magyar kutatók rendelkezésére, és a folyamatos bővítés eredményeként jelenleg 250 Gflops teljesítménnyel rendelkeznek. A nagysebességű hálózat adta lehetőségeket kihasználva a rendszer két node-ja kihelyezésre kerül az ELTE-re, illetve a Szent István Egyetemre. Eddig összesen több mint 150 felhasználó, 80 regisztrált projektje fémjelzi a szolgáltatás sikerét, egyben a szolgáltatás iránti fokozódó igényeket.

A szolgáltatás másik eleme a ClusterGrid rendszer, amely az országszerte kiépített PC laborokat grid rendszerbe fogja össze, úgy, hogy azok – amikor oktatási, kutatási, belső szolgáltatási célra nem használják őket (éjszakánként, hétvégenként) – a grides kapcsolaton keresztül képesek legyenek számításiidő-igényes feladatok elosztott futtatására. E projekt eredményeképpen egy mintegy 2000, zömmel Intel-alapú csomópontokból álló rendszer üzemel, amelynek elosztott elemei az ország különböző pontján, 30 intézményben találhatók, mégis teljesen biztonságosan használható. A rendszer összkapacitása átlagosan 400-600 Gflops, amely Európa 4-5. legnagyobb élesüzemben működő gridje. A rendszer elismertségét jól mutatja a Nordugrid-del történő együttműködés, amely a két grid összekapcsolása mellett jelentős fejlesztési feladatokat is magába foglal, és amelyet az EU jelentős forrásokkal támogat.

Az NIIF Intézet 2005 szeptemberében elindította adattárolási szolgáltatását is, amelynek legfontosabb feladata az, hogy a szuperszámítógépek és a grid által feldolgozott számítási feladatok nem ritkán több Gbyte nagyságú eredményeinek tárolásához biztonságos, egyszerűen elérhető környezetet teremtsen. A szolgáltatás, mely jelenleg a ClusterGrid projekt részét képzi, jelenleg 45Tbyte redundáns, hasznos diszk-kapacitást nyújt az akadémiai felhasználói közösség számára.

Az NIIF Intézet munkatársai 2005. tavaszán egy új, forradalmi technológián alapuló adattárolási megoldásra építkezve alakították ki a szolgáltatást. A megoldás az „ATA over Ethernet" (AoE) protokollon alapul, amelynek implementációi a diszkek által kiadott, illetve fogadott vezérlőparancsokat Ethernet csomagokba ágyazzák, és így továbbítják az adathálózaton. A megoldás révén az olcsó SATA diszkeket tudjuk összekapcsolni egy közönséges Ethernet switch segítségével, majd az így kialakított alrendszer egy file szerver szintén Ethernet portjára kapcsolva, közönséges blokk-eszközként érhető el. A kiszolgálókon telepített megfelelő kötetkezelő szoftver segítségével egységes, redundáns hálózati tárolóterületet lehet kialakítani.

6. Kollaboratív alkalmazások

Az NIIF Intézet a tagintézményekben folyó kutatási és oktatási tevékenység támogatására különböző internet alapú, az együttműködést támogató megoldásokat vezetett be és szolgáltat. Ezek között megtalálhatóak a hagyományos szolgáltatások (például webhosting, szerver hosting, e-mail, webtárhely stb.), illetve a nagysebességű IP hálózatokat kihasználó, a távközlés-informatika-média konvergenciáját jól példázó kollaboratív megoldások. Az NIIF Program keretében ez utóbbi csoportba tartozik a videokonferencia és VoIP szolgáltatás is, amelynek felhasználói köre és a szolgáltatás tartalma dinamikusan fejlődött az elmúlt időszakban.

Az NIIF Program videokonferencia projektjének célja a hazai felsőoktatási és akadémiai közösség országos méretű, IP alapú, professzionális minőségű videokonferencia infrastruktúrával és a hozzá kapcsolódó központi szolgáltatásokkal történő ellátása, biztosítva ezzel a felsőoktatási és kutatói szféra számára a napjainkban hozzáférhető legmodernebb és leghatékonyabb kommunikációs technológia használatát.

Az NIIF Intézet a projekt keretében 50 professzionális, tárgyalótermi videokonferencia végberendezést helyezett el 40 felsőoktatási intézménynél, kutatóintézetnél, illetve könyvtárnál, valamint két minisztériumban. A kiépített videokonferencia szolgáltatása IP alapú, amely az NIIF nagysebességű gerinchálózatára épül, biztosítva ezzel a videokonferencia forgalmi díjtól mentes és korlátozás nélküli felhasználását, költséghatékony üzemeltetését. Az alapszolgáltatáson kívül az NIIF számos értéknövelt szolgáltatást is biztosít felhasználói számára. Az NIIF által üzemeltetett központi kiszolgáló infrastruktúra hatékonyan támogatja a több résztvevős videokonferenciákat, amely lehetővé teszi, hogy egyszerre akár több tíz végpont is bekapcsolódhasson egyetlen konferenciába. Az egyre szélesedő és jelentősebbé váló külföldi kapcsolatokkal rendelkező akadémiai közösség számára az NIIF nemzetközi IP alapú videokonferencia kapcsolatot biztosít, amelyen keresztül a teljes európai és amerikai kutatói közösség korlátlanul és díjmentesen elérhető.

A videokonferencia projekt szerves részeként jött létre az NIIF Video on Demand archívum, illetve az eh-

hez kapcsolódó online közvetítési tevékenység, amelynek célja a jelentős felsőoktatási és akadémiai események (pl. konferenciák) előadásainak online internetes közvetítése és archiválása képpel, hanggal és prezentációval együtt. Az archívumban jelenleg már több mint 600 tudományos és szakmai előadás férhető hozzá, többek között Nobel díjas tudósok előadásai is.

Az NIIF VoIP szolgáltatása 2005-ben zárta működésének második teljes évét, amely ismételten bizonyította a szolgáltatás életképességét: a kialakított műszaki megoldás, a szolgáltatás minősége és rendelkezésreállása megfelelt a felhasználói igényeknek, valamint a pénzügyi konstrukció jelentős megtakarítás elérését biztosította. A szolgáltatást igénybe vevő tagintézményi kör és a rendszeren lebonyolított hívások száma az indulás óta megőrizte a dinamikáját: a rendszerbe kapcsolt intézmények száma másfélszeresére, míg a lebonyolított forgalom több mint kétszeresére növekedett eddig minden évben.

Jelenleg 69 intézmény – a felsőoktatási intézmények és kutatóintézetek többsége – kapcsolódik alközpontjával az NIIF VoIP rendszeréhez, így az egymás között ingyenesen lebonyolítható belső hívásokkal a felsőoktatási intézmények mellékeinek többsége elérhető. A szolgáltatás keretében lehetőség van a nyilvános hálózatokba való kihívásra is, nagyon kedvező árak mellett. Több vidéki nagy egyetem teljes kimenő hangforgalmát – beleértve a helyi hívásokat is – az NIIF VoIP rendszerén keresztül bonyolítja le.

A folyamatosan növekvő forgalom miatt a szolgáltatás rendelkezésreállása és minősége egyre inkább központi szerepet tölt be, így a 2005-ben elvégzett fejlesztések főként a rendelkezésreállás növelésére irányultak. A rendszer megbízhatóságát és egyben rugalmasságát növelték a központi hívásirányító rendszerben végrehajtott fejlesztések. A hívásirányító rugalmasságát bizonyítja, hogy a tavalyi év végén a korábban támogatott bekapcsolási mód mellett – az intézményi alközpont ISDN PRI vagy BRI kapcsolaton keresztüli bekapcsolása az NIIF által biztosított VoIP átjáróval – lehetőség nyílt a közvetlen SIP kapcsolatok fogadására IP PBX-ek felől.

7. Összefoglalás

Habár Magyarországon a telekommunikációs szektor nem olyan fejlett – korlátozott a verseny a telekommunikációs piacon, illetve a fekete üveg kapcsolatok, melyek a „korlátlan sávszélességű” megoldások kialakításához kellenek, csak igen korlátozottan érhetőek el –, a HBONE a magyarországi eScience infrastrukturális alapjait képes volt megteremteni.

Az NIIF Intézet a fejlesztései révén képes volt megteremteni a magyarországi eScience infrastrukturális alapjait, és az így létrejött kutatói hálózat biztosítja azokat az alapfeltételeket, amelyek a felhasználói kör eredményes munkájához nélkülözhetetlenek a hazai és nemzetközi együttműködésekben. Az együttműködést az európai élvonalba tartozó adathálózat mellett a jelentős számítási és tárolási erőforrások, a hozzáférést szabályozó köztes rendszerek, valamint a kollaboratív rendszerek széles köre biztosítja.

Róna Péter most lenne 75 éves

Ha nem Róna Péterről lenne szó, úgy kezdeném, hogy Állami-díjas, a műszaki tudományok kandidátusa... A volt munkatársaiban, szakmabeliekben, barátaiban és ismerőseiben róla élő kép leírását azonban nem így kell kezdeni. Odafentről neki sem tetszene ez.

Nagyszerű ember volt, kiemelkedő tehetség és a munka megszállottja. Soha nem az első sorból, de nagy empátiával figyelte és próbálta megérteni a környezetét. Elveivel nem alkudott meg, mégis mindenki szerette, tisztelte.

Szerénységére jellemző a kandidátusságának története. Munkatársai nyomására adta be azt a fiókjában levő, gyakorlatilag nyomdakész dolgozatot, amely disszertációként is kiemelkedő volt. Az „Intermodulációs zaj sokcsatornás frekvenciamodulált rádiórelé berendezésekben” amellett, hogy jelentős matematikai apparátus mély ismeretét bizonyította, szorosan kapcsolódott a nemzetközileg is elismert hazai mikrohullámú rádiórelé-rendszerfejlesztéshez. A formaságokra annyira nem adott, hogy a sikeres védés után nem kérte az automatikusan járó doktori címet.

Kiemelkedő tehetségét már középiskolásként bizonyította. A híres fasori gimnázium diákjaként egyszer harmadik lett, majd pedig megnyerte az országos matematikai versenyt. A BME Hadmérnöki Karát vérbeli civilként elvégezve a Távközlési Kutató Intézetbe került, ahol bekapcsolódott a mikrohullámú rendszerek fejlesztésébe. A komplex csapatmunkában elsősorban matematikai ismereteit, átfogó és lényeglátó rendszerszemléletét hasznosították. Fontos volt angoltudása, páratlan szókincse, de az oroszban és németben is felkészült volt. Munkáját az Intézetben az esti órákig végezte, majd otthon folytatta késő estig, illetve a hétvégeken és a szabadsága alatt is.

Legfontosabb munkái a 4, 6 és 7 GHz-es sávban működő rádiórelé összeköttetések rendszertervezéséhez kapcsolódtak, azon belül is a zajmérlegekben jelentős súllyal szereplő intermodulációs zajok számítását végezte, melynél a sztochasztikus folyamatok ismeretére volt szükség, de az igen összetett tölcsérparaboloid antennák tervezése is az ő kezében volt. Kiemelkedő szerepe volt a TÁKI-ban fejlesztett, a hazai híradástechnikai ipar termelésének jelentős részét kitevő berendezések gyártásba vitelében.

Az Intézet számára igen hasznos volt, hogy közeli és távoli munkatársai tudták, matematikai és műszaki problémáik megoldásáért jó esélyel fordulhatnak Róna Péterhez segítségért. Ebben kiváló memóriája, rendszeressége is szerephez jutott. A megoldáshoz sokszor használta a szekrény felső polcain sorakozó, sok évet lefedő füzeteit, amelyekben percek alatt eljutott a keresett részhez. (Fejében ez az információ is jól elfért a teljes Don Giovanni és az éppen olvasott angol krimi mellett.)

Szakmai ismeretei, tekintélye, munkabírása és nyelvtudása okán nagy szerepe volt a külföldi kutatóhelyekkel való együttműködésekben és a nemzetközileg is elismert Mikrohullámú Kollokvium-sorozat megvalósításában.

Róna Pétert 58. életévét alig betöltve, – kedvenc időtöltésének hódolva, tájékozódó futás versenypályájának kitűzése közben – egy forró, fülledt augusztusi vasárnapon a budai erdőkben érte a hirtelen halál.

Tíz évig dolgoztunk egymás mellett. Sokat tanultam tőle.

A barátom volt.

Rét András

10 Gigabit Ethernet

JÁKÓ ANDRÁS

BME Egyetemi Informatikai Szolgáltató Központ
jako.andras@eik.bme.hu

Kulcsszavak: Ethernet, 802.3, lokális hálózat (LAN), 10GBASE-T eszközök

A 10 Gigabit Ethernet [1] szabványosítása már jó néhány éve folyik. Több ajánlás megjelent már, de néhány ajánláson most is dolgozik az IEEE – ezek várhatóan idén vagy jövőre készülnek el. Ebben a cikkben a 10GigabitEthernet újdonságait mutatja be a szerző az Ethernet család korábbi, kisebb sebességű tagjaihoz képest.

1. Bevezetés

Az Ethernet családot leíró IEEE[2] 802.3 szabvány [1] folyamatosan hízik, immár több mint húsz éve. A 802.3 szabványhoz első megjelenése óta számos kiegészítés készült, mint például a 802.3u jelű 1995-ben, ami a 100BASE-TX fizikai réteget specifikálta (ez a ma is használatos csavart érpáros FastEthernet), vagy 2003-ban a csavart érpáron keresztüli tápellátásról szóló 802.3af. Most is több, pillanatnyilag nyolc ilyen kiegészítésen dolgoznak az IEEE munkacsoportjai. Ezek a kiegészítések aztán belekerülnek a szabványba, amit az IEEE néhány évente újra kiad – a legutolsó változat a tavaly megjelent IEEE 802.3-2005.

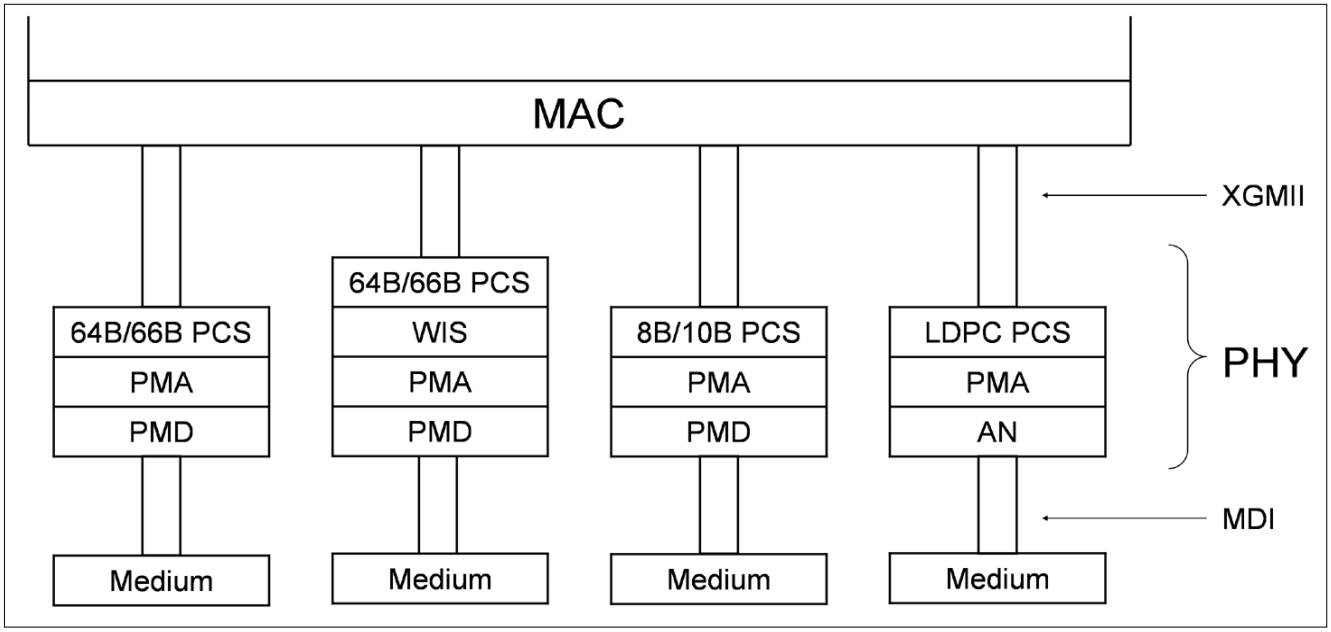
A legfrissebb már elkészült és a jelenleg kidolgozás alatt álló kiegészítések között is több olyan van, ami a 10 Gbit/s sebességű működést, és az arra alkalmas fizikai rétegeket írja le. Ezzel tehát ismét egy nagyságrenddel gyorsabb tagokkal bővült az Ethernet család a korábbi legnagyobb, 1 Gbit/s sebességű GigabitEthernethez képest.

2. MAC

A 10GigabitEthernet MAC[3] legfontosabb újdonsága, hogy ezen a sebességen csak full-duplex működést enged meg.

A busz topológiájú Ethernet fizikai rétegek (10BASE2, 10BASE5) esetén a CSMA/CD[4] protokoll és a half-duplex működés elengedhetetlen volt. Az igen ritkán hasz-

1. ábra 10 Gigabit Ethernet komponensek



1 Az IEEE 802.3 szabványban használt írásmód szerint a különféle sebességű Ethernetek megnevezése külön szóba írandó (pl. „Fast Ethernet" vagy „10 Gigabit Ethernet"), de ezeket a könnyebb értelmezés és az egyértelműség kedvéért a továbbiakban egybe fogom írni („FastEthernet", illetve „10GigabitEthernet" stb.)

2 IEEE: Institute of Electrical and Electronics Engineers

3 MAC: Media Access Control sublayer, közeghozzáférési alréteg

4 CSMA/CD: Carrier Sense Multiple Access with Collision Detection

nált 100BASE-T4 esetén a half-duplex működésre már nem a topológia miatt volt szükség, hanem azért, mert nem használtak hibrid áramköröket, így egy érpáron egyszerre csak egy irányba lehetett adatokat továbbítani, viszont a 100 Mbit/s sebesség eléréséhez a Cat3 minőségű kábelen egyszerre három érpárra volt szükség.

A rendelkezésre álló négy érpáron tehát nem maradt más lehetőség, mint két érpár felváltott használata egyszer az egyik, egyszer a másik irányban. A többi 1 Gbit/s-nál lassabb fizikai rétegnél maga a médium lehetővé tette a full-duplex működést is. Az IEEE 802.3 szabványba csak 1997-re került bele a full-duplex működés leírása (a 802.3x kiegészítésben), de full-duplex Ethernet termékek már valamivel korábban is léteztek (ami nem meglepő, különösen ha arra gondolunk, hogy a full-duplex működés a half-duplexhez képest szinte csak egyszerűsítés). A kábeleket összekapcsoló berendezések ára gyakran mégis indokolttá tette a jobb műszaki lehetőségek ellenére is a half-duplex mód használatát még éveken át. A switch-ek kezdetben ugyanis annyival drágábbak voltak a repeaterekné vagy a huboknál, hogy az csak kevés felhasználónak volt kifizetődő.

A GigabitEthernet fizikai rétegek mindegyike lehetővé tette a full-duplex működést, a szabvány alkotói mégis sok energiát fektettek abba, hogy megtartsák a half-duplex működés lehetőségét is. Ehhez az 1 Gbit/s sebesség miatt a carrier extension és a frame bursting bevezetésére volt szükség. A gyakorlat azonban azt mutatta, hogy – főleg a switch portok árának csökkenése folytán – a GigabitEthernetnél már senkinek sem volt szüksége a half-duplex működésre. Tehát az ahhoz szükséges két fent említett kiegészítés teljesen feleslegesen bonyolítja el a 802.3 szabványt.

A 10GigabitEthernet fizikai rétegben a GigabitEthernethez hasonlóan csak pont-pont összeköttetések lehetségesek, és minden 10GigabitEthernet fizikai réteg alkalmas full-duplex átvitelre. Ennek, és a GigabitEthernetnél tapasztalt fent említett tendenciáknak megfelelően a 10GigabitEtherneten már nincs half-duplex működés és az ahhoz szükséges CSMA/CD protokoll is hiányzik.

3. A 10 Gigabit Media Independent Interface (XGMII)

Az XGMII a MAC és a PHY (fizikai réteg) közti chip-to-chip interfész, azaz egy jól definiált elektromos felület a MAC és a PHY között, hogy azokat könnyű legyen egymástól függetlenül kialakítani. Az XGMII használata opcionális, de az IEEE szabvány az XGMII meglétét feltételezve specifikálja a különböző komponenseket. Az XGMII fizikailag tipikusan ASIC-en belüli logikai egységek között, vagy nyomtatott áramkörön valósulhat meg.

Ez utóbbi esetben az XGMII által összekötött MAC IC és PHY IC távolsága körülbelül 7 cm lehet, és az összeköttetésen HSTL (High Speed Transceiver Logics) jelszinteket kell használni.

Az XGMII irányonként (adás, vétel) egy-egy 32 bit széles adatbuszból, továbbá 4 vezérlő-, és egy órajelből áll. A jelzési sebesség az adatbuszon (és a vezérlő jeleknél) 312.5 Mbaud. A vezérlőjelekből derül ki, hogy a hozzájuk tartozó 8 bit az adatbuszon az Ethernet keret egy byte-ja, vagy valamilyen vezérlő byte (ami például a keret elejét, végét, vagy a keretek közti szünetet jelzi).

3.1. XGMII Extender, XAUI

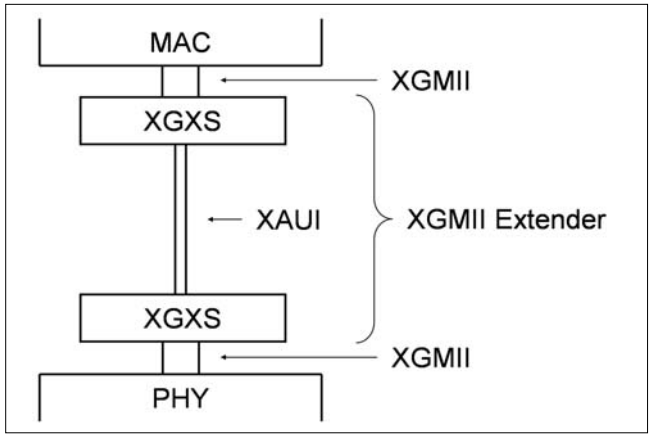
Az XGMII Extender célja az XGMII által nyomtatott áramkörön áthidalható kb. 7 cm távolság növelése (de még mindig csak egy nyomtatott áramkör méreteiben gondolkodva, hiszen így is csak kb. 50 cm lehet a távolság a MAC és a PHY között), valamint a párhuzamos vezetékek számának csökkentése. Az XGMII Extender nem más, mint a 10 Gigabit Attachment Unit Interface (XAUI) két végén kiegészítve egy-egy XGMII Extender Sublayer (XGXS) komponenssel. Ez a két XGXS biztosítja, hogy az XGMII Extender komplexum egészében kívülről mindkét vége felől úgy „nézzen ki”, mint egy egyszerű XGMII.

Az XAUI irányonként mindössze 4 vonalból áll (szemben az XGMII irányonkénti 37 vonalával). A vonalak differenciális meghajtásúak, a jelzési sebesség 3.125 Gbaud. Ez a jelzési sebesség a GigabitEthernetnél megismert 8B/10B kódolás használatából, és a vonalankénti 2.5 Gbit/s adatsebességből adódik. A 8B/10B kódolás nagyobb szimbólumterének köszönhetően nincs szükség külön vonalakra a jelzésekhez, és az órajel is visszanyerhető a jelfolyamból. A 8B/10B kódolást és dekódolást a két XGXS végzi, csak úgy, mint az órajel előállítását a 8B/10B dekódolási oldalon.

4. Fizikai réteg

Az itt tárgyalt fizikai rétegek közül a 10GBASE-T és a 10GBASE-LRM jelenleg kidolgozás alatt áll, még nem része a szabványnak, tehát ezekről még nincs véglegesnek tekinthető információ. A többi már megtalálható a szabvány aktuális változatában (IEEE 802.3-2005).

2. ábra XGMII Extender



4.1. Taxonómia

4.1.1. LAN és WAN fizikai rétegek

A 10GigabitEthernetnél megkülönböztethetünk úgynevezett LAN[5] és WAN[6] fizikai rétegeket. A LAN PHY (10GBASE-R, 10GBASE-T, és 10GBASE-X) az Ethernetnél már megszokott megoldás, amikor a médiumra az Ethernet keretek közvetlenül kerülnek (természetesen megfelelő kódolással), az adatkapcsolati rétegben szomszédos Ethernet állomások pedig kábelek és esetleg a fizikai rétegben működő aktív Ethernet hálózati eszközök (hub, repeater, media converter) segítségével kapcsolhatók össze egymással. A 10GigabitEthernet WAN PHY (10GBASE-W) ezzel szemben adáskor SDH/SONET[7] keretezéssel látja el az Ethernet kereteket, így két ilyen Ethernet állomás közé nem Ethernet aktív eszközöket, hanem SDH/SONET hálózatot, pontosabban egy SDH/SONET hálózaton megvalósított pont-pont összeköttetést „tehetünk”. A keretezésbeli különbségek miatt LAN és WAN PHY nem köthető össze egymással.

A LAN PHY elnevezés ne tévesszen meg senkit, itt a hálózat kiterjedését tekintve nem feltétlenül lokális hálózatról van szó, hiszen a LAN PHY-k között van olyan, ami 40 km hosszú szakasz áthidalására is képes – és akárhogy is nézzük, viszonylag kevés olyan LAN létezhet a világon, amiben ekkora hálózati szegmensek is előfordulnak.

4.1.2. Soros és párhuzamos fizikai rétegek

Osztályozhatjuk a fizikai rétegeket aszerint is, hogy hány jelfolyamot használnak a médiumon. A 10GBASE-R és a 10GBASE-W PHY-k egyetlen, körülbelül 10 Gbit/s sebességű jelfolyamot használnak – ezeket soros PHY-nek szokás nevezni. Ezzel szemben a 10 GBASE-T és a 10GBASE-X PHY-k négy kisebb sebességű párhuzamos jelfolyammal érik el a két szomszédos Ethernet állomás közt a 10 Gbit/s adatátviteli sebességet. A négy párhuzamos jelfolyam optikai szálon hullámhossz multiplexálással, réz kábelen pedig külön vezetők használatával valósul meg.

4.1.3. Átviteli közeg

A harmadik lehetséges szempont a 10GigabitEthernet fizikai rétegek osztályozására az átviteli közeg (médium). Ez lehet többféle optikai szálpár, lehet úgynevezett twinaxiális réz kábel, vagy lehet csavart érpáros réz kábel.

4.2. Soros fizikai rétegek

A soros (10GBASE-R és 10GBASE-W) fizikai rétegek nagy részének specifikációja 2002-re készült el. Ezeket az IEEE 802.3 szabvány 802.3ae jelű kiegészítése írta le (ami ma már része a szabvány 2005-ös kiadásának). Az egyetlen kivétel a jelenleg kidolgozás alatt álló 802.3aq jelű kiegészítésben [2] specifikált 10 GBASE-LRM.

4.2.1. 64B/66B PCS

A 64B/66B PCS (Physical Coding Sublayer) használatos mindkét soros PHY csoportnál, azaz a WAN PHY-k (10GBASE-W) és a soros LAN PHY-k (10GBASE-R) esetén is.

1. táblázat
10GigabitEthernet taxonómia

	10GBASE-SR	10GBASE-LRM	10GBASE-LR	10GBASE-ER	10GBASE-SW	10GBASE-LW	10GBASE-EW	10GBASE-LX4	10GBASE-CX4	10GBASE-T
	R				W			X		T
soros	■				■					
párhuzamos								■		■
LAN	■							■		■
WAN					■					
optikai szál	■				■			■		
twinax									■	
csavart érpár										■

Ez a PCS a 64B/66B blokk kódolást alkalmazza. Adáskor a MAC-től érkező adat byte-okat és vezérlőinformációkat először 64 bites blokkokba szervezi, majd minden ilyen 64 bites blokk elé két bit szinkronizáló fejlécet illeszt. A „01” fejléc azt jelenti, hogy utána 64 adatbit következik, azaz egy Ethernet keret 8 byte-ja. Az „10” szinkron bitek pedig azt jelentik, hogy a következő 64 biten vannak vezérlőinformációk (és esetleg adat byte-ok is). Ebben az esetben a 64 bitből az első 8 bit adja meg az adat és a vezérlőinformációk elrendezését a maradék 56 biten. A 66 bites kódszavak első két

5 LAN: Local Area Network, lokális hálózat
6 WAN: Wide Area Network, nagy távolságú hálózat
7 SDH: Synchronous Digital Hierarchy / SONET: Synchronous Optical Network

szinkron bitje „00” vagy „11” értékű nem lehet. Ez alapján, hogy a bitfolyamban pontosan 66 bitenként mindig vagy a „01” vagy az „10” minta fordul elő, a vevő oldali PCS azonosítani tudja a bitfolyamban a 66 bites blokkok határát.

A 66 bites blokkok hátsó 64 bitjén egy önszinkronizáló folyamkódoló alkalmazása biztosítja a megfelelő gyakoriságú szintváltásokat, hogy a vevő oldalon a jelfolyamból az órajel könnyen kinyerhető legyen.

Összegezve a fentieket, adáskor első lépés a 64 bites blokk összeállítása, utána következik a folyamkódolóval való „megkeverés”, majd végül a blokk tartalmának megfelelő két bites szinkron fejléc hozzáadása történik. Vételkor először a 66 bites blokkok határát kell megkeresni a szinkron fejlécek segítségével, utána visszaállítani a „megkevert” 64 bitet, és végül a szinkron fejléc tartalmának megfelelően kinyerni a 64 bites blokkból az adatokat és/vagy a vezérlőinformációkat.

LAN PHY esetén a 10GigabitEthernet adatsebesség (a MAC és a PHY között) 10 Gbit/s (azaz 10^{10} bit/s). A fizikai közegen a soros LAN PHY 64B/66B kódolásából adódóan így 10.3125 Gbaud a jelzési sebesség.

4.2.2. WAN PHY

10GBASE-W PHY használatakor az adatkapcsolati rétegben egymással szomszédos 10GigabitEthernet állomások közé SDH vagy SONET hálózatot, pontosabban egy SDH VC-4-64c vagy SONET STS-192c pont-pont összeköttetést kapcsolhatunk. (Ezeket konyhanyelven STM-64, illetve OC-192 néven szokás említeni.)

A vonali sebesség az optikai szálon ilyenkor 9.95328 Gbit/s, az adatsebesség pedig 9.58464 Gbit/s (az SDH/SONET fejlécek miatt). A MAC és a PHY között az átviteli sebesség ennél nagyobb, pontosan 10 Gbit/s. A különbség áthidalása érdekében WAN PHY esetén a MAC úgynevezett „IFS strech” módban működik, azaz adáskor keretenként a keret méretével arányos hosszúságú extra szünetet (idle szimbólumokat) iktat be, tehát az interframe gap a minimálisan előírtnál hosszabb lesz. 104 bitenként 8 bit extra interframe gap szükséges a sebességkülönbség kompenzálásához. Ezeket az idle szimbólumokat a PHY eldobja, így a VC-4-64c, illetve az STS-192c adatsebességnek megfelelő továbbítandó jelfolyamot kap.

Vételkor ennek a fordítottja történik, azaz a PHY szúr be szünetet a vett keretek közé, hogy a MAC és a PHY között meglegyen a 10 Gbit/s sebesség. A MAC-nek vételkor ezzel semmi különleges teendője nincs, hiszen az egyébként is teljesen normálisnak számít, hogy a vett keretek közt kisebb-nagyobb szünetek vannak.

A WAN Interface Sublayer (WIS) a 10GBASE-W fizikai réteg fontos komponense, melynek feladata adáskor a 64B/66B PCS-től kapott bitfolyam SDH/SONET keretezéssel való ellátása, illetve vételkor az adatok kinyerése az SDH/SONET keretekből. A keretezéssel együtt természetesen a WIS feladata az SDH/SONET fejlécekben szereplő jelzések, riasztások kezelése is.

4.2.3. Soros PMD

Soros 10GigabitEthernet fizikai rétegek többféle fizikai médiummal és többféle PMD-vel (Physical Medium Dependent sublayer) léteznek. A fizikai médium minden soros PHY esetén optikai szálpár.

Multimódusú szálpáron működik a Short Wavelength Serial PMD (10GBASE-SR és 10GBASE-SW PHY) 850 nm névleges hullámhosszon, valamint a 10GBASE-LRM PMD 1310 nm névleges hullámhosszon. Az áthidalható távolság a fényvezető szál megfelelő hullámhosszon mérhető modális sávszélességétől függ. Ezeket a *2. táblázat* foglalja össze (a könnyebb összehasonlítás érdekében szerepel a táblázat utolsó oszlopában a 10GBASE-LX4 párhuzamos PMD is, amiről bővebben a következő fejezetben lesz szó).

A 10GBASE-LRM PMD a 10.3125 Gbaud jelzési sebesség melletti 220, illetve 100 méteres távolság elérése érdekében a vevő oldalon elektronikus diszperzió kompenzációt alkalmaz.

1310 nm-es 10GBASE-LRM PMD multimódusú szálon való használata esetén úgynevezett „mode-conditioning patch” kábel beiktatása szükséges az adónál (hasonlóan ahhoz, mint például amikor nagyobb távolságú multimódusú szakaszon használunk 1000BASE-

2. táblázat
Multimódusú optikai szálon áthidalható távolság a kábel típusának függvényében
*(az első sorban szereplő 160/500 MHz*km modális sávszélességű kábel az ún. „FDDI grade” kábel)*

mag átmérő [µm]	modális sávszélesség [MHz*km]		áthidalható távolság [m]		
	850 nm	1300 nm	10GBASE-SR, -SW (850 nm, ~10 Gbaud)	10GBASE-LRM (1310 nm, ~10 Gbaud)	10GBASE-LX4 (1310 nm, ~3 Gbaud)
62.5	160	500	26	220	300
	200	500	33	220	300
50	400	400	66	100	240
	500	500	82	220	300
	2000	500	300	220	300

LX PMD-t). A probléma forrása a régi multimódusú szálaknál a gyártási technológia, ami miatt a sugár szerinti törésmutató profil a 0 környékén (a szál közepén) gyakran nem eléggé egyenletes, azaz viszonylag nagy ugrások lehetnek benne [3].

Ez a régebben használt – csak kisebb jelzési sebességekre alkalmas – LED fényforrás esetén nem okozott gondot, hiszen a széles szögtartományban világító LED-ből a szál magját betöltő fény (OFL, Overfilled Launch) energiájának csak kis hányada jut a szál hibás részére. Viszont a sokkal kisebb keresztmetszeten és szögtartományban sugárzó LASER fényforrással belevilágítva ugyanezen szálak közepébe az energiának igen nagy része jut a mag hibás középső részére, és ez könnyen elviselhetetlenül nagy DMD-hez (Differential Mode Delay) vezethet.

A probléma elkerülésére alkalmazott speciális patch kábel egy monomódusú és egy graded index multimódusú szakaszból áll, amelyek szándékosan excentrikusan vannak egymáshoz illesztve. A 10GBASE-LRM adó oldalára kerül a monomódusú szakasz, amiből a LASER által kibocsátott fénysugár a multimódusú kábelbe nem a közepén, hanem kicsit arrébb jut be, és ezáltal a régi multimódusú optikai kábelszakaszon elkerüli a mag feltehetőleg hibás középső részét.

Monomódusú szálpáron, 1310 nm névleges hullámhosszon működik a 10GBASE-LR és a 10GBASE-LW fizikai rétegben használt Long Wavelength Serial PMD. Az ezzel áthidalható távolság 10 km.

A legnagyobb áthidalható távolságot, 40 km-t az Extra Long Wavelength Serial PMD nyújtja. Ebben a csoportban is megvan a LAN (10GBASE-ER) és a WAN (10GBASE-EW) PHY. A használt médium természetesen monomódusú optikai szálpár, a névleges hullámhossz pedig 1550 nm. Ennél a PMD-nél az optikai szakasz csillapítása legalább 5 dB kell, hogy legyen. Ha ez nem adódik ki a kábel és a csatlakozók csillapításából, akkor megfelelő méretű csillapító tag beépítése szükséges.

4.3. 10GBASE-X fizikai rétegek

A két 10GBASE-X fizikai réteg közül a 10GBASE-LX4 az IEEE 802.3 szabvány 802.3ae jelű, 2002-es kiegészítésében szerepel. A 10GBASE-CX4 specifikációja 2004-re készült el, a szabvány 802.3ak jelű kiegészítéseként. Ma már mindkettő része a szabvány 2005-ös kiadásának.

4.3.1. 10GBASE-X PCS

A 10GBASE-X fizikai rétegek a GigabitEthernetből ismert 8B/10B blokk kódolást használják, amely 8 bites adatblokkokat képez le 10 bites szimbólumokra. A 10 bites kódszavak között az adat byte-ok megfelelőin kívül van még néhány érvényes, jelzésre használt kódszó is. Ezeket a speciális kódszavakat használja az 10GBASE-X PCS például a keretek elejének és végének megjelölésére, vagy a keretek közti szünetek kitöltésére. A 8B/10B kódolás lehetővé teszi bithibák detektálását. A kód úgy van kialakítva, hogy minden 10 bites kódszóban legalább 3 szintváltás legyen, így az órajel kinyerhető magából a csatornán vett adatfolyamból. Szintén detektálható egyéb vezérlőjelek nélkül – az idle szimbólumok segítségével – a kódszavak határa is.

A 10GBASE-X PCS feladata adáskor a MAC felől érkező 32 bites adatblokkok és vezérlőinformációk 8B/10B kódolása. Az így kapott négy kódszó 4 külön vonalon kerül a csatornára. Az idle szimbólumokat a PCS úgy választja meg, hogy az elektormágneses spektrum egyenletes, a fehér zajhoz hasonló legyen, tehát ne okozzon kellemetlen interferenciát.

Vételkor a PCS feladata a 10 bites kódszóhatárok detektálása vonalanként, majd a 4 kódszó egymáshoz igazítása, hiszen a négy vonalon keletkezhet átvitel közben egy kis csúszás a túloldalon egyszerre leadott szimbólumok közt. Ezután az így kapott négy 10 bites szimbólumot a PCS dekódolja, és továbbítja a MAC felé.

Mivel a 10GBASE-X PMD-k ugyanazt a kódolást használják, mint az XAUI, és mivel az XGMII interface használata opcionális, ezért 10GBASE-X PMD és XAUI együttes használata esetén a PHY és az XAUI közti XGXS, valamint a PHY PCS és PMA komponensei kihagyhatók, hiszen ezek ilyenkor feleslegesen konvertálnák a jeleket egyik formából a másikba és vissza. Ilyenkor tehát az XAUI közvetlenül csatlakozhat a PMD-hez, a PCS és a PMA funkcióját pedig az XAUI és a MAC közti XGXS látja el.

Ebben az esetben azonban szükséges lehet az XAUI-n keletkező esetleges jitter kompenzálására a PMD és az XAUI között.

4.3.2. 10GBASE-X PMD

A MAC és a LAN PHY közti 10 Gbit/s adatsebesség négy párhuzamos jelfolyamra bontása és a 8B/10B kódolás alkalmazása folytán a 10GBASE-X PMD jelzési sebessége 3.125 Gbaud.

A 10GBASE-LX4 PMD optikai szálpáron működik. Használható egyaránt mono- és multimódusú optikai szálakon is. Az áthidalható maximális távolság monomódusú szálon 10 km, 500 MHz*km modális sávszélességű multimódusú szálon 300 m, 400 MHz*km sávszélességűn pedig 240 m *(lásd 1. táblázat)*. Multimódusú kábel esetén itt is szükséges a 10GBASE-LRM PMD-nél tárgyalt mode-conditioning patch kábel használata. A négy jelfolyam átvitele az optikai szálon hullámhossz-osztásos multiplexálással (WDM) történik. A vivők (konyhanyelven lambdák) névleges hullámhosszai 24.5 nm-enként helyezkednek el az 1310 nm körüli optikai ablakban.

A 10GBASE-CX4 réz kábelen működik. Tipikusan géptermi alkalmazásokra készült, a vele áthidalható távolság mindössze 15 m. Az átviteli közeg 100 Ω impedanciájú, úgynevezett twinax kábel. A twinaxiális kábel felépítésében hasonlít a koaxiálisra, de a belsejében nem egy, hanem két – külön-külön szigetelt – vezető van, melyeket a 10GBASE-CX4 PMD differenciálisan hajt meg. A négy jelfolyam átvitele négy twinaxiális kábelen

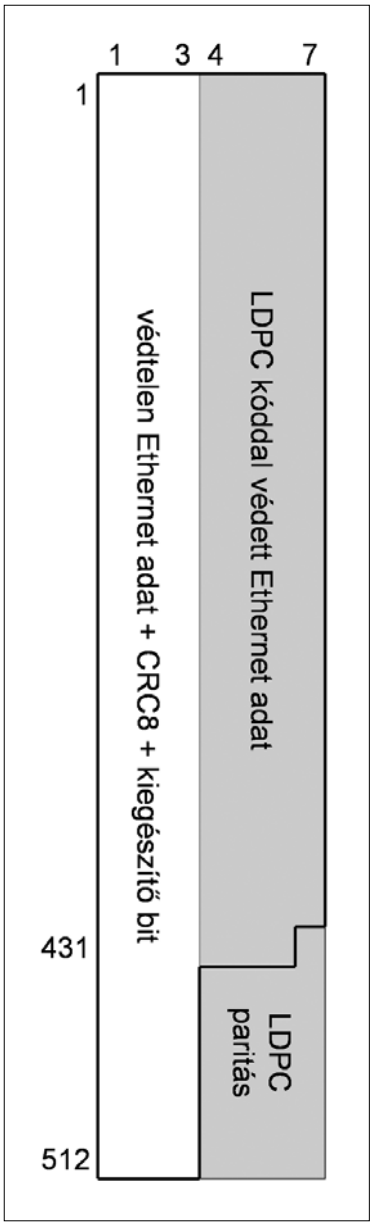
történik, így az adáshoz és vételhez egyszerre 8 twinaxiális kábelre van szükség. Az érintkezők száma 25, mivel a 8 érpár külön-külön, és a teljes kábel együtt is árnyékolva van. Az MDI csatlakozója az IEC 61076-3-113 előírásainak megfelelő Infiniband 4x típusú.

4.4. Csavart érpáros fizikai réteg

A GigabitEthernethez hasonlóan a 10 Gbit/s sebességű fizikai rétegek között is jóval később fog elkészülni a csavart érpáron működő változat, mint például az optikai szálpáron működő társai.

Ez azzal magyarázható, hogy a csavart érpáros kábel sávszélesség kapacitása jóval kisebb, mint egy optikai szálé, ezért komoly kódolási és jelfeldolgozási arzenál bevetésére van szükség a nagy adatátviteli sebesség eléréséhez. A 802.3 szabvány csavart érpáros (10GBASE-T) fizikai réteget leíró kiegészítése (802.3an [4]) jelenleg kidolgozás alatt áll, de várhatóan hamarosan elkészül.

A 10GBASE-T az Ethernet család kisebb sebességű tagjaihoz hasonlóan 4 csavart réz érpárból álló kábelt használ, bár a 10 Gbit/s sebességhez szükséges kábel valamivel bonyolultabb felépítésű – és ebből adódóan kedvezőbb átviteli tulajdonságokkal rendelkezik – mint a kisebb sebességekhez szükséges csavart érpáros kábelek.



3. ábra
Az LDPC kódoló alkalmazása

4.4.1. Auto-negotiation

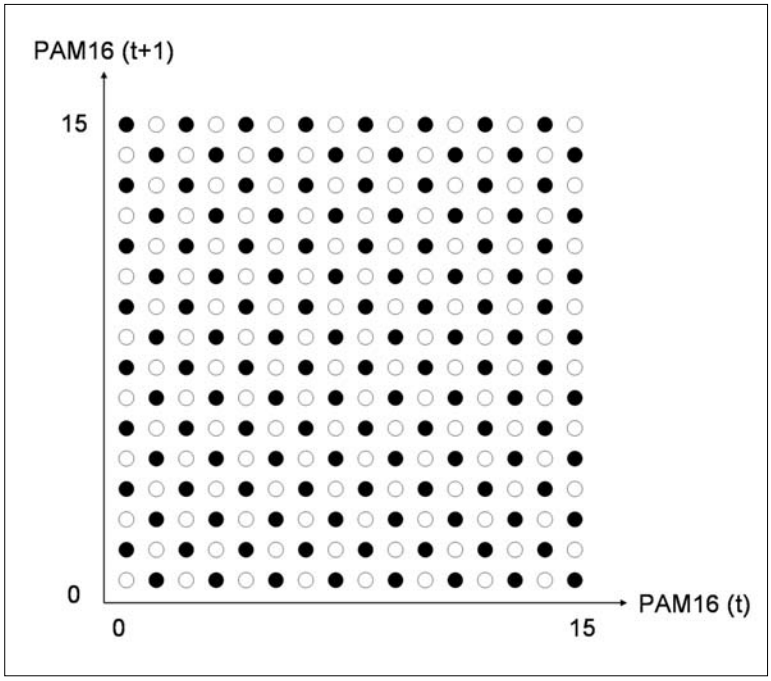
A 10GBASE-T a többi csavart érpáros Ethernet fizikai rétegnél megszokott auto-negotiationt használ. Az auto-negotiation alapvető funkciói nem változtak a 1000BASE-T-hez képest. Az eljárás ki van egészítve a 10 Gbit/s sebességű kapcsolathoz szükséges elemekkel, és néhány kisebb optimalizáláson is átesett, de természetesen a korábbi változatokkal felülről kompatibilis maradt. (A duplexitás egyeztetésére 10 Gbit/s sebesség esetén nincs szükség, de mivel a sebességet és a duplexitást úgy is egyszerre, egy paraméterben kezeli az auto-negotiation, ezért ez sem jelent lényegi változást.)

4.4.2. PCS

A kódolási lépések sorában adáskor az első a 64B/65B kódolás. Ez majdnem azonos a soros fizikai rétegeknél használatos 64B/66B kódolással. A különbség annyi, hogy itt kettő helyett csak egy bites a 65 bites blokkok fejléce, ami jelzi, hogy az utána következő 64 biten csak adat byte-ok vannak-e, vagy vezérlőinformációk is. (Az 1 bites fejléc értelemszerűen nem játszik szerepet a blokkhatárok detektálásában.)

A következő lépésben az adó összegyűjt 50 darab ilyen 65 bites blokkot, amihez 8 bit CRC-t (Cyclic Redundancy Check) ad, majd további 1 (hálózati információt nem hordozó) bittel egészíti ki. Ez utóbbi kiegészítésre azért van szükség, hogy összeálljon egy pontosan 3259 bites blokk, ami a kódolás következő lépéséhez kényelmes méret. Ebből a blokkból 3*512 bit (köztük az 1 kitöltő bit is) megmarad hibajavító kódolás nélkül, a másik 1723 bit mellé pedig LDPC (Low-Density Parity-Check) lineáris szisztematikus blokk kódolót [5] alkalmazva 325 bit paritás kerül.

Így az adó összesen 1723+325=2048=4*512 hibajavító kóddal védett bithez, továbbá 3*512 korábban „félretett” védtelen bithez jut. Ez együtt 512 db olyan 7



4. ábra
DSQ128 konstelláció

bites szóba rendezhető, ahol minden szó első 3 bitje védtelen, a második 4 bitje pedig hibajavító kóddal védett.

A csatornán, vagyis a csavart érpáros kábelen minden érpáron 16 szintű PAM (Pulse Amplitude Modulation) szimbólumokat küld az adó. Két, időben egymást követő, egyazon érpáron leadott PAM16 szimbólum 256 lehetséges kombinációjából az adó egy 2 dimenziós, 16*16-os mátrix minden második elemét sakktáblaszerűen elhagyó 128 elemű, maximális távolságú konstellációt használ. Az így kijelölt 128 db PAM16 szimbólumpárt a szabványtervezet DSQ128 (double square 128) szimbólumoknak nevezi.

Ezek a DSQ128 szimbólumok 8 db, egyenként 16 elemű, „csúcsára állított" négyzet alakú csoportba vannak osztva. A csoportok a 16*16-os mátrix széleinél a szemközti oldalon folytatódnak.

A fent említett 512 db 7 bites szó mindegyike egy-egy DSQ128 szimbólumot jelent a csatornán. A 128 elemű konstellációban a csoportot a 7 bites szó első 3 védtelen bitje jelöli ki, a 16 elemű csoporton belüli elemet pedig a szó hátsó 4 védett bitje határozza meg. Ez a módszer biztosítja, hogy a védtelen bitek esetleges módosulása a csatornán a nagy távolság miatt ne maradhasson észrevétlen, illetve könnyen javítható legyen. Az LDPC kóddal védett 4 bit módosulása esetén pedig a hibajavító kódolás segíthet a szimbólumok közti kis távolság ellenére is.

Összegezve a fentieket, az adó 50*64 bitből képez 512 db 7 bites szót, majd minden szót két PAM16 szimbólumban ad le. Ez 10 Gbit bemenetre $3.2*10^9$ PAM16 szimbólumot jelent, ami 4 érpárra elosztva $800*10^6$ szimbólumot eredményez érpáronként. A jelzési sebesség tehát 800 Mbaud.

Vételkor az LDPC dekódolás soft decision módszerrel, esetlegesen több iterációs lépésben történik. A dekóder bemenetére tehát még a 16 szintű A/D konverzió előtti, sokkal finomabb felbontású információ kerül, így gyakorlatilag nem vész el az az információ, amit az analóg jelszintek hordoznak. A dekóder a 16 diszkrét érték helyett – amivel hard decision módszer esetén dolgozna – valószínűségi változóként kezel minden PAM16 szimbólumot, és ezek eloszlását a vonalon vett, finom felbontású jelszint szerint határozza meg. Ezekhez a valószínűségi változókhoz próbál meg iterációs lépésekben olyan lehetséges értékeket keresni, aminek egyrészt nagy a valószínűsége, másrészt helyes LDPC paritást ad.

A vevő a potenciális dekódolt blokkot a 8 bites CRC-vel ellenőrzi, hogy vajon valóban sikerült-e a dekódolás, vagy csak véletlenül talált egy olyan bitsorozatot, amire az LDPC kód stimmel.

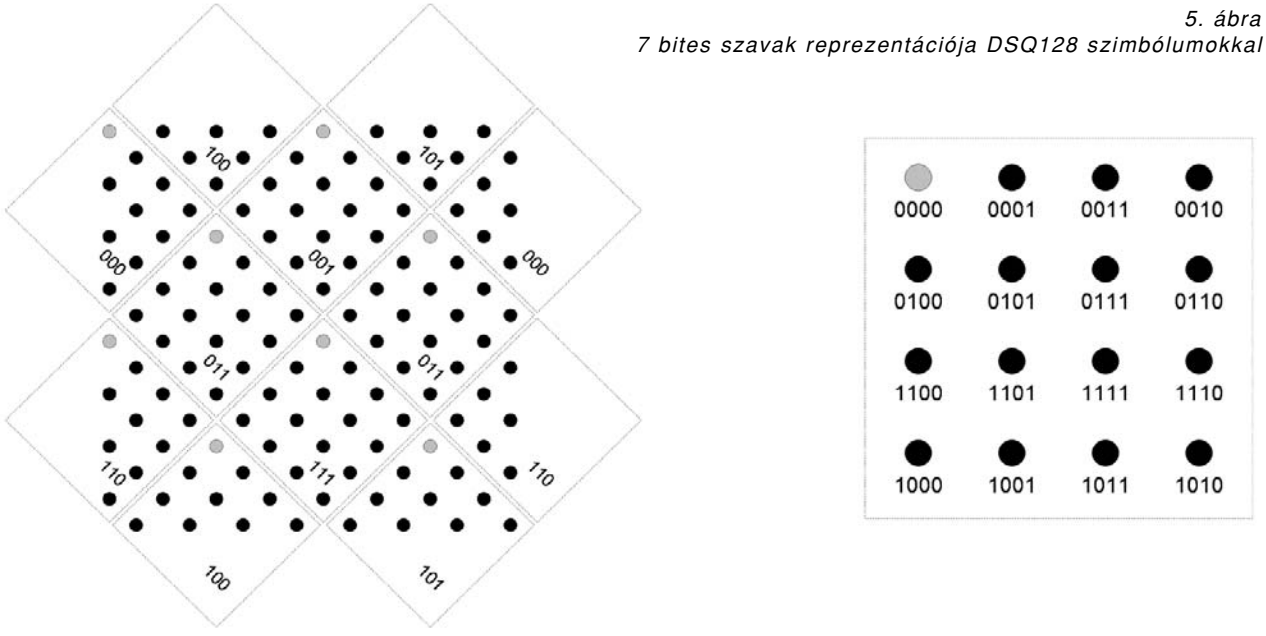
4.4.3. PMA

A csavart érpáros Physical Medium Attachment alréteg főként DSP (Digital Signal Processing) technológiákra épül.

Egyik fontos eleme adáskor a Tomlinson-Harashima Precoder használata. Ebben az eljárásban a szomszédos 10GigabitEthernet állomások a csatorna karakterisztikáját speciális teszt szimbólumok segítségével vizsgálják, majd adatátvitelkor equalizerek segítségével úgy torzítják a leadott jelet, hogy az minél jobban kompenzálja a csatorna előzetesen megállapított torzítását.

Az alkalmazott jelfeldolgozási módszerek másik lényeges csoportja a különféle visszhangok és áthallások miatt keletkező zavarok elnyomása. Visszhangok egyrészt a hibrid áramkörök, másrészt a különböző csatlakozókon keletkező reflexiók miatt adódnak. Áthallás keletkezik az adott kábel többi érpárja, valamint a közelben vezetett többi kábel szórt energiájából. Jól kezelhető az áthallások közül például a közeli áthallás (NEXT, Near-End Cross-Talk), mely az ugyanazon kábel

5. ábra
7 bites szavak reprezentációja DSQ128 szimbólumokkal



másik érpárjain adott jelek szórt energiáiból származik, hiszen itt a zavaró jel jól ismert, így viszonylag könnyű kompenzálni azt.

4.4.4. Médium

A 10GigabitEthernethez használható csavart érpáros kábel a Cat6a (augmented Category 6) minőségű UTP (Unshielded Twisted Pair) kábel. A Cat6a specifikáció egyelőre nincs készen, de várhatóan még 2006-ban megjelenik.

Az előzetes specifikációnak megfelelő kábelek jellemzően négy fő újítással érik el a jobb átviteli képességet. Az érpárok csavarása sűrűbb, intenzívebb, azaz egységnyi hosszon a korábbinál többször keresztezi egymást a pár két tagja. Az érpárok csavarásának intenzitása egymástól eltérő. Az érpárok térbeli pozicionálását rendszerint műanyag terelőidomok segítik a kábelen belül.

A kábel külső burkolata – és így az egész kábel – vastagabb, hogy a szomszédos kábel érpárjaitól való távolság nagyobb legyen. Ezek a változtatások mind a kábelen belüli és a kábelek közti áthallás, valamint az egyéb külső zavarok hatásának csökkenéséhez vezetnek.

4.4.5. A 10GBASE-T fennálló kihívásai

Az elért jelentős eredmények mellett a csavart érpáros 10GigabitEthernet létrehozásában fontos kihívást jelent egyrészt az interface komplexitása és hatékonysága közti megfelelő kompromisszum megtalálása, mind a különböző DSP komponensek, mind a dekóder esetén. Másrészt lényeges feladat az energiaigény leszorítása – ezen a téren mostanában a teljesítmény 10 W alá szorítása a cél.

Ezen fennálló problémák mellett az előrehaladást látva várható, hogy a 10GBASE-T specifikáció a közeljövőben elkészül, és utána hamarosan megjelennek az első termékek is.

4.5. Backplane Ethernet

Szándékosan nem szóltam idáig azokról az Ethernet fizikai rétegekről, amelyek a számítástechnikai készülékek belsejében az egyes modulok egymással való összekötésre kívánnak megoldást nyújtani, hiszen ez viszonylag távol áll az Ethernet megszokott adathálózati felhasználásától. De egy 10GigabitEthernetről szóló cikk nem lehet teljes ezek említése nélkül, hiszen backplane Ethernetről szóló IEEE 802.3ap tervezetben két 10GigabitEthernet fizikai réteg is szerepel.

A cél 1 méter távolság áthidalása az ilyen készülékek hátlapján jellemző környezetben. A kidolgozás alatt álló 10GBASE-KX4, illetve 10GBASE-KR ezt a korábban ismertetett (10GBASE-X vagy 10GBASE-R) jellemzőkkel valósítja meg.

5. Összefoglalás

Az Ethernet család a 10GigabitEthernet megjelenésével ismét egy nagyságrenddel gyorsabb tagokkal bővült a korábbiakhoz képest. Az IEEE 802.3 szabvány fejlődésében is megfigyelhető az a trend, ami az Ethernet alkalmazásában is, hogy az Ethernet egyre nagyobb teret hódít a LAN felhasználáson kívül is. Az átviteli közegeket tekintve a 10GigabitEthernet paletta hasonló, bár valamivel gazdagabb, mint a GigabitEthernet, és az egyes médiumok megjelenésének sorrendje – tükrözvén az adott probléma nehézségét, bonyolultságát – is hasonló.

A jövőt tekintve fontos eseménynek ígérkezik a 10GBASE-T eszközök megjelenése. Az azt követő jelentős újdonság talán az átviteli sebesség ismételt növelése lehet, de egyelőre nem tudni, hogy a következő lépcső a 40 vagy a 100 Gbit/s lesz-e.

Irodalom

[1] „IEEE Std 802.3-2005, Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications”, 2005. IEEE, ISBN 0-7381-4741-9

[2] „IEEE Draft P802.3aq/D3.1, Amendment: Physical Layer and Management Parameters for 10 Gb/s Operation, Type 10GBASE-LRM”, 2006. IEEE, ISBN 0-7381-1799-4

[3] Abott, J.S., et al.: „Analysis of Multimode Fiber Behavior with Laser Sources in the Development of the Gigabit Ethernet Fiber Optic Specification”, 1998. IWCS Proceedings

[4] „IEEE Draft P802.3an/D3.1, Amendment: Physical Layer and Management Parameters for 10 Gb/s Operation, Type 10GBASE-T”, 2006. IEEE, ISBN 0-7381-4889-X

[5] Gallager, R.G.: „Low-Density Parity-Check Codes”, 1963. The MIT Press, Cambridge, MA, http://web.mit.edu/gallager/www/pages/ldpc.pdf

[6] Langner, P., Woodruff, B., Kohl, B.: „10 Gigabit Ethernet on Unshielded Twisted-Pair Cabling, Moving 10 Gigabit Ethernet into a Volume Platform”, DesignCon 2006, http://www.ethernetalliance.org/technology/white_papers/

A WiFi rendszerek
multimédiás alkalmazásokra gyakorolt hatása

GÁL ZOLTÁN, KARSAI ANDREA, OROSZ PÉTER

Debreceni Egyetem Informatikai Központ
zgal@cis.unideb.hu, kandrea@fox.unideb.hu, oroszp@delfin.unideb.hu

Lektorált

Kulcsszavak: IPv4, IPv6, IEEE 802.11b/g, IEEE 802.11a, WiFi, L2/L3 roaming, VoIP, kodek, QoS, H.323

A WiFi hot-spotok kialakításánál alapvető kérdésként vetődik fel, hogy a 802.11b, a 802.11g, és/vagy a 802.11a szabványnak megfelelő rendszer telepítésére kerüljön sor. Ennek eldöntése gazdasági racionalitási megfontolásokon túlmenően hatékonyság elemzést is szükségessé tesz. Mivel egyetemi környezetben egyre jobban elterjednek az IP telefon rendszerek, feladatként jelenik meg a WiFi telefonok campus területén beltéri, illetve kültéri környezetben, mozgás közbeni használhatóságának elemzése. A cikkben ismertetjük az IEEE 802.11a, 802.11b, 802.11g WiFi átviteli technikák segítségével működtetett multimédiás (videó, streaming, IP telefon) alkalmazások minőségét befolyásoló jellemzőket.

1. Bevezetés

Az IEEE 802.11 családhoz tartozó vezeték nélküli adatátviteli mechanizmusok a mobilitás miatt széles körben terjedtek el úgy beltéri, mint kültéri környezetben. A hotspotok kialakításánál alapvető kérdésként vetődik fel, hogy a 802.11b/g és/vagy a 802.11a szabványnak megfelelő rendszer telepítésére kerüljön-e sor. Ennek eldöntése gazdasági racionalitási megfontolásokon túlmenően hatékonyság elemzést is szükségessé tesz. Mint ismeretes, a WiFi rendszer az ISM frekvencia sávokra épül, ami lehetővé teszi, hogy ugyanazon fizikai környezetben egymástól függetlenül akár több szolgáltató is hot-spotokat telepítsen. A gyakorlati tapasztalat szerint kültéri környezetben a különböző szolgáltatók a használt rádiós csatornákat egymás között egyeztetés nélkül, vagy csak ritkán egyeztetett formában használják. Mivel a kisugárzott mikrohullámú energiára ETSI szabványok vonatkoznak, a sűrűn telepített WiFi rendszerek egymásra zavaró hatással vannak.

Céges, illetve egyetemi környezetben egyre hangsúlyosabban fogalmazódik meg az igény, hogy a WiFi mobil eszközök (notebook, palmtop, intelligens mobil telefon) multimédiás szolgáltatásokat is biztosítsanak. Mivel egyetemi környezetben egyre jobban elterjednek az IP telefon rendszerek, egyértelmű feladatként jelenik meg a WiFi telefonok campus területén beltéri, illetve kültéri környezetben, mozgás közbeni használhatóságának elemzése.

A 2,4 GHz-es ISM tartományban a WiFi IP telefon beszédtovábbítási tulajdonságai a hangkódolási algoritmustól függnek. Az 5 GHz-es WiFi átvitel speciális csatornakódolási mechanizmusa hatékonyabb, mint az IEEE 802.11g esetén, ugyanakkor az átviteli sebesség nagyon érzékeny a bázisállomástól mért távolságra. Mozgás közben a nagyobb tömörítési aránnyal működő adatátviteli szabvány érzékenyebb a rádiós cellák közötti váltásra, mint az alacsonyabb tömörítésű algoritmus.

Előzetes elemzések alapján ismerjük, hogy a mobil terminálokon használható multimédiás szolgáltatások minőségét erőteljesen befolyásolja a készülék roaming közbeni fizikai mozgásának sebessége [1]. A mobil terminálokon működő multimédiás alkalmazások minősége erőteljesen függ az adatkapcsolati rétegben lejátszódó folyamatoktól.

2. Multimédia kódoló/dekódoló technológiák áttekintése

A DSP (Digital Signal Processing) architektúrák utóbbi években bekövetkezett látványos fejlődése, valamint a humán beszédfelismerés területén végzett kutatásoknak köszönhetően a hang kódoló/dekódoló (kodek) technológiák komoly előrelépést tettek[2]. Az új kodekek az egyszerű AD/DA átalakításon túlmenően, a becslő minták alkalmazása segítségével a bemenő hangjelet analizálják és minimális sávszélességet igénylő adatfolyamként képesek tovább küldeni.

1.1. PCM

Az egyszerű PCM (Pulse Code Modulation) kódolású hang az ITU-T G.711-es szabvány szerint történik[3]. A 64 kbps-os PCM hang tömörítése a μ-law és az A-law eljárásokkal valósul meg úgy, hogy a 12, 13 bites mintavételt logaritmikus törvény szerint képezi le 8 bitre. A két leképezési törvény analitikus formáját az *1. és a 2. ábra* mutatja (a következő oldalon).

Előnyök: egyszerű, kis komplexitású, kis késleltetés, jó hangminőség. Hátrány: nagy sávszélesség igény.

1.2. ADPCM

Az ADCPM (Adaptive Differential Pulse Code Modulation) ugyancsak gyakori kompressziós megoldás, amely az ITU-T G.726 szabványban van rögzítve. Ez négybites mintákat alkalmaz, amelyeket 32 kbps-os szállítási sebességgel továbbít. A PCM-mel ellentétben

$$y = \mathrm{sgn}(x) \cdot \frac{\ln(1+\mu\cdot|x|)}{\ln(1+\mu)},$$

ahol:
y – normalizált kimenet, [-1, 1] között
x – normalizált mintavétel, [-1, 1] között
μ = 255, kompressziós paraméter

$$y = \begin{cases} \dfrac{A}{1+\ln(A)}x, & ha \quad |x| \le \dfrac{1}{A} \\ \dfrac{\mathrm{sgn}(x)}{1+\ln(A)}\cdot\left(1+\ln|Ax|\right) & ha \quad \dfrac{1}{A} < |x| \le 1 \end{cases}$$

ahol:
y – normalizált kimenet, [-1, 1] között
x – normalizált mintavétel, [-1, 1] között
A = 255, kompressziós paraméter

1-2. ábra A PCM μ-law és PCM A-law eljárások

a négybites szók nem közvetlenül a beszéd amplitúdóját kódolják, hanem az amplitúdók különbségét és a változások rátáját. Ehhez egy nagyon egyszerű lineáris becslést alkalmaz.

Előnyök: egyszerű, kis komplexitású, jó minőségű hang, kis késleltetés, több kódolási sebesség. Hátrányok: viszonylag nagy sávszélesség igény, kis sávszélességen a hang minősége romlik.

1.3. AMR-NB

Az AMR-t (Adaptive Multi Rate – Narrow Band) a GSM és az UMTS mobilhálózatokban használják. Az algoritmus nyolc kompressziós arányt támogat (4,75; 5,15; 5,90; 6,70; 7,40; 7,95; 10,20; 12,20 kbps). Az algoritmus bármikor képes váltani ezen arányok között, ami IP alapú hálózatokban előnyt jelent. A küldő bármikor megváltoztathatja a kimenő sávszélességet az RTP által valós időben szolgáltatott statisztikák alapján: az RTP réteg visszajelzésére a kódoló a következő hangmintákat már a megváltozott kódolási sebességgel tömöríti, és ezt a dekóder ugyanúgy dekódolni tudja. A 20 ms-os műsorkeretek kódolása ACELP algoritmus alkalmazásával, és 5 ms lookahead értékkel történik.

Előnyök: egyszerű, viszonylag kis komplexitású, kis sávszélesség igény, kis késleltetés, jó hangminőség, több kódolási sebesség. Hátrányok: még kevés implementáció létezik, nincs nyílt forráskód.

1.4. AMR-WB

Az AMR-WB (Adaptive Multi Rate – Wide Band) mechanizmust a G.722.2 kódoló alkalmazza, amely nagy sávszélességre optimalizált ACELP algoritmust használ és 7 kHz-es hangjelet kódol 16 kHz-en mintavételezve. Adaptívan változtatja a kódolási sebességet (23,85; 23,05; 19,85; 18,25; 15,85; 14,25; 12,65; 8,85; 6,6 kbps). A kódoló 20ms hosszúságú kereteket és 5ms lookahead buffert használ.

Előnyök: nagyon jó minőségű hang, kis késleltetés, több kódolási sebesség. Hátrányok: nagy sávszélesség igény a jó minőségű hanghoz, közepesen nagy számolási komplexitás.

1.5. Az RTP protokoll

Az RTP (Real-Time Protocol) valós idejű forgalom számára végponttól-végpontig terjedő szállítási szolgáltatást (hang, kép) biztosít. Ehhez olyan szolgálatokat vesz igénybe, mint a PDU azonosítás, sorszámozás, időbélyegzés, és az átvitel felügyelete. Az RTP protokoll alkalmazás szintű keretezést valósít meg. Általában UDP felett alkalmazzák, felhasználva annak multiplexelési és ellenőrző összeg képzési szolgáltatásait, de ritkán TCP felett is működtetik. Az RTP nem garantálja a csomagok megérkezését, és a helyes sorrendben érkezést sem.

A mechanizmusnak két része van, az RTP és az RTCP (Real-Time Control Protocol). Az RTP PDU-k a valós idejű adatot szállítják, míg az RTCP PDU-k az átvitel minőségére és az entitásokra vonatkozó vezérlő információkat továbbítanak. Az RTP az IP hálózatokra jellemző változékony és túlterhelt hálózati feltételre van optimalizálva. Az RTP a tartalom adatokat továbbítja egyik irányba és az RTCP kétirányú csatornáit használja a minőségi jellemzőket is magába foglaló vezérlő információk számára. Az RTP viszony kiépítésekor az alkalmazások meghatározzák mind az RTP, mind az RTCP számára a műsor csatornánkénti szállítási címét. Ez entitásonként az IP hálózati cím és a portszám páros lesz. Minden RTP csomagnak fix szerkezetű fejléce van, amelyet a *3. ábra* szemléltet.

Az első tizenkét bájt minden RTP csomagban megtalálható, viszont a közreműködő forrás azonosítók listája (CSRC) csak akkor fordul elő, ha azokat a keverő elhelyezte a csomagba. A mezők jelentése az alábbi:

- *V:* verzió (jelenleg 2)
- *P:* kitöltés (Padding), ha a bit értéke 1, akkor a csomag végén vannak kitöltő bájtok, amelyek nem a tartalom adat részei. Az utolsó kitöltő bájt tartalmazza, hogy hány kitöltő bájtot kell figyelmen kívül hagyni. Kitöltésre lehet szükség, például fix blokkméretű titkosító algoritmus alkalmazásánál.
- *X:* kiterjesztés (Extension) : ha értéke 1, akkor a fix fejléc után következik pontosan egy fejléc kiterjesztés.
- *CC:* közreműködő forrásszámláló (CSRC Count): a fix fejléc után következő közreműködő forrás azonosítók száma.
- *M:* jelző (Marker) : a jelző bit értelmezése az alkalmazás profilban van meghatározva. Jelezheti például a képkockák határát a csomagfolyamban.
- *PT:* tartalom adat típus (Payload Type): az alkalmazás profilban adott, hogy a típuskódhoz milyen tartalom adat formátum tartozik. Egy RTP adó egy adott tartalom adat típust bocsát ki egy viszonyban.

– *SN:* sorszám (Sequence Number) egyesével növekszik, minden elküldött csomaggal. A vevő ezáltal tudja észlelni, ha csomagvesztés történt, illetve helyre tudja állítani a sorrendet. Biztonsági okokból a kezdeti értéke véletlengenerált szám.
– *TS:* időbélyeg (Time Stamp) az RTP csomag adatrészében található első bájt mintavételezési időbélyege monoton és lineárisan növekvő órától származik. A kezdőérték itt is véletlengenerált szám. Egymás utáni RTP csomagoknak lehet ugyanaz az időbélyege, ha egyszerre keletkeztek, például ha ugyanahhoz a képkockához tartoznak. Az egymás után küldött csomagokban található időbélyegek nem feltétlenül monoton növekvők, ha az adatok nem a mintavételezésük sorrendjében kerülnek továbbítására, mint például az MPEG interpolált képkockáinál.
– *Szinkronizációs forrás* (SSRC) azonosító: azonosítja a forrást szinkronizáció céljából. Véletlen módon választott azonosító, minden forrásra egyedi. Ha megváltozik a szállítási cím, akkor meg kell változtatni az SSRC azonosítót is.
– *Közreműködő forrás* (CSRC) azonosító: 0-15 db, egyenként 32 bit, azonosítja az adatfolyamhoz tartozó közreműködő forrásokat. Ezt a keverő helyezi el a fejlécben, a közreműködő források SSRC azonosítóit felsorolva, így a vevő azonosítani tudja az adókat.

E mezők felhasználásával az RTP olyan funkciókat tud ellátni, mint az idő helyreállítás (időbélyeg mező), adó-azonosítás (SSRC), tartalom azonosítás (PT), sorszámozás, veszteségészlelés. Nem az RTP hatáskörébe tartoznak a szolgáltatás minőség garantálása, az erőforrásfoglalás, az időben történő kézbesítés, valamint a csomagvesztés helyrehozása. Mindezek mellett az RTP alkalmas valós idejű tartalom szállítására.

Az RTCP-t az RTP-vel együtt használják és elsősorban az RTP átvitelének a monitorozására, illetve szabályozására szolgál. Célja az adatátvitel minőségéről és a viszony résztvevőiről való értesítés. Az RTCP működése a szabályozó csomagok viszonybéli összes résztvevőnek való időnkénti újraküldésén alapul.

Az RTCP is UDP felett fut. Több fajta RTCP csomag van, amelyek a vevő-jelentést, az adó-jelentést, a forrásleírást, a kapcsolatbontást és az alkalmazásra jellemző feladatkör-információt tartalmazza. A különböző típusú csomagok szerkezete eltérő, viszont több különböző csomagot egybe lehet fogni, és együttesen lehet elküldeni.

1.6. Hangkódolók/dekódolók csoportosítása

A PCM és az ADPCM a *hullámforma kodekek* csoportjába tartoznak, amelyek a hullámforma redundáns karakterisztikáit használják fel. Az utóbbi 10-15 évben kifejlesztett más kompressziós technikák a beszéd forrás karakterisztikáira építenek. Ezek jelfeldolgozás és tömörítés segítségével az eredeti beszédjelnek csak az egyszerűsített paramétereit küldik el, így kisebb sávszélességet igényelnek. Ezeket *forrás kodekeknek* nevezzük és ide tartoznak az LPC (Linear Predictive Coding), a CELP (Code Excited Linear Prediction), valamint az MP-MLQ (Multipurpose Multilevel Quantization) eljárások. A fejlett becslő kodekek az emberi beszédjel forrást matematikai modellel helyettesítik és tömörített hangküldés helyett a hang reprezentációját továbbítják.

A legnépszerűbb telefon hangkódolási és csomagkapcsolt hang szabványok az alábbiak:

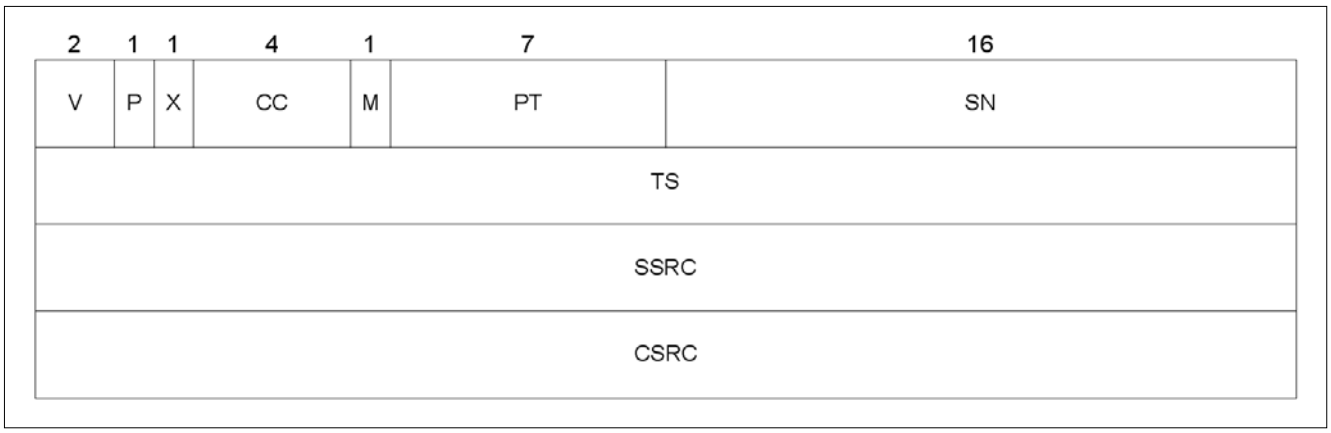
• *G.711:* A 64 kbps PCM hangkódolási technika, amely a hagyományos digitális PBX központokban, illetve hálózatokban használatos.

• *G.726:* Ez 40, 32, 24, 16 kbps-os ADPCM kódolást használ. Az ADPCM hang a csomagkapcsolt és a hagyományos PBX hálózatok közötti hangátvitelhez javasolt.

• *G.728:* Ez a CELP tömörítés kis késleltetés ingadozásos változatával 16 kbps-os sávszélességen továbbítja a beszédet. A CELP hangot transzkódolni kell nyilvános telefon formátumra ahhoz, hogy nyilvános végpontokkal sikeres kommunikáció jöhessen létre.

• *G.729:* Ez CELP tömörítéssel a hangot 8 kbps-os jelfolyammá alakítja. A két alváltozata a processzálás komplexitásában lényegesen különbözik egymástól, és mindkettő a 32 kbps-os ADPCM-nek megfelelő beszédminőséget biztosítja.

3. ábra Az RTP PDU fejrészének formátuma



• *G.731:* Ez beszéd vagy multimédiás szolgáltatás hang komponensének tömörítését végzi, nagyon alacsony sávszélesség mellett. A H.324 protokoll család részeként az 5,3 kbps, illetve a 6,3 kbps sávszélességen dolgozik. Előbbi CELP, utóbbi pedig MP-MLQ technológiát alkalmaz, miközben jó minőségű beszédátvitelt és további rugalmasságot biztosít a rendszer számára.

• *GSM:* A GSM (Global System for Mobile Communications) az ETSI I-30036 szabványa, amely széles körben használt az európai mobil rádióhálózatokban hang és kis sávszélességű adatkommunikációra. A GSM teljes sebességű hangkódoló 13 kbps sebességen működik és RPE (Regular Pulse Excited) kódolót használ 8 kHz mintavételezési frekvencia mellett. A félsebességű GSM kódoló 7 kbps sávszélességet igényel 5 kHz mintavételezés mellett. A bemeneti hang 20 ms hosszúságú keretekre van osztva és minden keretre 8 rövid távú becslést végeznek. Ezután minden keret további 5 ms hosszúságú alkeretekre bomlik, melyekre a kódoló késleltetést és nyereséget számol a hosszú távú becslő számára. Végül a maradék jelet kvantálja minden alkeretben.

A GSM kódoló jó minőségű hangot generál, mindazonáltal a G.728 kódoló (CELP) mégis felülmúlja a nagyobb sávszélességgel. A GSM kódoló kis számításigényű. Előnyök: egyszerű, viszonylag kis komplexitású, kis sávszélesség igény, kis késleltetés, nyílt forrás. Hátrányok: a sávszélesség/hangminőség arányban a G.729 felülmúlja.

1.7. A NullSoft Video protokoll

A NullSoft Video (NSV) formátum egy olyan bitstream jelfolyam, amely képes biztosítani a hang és a videó közös becsomagolását [4]. A gyakorlatban alkalmazott mindegyik hang- és videó tömörítési mechanizmussal együttműködik. Mivel bitstream formátum, így nem igényli a teljes fájl letöltését a lejátszáshoz. Képes streaming szolgáltatásra, megbízható szinkronizálás valósul meg a jelfolyam bármely pontján. Másodlagos adatcsatornák segítségével több hang-, feliratozás-, vagy más adatfolyam is biztosítható. Az NSV fájl szerkezete két fő részből áll: egy opcionális fájl fejrész és egy kötelező bitstream alkotja. Minden több bájtos egész szám LSB formátumban van ábrázolva, azaz a legkisebb helyiértékű bájt baloldalon helyezkedik el. Így egy négy, illetve egy húszbites szám három bájtot fog elfoglalni.

Az NSV fájl fejrész formátuma: Az NSV fájlnak csak egy fájl fejrésze lehet, amely tartalmazza a fájl méretét bájtokban és ezredmásodpercben, a tartalomjegyzéket, amely a VBR tartalom szabatos keresését biztosítja, és a metaadatokat. A fájl fejrész tartalmazhat további olyan információkat, mint a műsor címe, szerzője, javasolt képernyő oldalméreteinek aránya stb. A metaadat bármennyi név-érték párt tartalmazhat.

Az NSV fájl fejrész tartalom tábla (TOC, Table of Contents) formátuma: Négybájtos egész számok tömbje. A TOC v1.0 esetén a bejegyzés sorszáma a bejegyzés idejével arányos. A bejegyzés értéke képezi az NSV bitstream-ben elfoglalt offset pozíciót. Nagyobb fájl esetén a keresés pontatlan volt. A TOC v2.0 esetén viszont adott bejegyzés a kulcskeret offset-jét adja a bitstream részletben, míg a tartalom méretével növelt sorszámú bejegyzés a kulcskeret abszolút helyét mutatja. Ez pontos keresést tesz lehetővé.

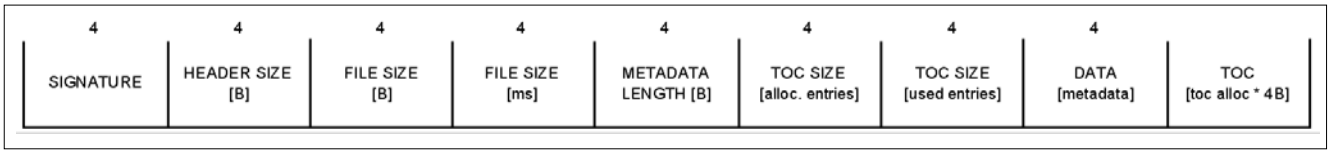
Az NSV bitstream formátum: A jelfolyam NSV kereteket tartalmaz, amelyek lehetnek szinkronizációs vagy nem-szinkronizációs keretek. Az NSV jelfolyam legalább egy szinkronizációs keretet kell, hogy tartalmazzon. A kétfajta keret az első részben különbözik egymástól, de mindkettő tartalmaz hasznos teher részt is. A szinkronizációs keret a műsor leírását tartalmazza. Ez maga a videó kulcskeret vagy közvetlenül előtte kell hogy legyen. A nem-szinkronizációs keret több hasznos terhet szállít, de nem tartalmaz járulékos információkat. Ezeket alacsonyabb sávszélesség esetén alkalmazzák.

A hasznos teher minden esetben az aktuális adattípus kódját és magát az adatot tartalmazza. A típuskód függvényében az adat szerkezete beazonosítható, így az adat struktúra a további csatornák és műsorjellemzők adatait is tartalmazhatja. A hang és a videó adat csomagok egy-egy keretben továbbítódnak. Igénytől függően a hang megelőzi vagy követi a videót. A kiegészítő információk (műsor címe, 16:9/4:3 megjelenítési arány, másodlagos hang csatorna stb.) csatornáinak száma összesen 15 lehet.

2. A VoIP hálózat jellemzői

Miután a hang tömörítése és adattá konvertálása megtörtént, az RTP (Real Stream Protocol) segítségével az IP hálózaton megtörténik a jelfolyam továbbítása. VoIP hálózatban úgy a sávszélességet, mint a hálózat késleltetését figyelembe kell venni. A sávszélesség igények kritikusak és nem csak a kiválasztott kodektől függ, hanem az egyes protokollok (IP, UDP stb.) overhead-jétől is [5]. A késleltetés a jelterjedési sebességtől, a küldő és a fogadó csomópont pufferének kezelési mechanizmusától, valamint a csomagolási késleltetéstől függ.

4. ábra Az NSV PDU fejrészének formátuma



2.1. Sávszélesség követelmények a VoIP hálózatban

A hang párbeszéd IP hálózat feletti működését több tényező befolyásolja. Az alkalmazott kodek sávszélesség igénye a 3...64 kbps tartományban lehet. A hang protokoll adatelem (PDU) leggyakrabban 20 bájtnál rövidebb, míg az L2 (Ethernet) és az L3 (IP) rétegek szignifikáns overhead-et képeznek. Emiatt a valós fizikai sávszélesség igényt nagymértékben az overhead-ek befolyásolják [6].

E probléma egyszerűsítésére különböző megoldásokat vezettek be. Hangaktivitás felismerés (VOD, Voice Activity Detection) segítségével a küldő a csomagolt jelfolyamot megszakítja, ha a lokális analóg forrás jelszint egy megadott küszöbérték alá kerül. Ezáltal a sávszélesség igény közel felére csökken, mivel a humán beszélgetés közben várhatóan a személyek fele ideig a másikat hallgatják. Ez a megoldás viszont körültekintést igényel a ki/bekapcsolási pillanatok meghatározásánál, mivel taralom kieséseket okozhat. Ugyanakkor a beszélgetés közbeni teljes csend is zavaró lehet. Emiatt alkalmazni szokták a komfort zajt, amely a nem beszélő fél párjánál a hangszóróban lokálisan generált halk fehérzajként jelenik meg.

Fejlettebb rendszerek a távoli környező háttérzajt reprodukálják a távoli személy hallgatási időintervallumaiban. Egy másik megoldás az RTP PDU fejrészének tömörítése. Mivel az RTP PDU fejrészében több információ duplikált vagy redundáns módon jelen van, az útvonal mentén elhelyezkedő routerek a fejrészt tömörítik, így a beszéd számára szükséges sávszélesség lényegesen csökken. A leggyakoribb LAN/MAN technológiai környezetben a szükséges fizikai sávszélesség az *1. táblázat* szerint alakul. Az IP/UDP/RTP 40 bájt, az Ethernet pedig 14 bájt overhead-et képez.

Minden egyes beszédkapcsolat két hívás jelfolyamot, míg a videókapcsolat négy vagy hat egyidejű hívás jelfolyamot jelent.

2.2. Késleltetés a VoIP hálózatban

A VoIP rendszerek tervezésénél általánosan elfogadott szabály, hogy a végponttól végpontig terjedő késleltetés 150 ms alatt maradjon. A ma használatos médiák átviteli késleltetése önmagában az emberi fül számára ugyan nem érzékelhető, a kezelési késleltetéssel együttesen azonban már észrevehető torzulást okozhat. Felhasználói részről a késleltetés tolerancia küszöbe 250 ms. Ennél nagyobb késleltetést elszenvedett hangfolyam interferál a természetes hangfolyammal, így kiolthatják egymást, torzulás érzékelhető. A kezelési késleltetés befolyással van a hagyományos vonalkapcsolt telefonhálózatokra is, de a csomag alapú átvitelnél a pufferelés miatt jelentősége erősen megnő. Ezért a késleltetés tervezésénél ezt 150-200 ms alatt kell tartani.

A G.729 szabvány algoritmus szerinti késleltetése 20 ms körül van, amelynek tervezésénél számításba vették a jövőbeli igényeket is. Egy VoIP termék általánosan 10 ms-onként generál egy keretet, majd párosával helyezi ezeket csomagba, így a késleltetés értéke 20 ms lesz. Csomag alapú hálózat esetén a késleltetés származhat egyrészt az aktuális csomag kimeneti sorba való helyezéséből, másrészt a sor késleltetéséből. Ennek értéke eszközfüggő, optimális esetben nem haladja meg a 30 ms-ot.

A VoIP alkalmazások nemcsak a késleltetésre, hanem annak változására is érzékenyek. Ellentétben a vonalkapcsolt hálózatokkal, a csomagkapcsolt átvitelinél a késleltetés értéke a hálózati forgalomtól függően erősen ingadozhat. A dzsitter a késleltetésnek rövid időn belüli változása, azaz a csomag várt és valós érkezési időpontja közötti ingadozás. Az eszközök ezt „playout" pufferekkel kompenzálják, hogy a hang vételében ne legyenek szakadások. Ez a teljes rendszer késleltetését tovább növeli. A puffer mérete lehet fix méretű, illetve bizonyos eszközöknél adaptív. VoIP esetében a dzsitter a minőséget legszembetűnőbb módon akadályozó paraméter. Általában a csomagkapcsolt hangátvitelnél a forgalom különböző késleltetésű, és minőségi paramétereket nyújtó rendszereken halad keresztül. Ezek alapvetően gyenge minőséget eredményeznek. Az ilyen alkalmazások általános jellemzője a nagyméretű fogadó oldali puffer, amely általában egy másodperc feletti hanganyag pufferelését teszi lehetővé.

2.3. Szolgálat minőség a VoIP hálózatban

A csomagkapcsolt hálózatokban a hangminőséget döntően befolyásolja a hálózatra jellemző késleltetés és a dzsitter, így a hálózatok tervezésénél különös figyelmet kell fordítani a QoS paraméterek biztosítására. További lényeges szempont a hangforgalomnak az adatforgalomtól való védelme, valamint a kritikus adatforgalom védelme a hangforgalom esetleges nagyobb sávszélesség-foglalásával szemben. A hatékony QoS tervezés elemei a megfelelő sávszélesség, a csomagvesztés, a késleltetés, és a dzsitter. E tényezők megfelelő szintű biztosítása a következőkben felsorolt leggyakoribb eszközökkel történik.

1. táblázat VoIP/csatorna sávszélesség összehasonlítás

Algoritmus	*Hang sávsz. [kbps]*	*Kodek késleltetés [msec]*	*Hang PDU méret [B]*	*Hang ráta [PDU/sec]*	*L2 PDU méret [B]*	*Fizikai sávsz. [kbps]*
G.729	8,0	15,0	20	50	74	29,60
G.711	64,0	1,5	160	50	214	85,60
G.723.1	6,3	37,5	30	26	84	17,47
G.723.1	5,3	37,5	30	22	84	14,78

– *Vezérlési stratégia:* Forgalom limitálás, mely a csomagok eldobását jelenti, amennyiben az adott hálózati eszközök közötti forgalom túllép egy megadott küszöbértéket. Ez megadható az eszközre bemeneti vagy kimeneti oldalon. Tipikus példája a RED (Random Early Detection) és a WRED (Weighted RED). Ezek a technikák beazonosítják azokat a csomagokat, amelyek szükség esetén eldobhatók.

– *Forgalomtervezés:* Egyenletes bemenő és kimenő rátájú csomagmennyiség alapján biztosítja a pufferelést. A vezérlési stratégiával ellentétben a forgalomtervezés igyekszik elkerülni a csomagok eldobását, ezzel viszont növeli a pufferelésből származó késleltetést és dzsittert.

– *Híváskezdeményezés kontroll:* Az alkalmazás sávszélesség igényének elutasítását szabályozza. VoIP esetében a hívás számára szükséges sávszélesség lefoglalására használható például az RSVP (Resource Reservation Protocol). Egy H.323 gatekeeper korlátozhatja a hívásonként lefoglalható sávszélességet.

– *Várakozási sorok/ütemezés:* A pufferelés során használható, a csomagok prioritásának felderítésével. Külön sor tartható fenn a késleltetés-érzékeny hangcsomagok, és külön az adatcsomagok számára. VoIP esetében gyakori mechanizmus az IP RTP prioritási sor.

– *Tagging/megjelölés:* Különböző technikák használatosak a speciális kezelést igénylő csomagok megjelölésére. VoIP esetében a csomagok megjelölhetők például az IP precedencia bitekkel (IP fejrész ToS mezője). A csomagok megjelölés mechanizmusa a hálózat-határokon átnyúló QoS paraméterek megőrzéséhez szükséges.

– *Fragmentálás:* Bizonyos eszközökön engedélyezhető a nagyméretű csomagok további darabolása, mielőtt a kis sávszélességű linken azt továbbítaná. Ez megvédi a hangcsomagokat a nagyméretű adatcsomagok továbbításához szükséges hosszú várakozástól. Így a hangcsomag bekerülhet egy nagyméretű adatcsomag darabjai közé.

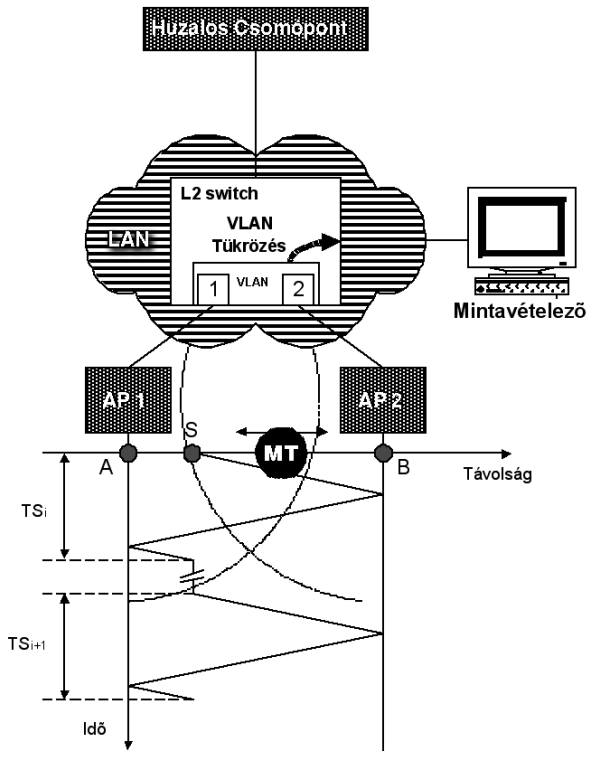
3. A mérési környezet és a mért adatok

A mérésekhez olyan eszközparkot használtunk, amelynél úgy a bázisállomások (AP_1, AP_2), mint a mobil terminál (MT) képes IEEE 802.11a, valamint IEEE 802.11b/g szabványoknak megfelelő mechanizmussal forgalmazni. Ehhez az *5. ábra* szerinti beltéri teszt hálózaton gyalogos közlekedés közben a mobil terminál mozgása miatt bekövetkező L2 roaming hatását vizsgáltuk.

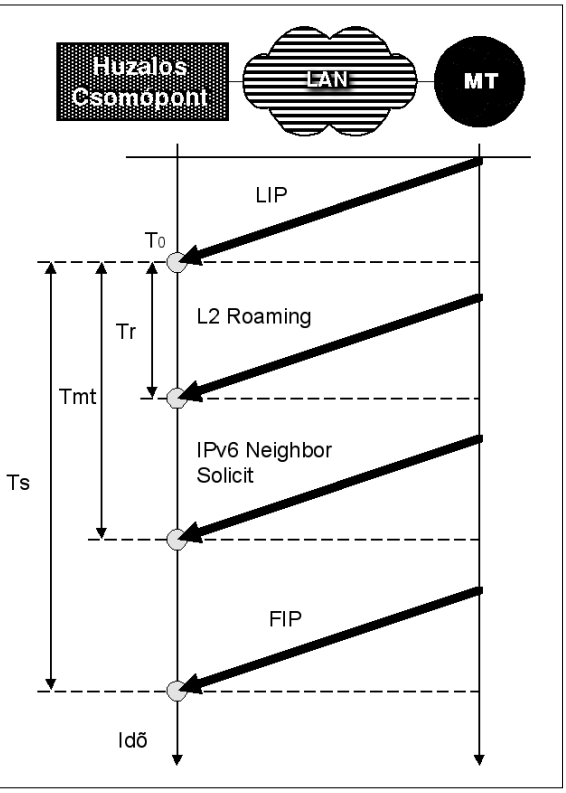
Az MT 5-6 km/h (1,4-1,7 m/sec) sebességgel haladt a bázisállomásokat összekötő egyenessel párhuzamos irányban oda-vissza. Egy mérési periódus (TSi) alatt az MT a AP_1 mikrocellájából L2 roaming hatására átkerült a AP_2 mikrocellájába, majd visszafelé haladva újabb L2 roaming hatására visszakerült a AP_1 hatáskörébe. Multimédiás szolgáltatásként video streaming, illetve IP telefon alkalmazásokat futtattunk a mobil terminálon. Az MT egy notebook, amelyen WinAmp, illetve SoftPhone szoftverek futottak a streaming (TCP), illetve telefonbeszélgetés (UDP) elemzéséhez.

TCP forgalom esetén a huzalos csomópont egy streaming szerver, amiről különböző sávszélességű, NullSoft Video (NSV) szabványú multimédiás műsoro-

5. ábra A mérési környezet



6. ábra A mért időtartamok



kat töltöttünk le. UDP forgalom méréséhez a huzalos és az MT csomóponton SoftPhone telefonszoftvert futtattunk, amelyek között telefonbeszélgetés zajlott. A LAN belsejében elhelyezkedő Phone Center-ben választottuk ki a hangkódolási mechanizmust.

A streaming (TCP) műsorok sávszélesség értékei a következők voltak: 80, 150, 300, 500 kbps. A hangkódolási (UDP) mechanizmusok pedig a következők: G.728 (16 kbps), GSM (29 kbps), G.711 (80 kbps), Wideband (272 kbps). Úgy a TCP, mint az UDP forgalmak esetén a bázisállomások Data Retry paraméterét fixen 32-re állítottuk, míg a Beacon periódust a 20 ms, 50 ms, 100 ms értékek között módosítottuk. A WinAmp program fogadó pufferét és a lejátszó puffere is fixen 1000 msecon állt. Ezek alapján IEEE 802.11 szabványonként TCP-re tizenkét mérést és UDP-re is ugyanennyi mérést végeztünk, így összesen hetvenkét mérési eljárást folytattuk le.

A két bázisállomás (AP_1, AP_2) egy L2 kapcsoló két portján, ugyanabban az L2 VLAN-ban helyezkedett el. A huzalos hálózaton megjelenő Ethernet kereteket a kapcsoló VLAN-jából egy dedikált fizikai portra történő tükrözéssel juttattuk el a mintavételező géphez, amely TCPDump program segítségével Libcap formátumú fájlba tárolta azokat. Utólag Ethereal v0.10.14 protokoll analizátor program segítségével elemeztük a tárolt folyamatokat és ezáltal lehetséges volt beazonosítani az alkalmazások minőségét befolyásoló időtartamokat. A bázisállomások által sugárzott rádiós energia IEEE 802.11b/g esetén 5 mW, az IEEE 802.11a esetén, pedig 11 dB volt. A két bázisállomás közötti fizikai távolság 50 méter, az MT rádiós forgalma nyitott azonosítás és titkosítás nélküli volt. Minden egyes TSi mérési eljárásnál (i=1,2,...72) az MT az S pontból indult és a B, majd S, A pontokon újból az S pontba érkezett vissza.

A multimédiás alkalmazások minőségét befolyásoló időtartamok meghatározásához Ethereal protokoll analizátorral minden egyes letárolt fájlban beazonosítottuk a *6. ábra* szerinti T0 időpontot. Ez nem más, mint az L2 roaming előtti LIP csomag (Last Important Packet) huzalos csomóponthoz történő beérkezésének időpillanata. Ez tulajdonképpen az MT cellaváltás előtti legutolsó tartalom adateleme. TCP, illetve UDP forgalmak esetén a LIP és a FIP csomagok jelentését a *2. táblázat* tartalmazza.

Tr időtartam alatt az L2 roaming folyamat játszódik le, aminek részletezését más cikkben mutattuk be [1].

A Tr időtartam beazonosítása a roaming keretek új bázisállomáshoz megérkezésének érzékelésével történt. Az MT gépen IPv6 kliens program is fut, amely az IPv4-hez képest rögtön érzékeli a protokoll stack kettes rétegének helyreállását, és azonnal megkezdi a szomszédos csomópontok felfedezését.

A Tmt időtartam az MT LLC (Logical Link Control) szintű forgalmazás képességének késleltetését jelenti. Az IPv6 kliens e tulajdonságát ahhoz használtuk fel, hogy a határozott roaming során küldött kereteket pontosan beazonosíthassuk, mivel az MT S→B→S→A→S beltéri pontok mentén történő haladása közben az épület falain bekövetkező reflexiók miatt esetenként kettőnél több cellaváltást is tapasztaltunk.

A Ts időtartam az MT-n futó multimédia kapcsolat működésének késleltetése. Ezt a felhasználó közvetlenül érzékeli és ennek nagy értéke a szolgáltatás akadozásához, illetve a kapcsolat teljes megszakadásához vezethet. Ennek meghatározása a FIP csomag (First Important Packet) beérkezésének beazonosításával történt.

4. A mérési eredmények elemzése és értelmezése

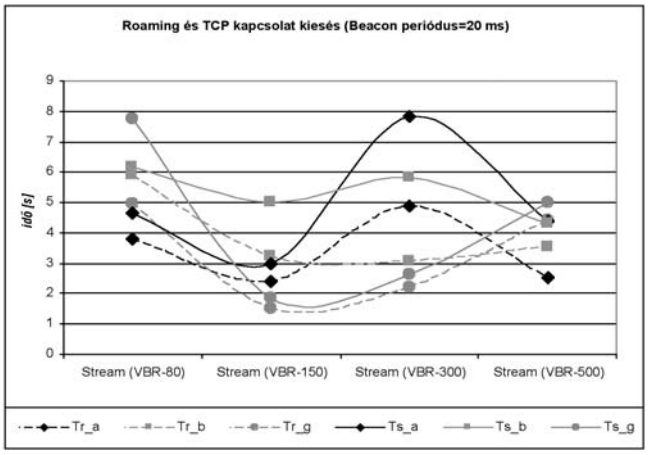
A mérési eredmények összehasonlítása és elemzése fontos következtetések levonására ad lehetőséget. A különböző IEEE 802.11 szabványok eltérő módon viselkednek beltéri környezetben végrehajtott cellaváltások esetén [7]. A roaming folyamat lejátszódása nagymértékben függ a bázisállomáson beállított beacon periódus (T_b) időtől. Ez a periódus egyben konfigurációs paraméter is [8]. A terminál a bacon-ben továbbított jelzés alapján megtanulja a bázisállomás periódusát [9]. Amennyiben az MT nyolc periódus ideig nem kap bacon-t, kezdetét veszi a roaming folyamat [1]. A beérkező beacon keretek folyamatos figyelésével az MT érzékeli a vezeték nélküli kapcsolat minőségének romlását és cellaváltást kezdeményez.

A TCP forgalom mért értékeinek grafikonjait a következő oldali *7., 8., 9. ábra,* az UDP forgalomra vonatkozó grafikonokat pedig a *10., 11., 12. ábrák* mutatják.

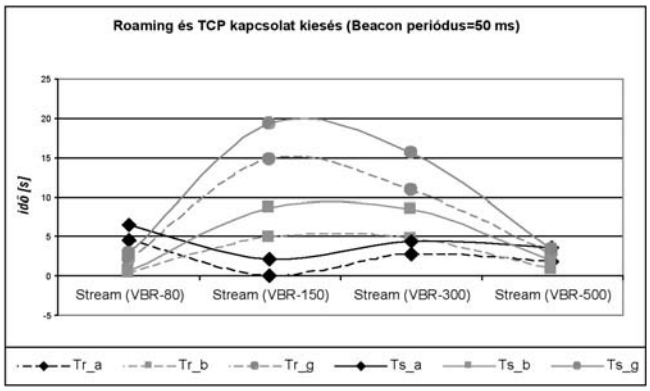
• Ha beacon periódust az alapértelmezett 100 ms értékről 50 ms, majd 20 ms-ra csökkentjük, akkor az MT gyakrabban érzékeli a jel/zaj viszony változását, így mozgás közben érzékenyebb lesz a környezeti viszonyok változására. Ilyenkor minden egyes streaming technológia esetén a cellaváltási idő 0,5-2,8 sec értékről előbb 0,1-14,9 sec értékre nő, majd 1,5-5,9 sec értékre csökken, a TCP kapcsolat kiesése pedig 2,5-17 sec értékről előbb 2,4-19,8 sec értékre nő, majd 1,8-7,9 sec értékre csökken. Tehát a T_b=20 msec periódusidő jobb, mint a 100 msec érték. Ez hasznos konfigurálási

2. táblázat Fontos csomagok jelentése

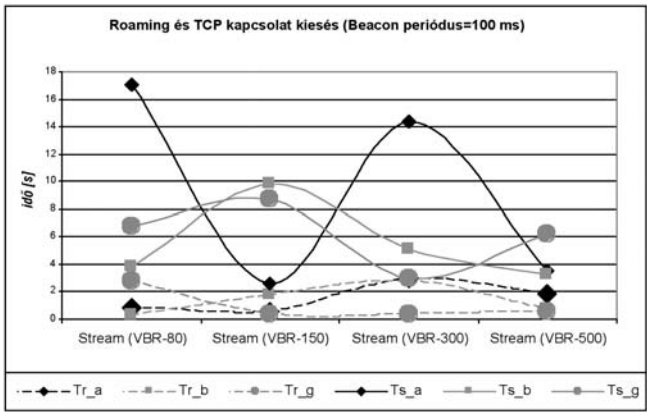
Szállítási réteg	*Fontos csomag*	*Jelentés*
TCP	LIP	L2 roaming előtti utolsó ACK csomag (60 bájt) az MT-től a szerverhez
TCP	FIP	L2 roaming utáni első ACK csomag (60 bájt) az MT-től a szerverhez
UDP	LIP	L2 roaming előtti utolsó UDP csomag az MT-től a huzalos csomóponthoz
UDP	FIP	L2 roaming utáni első UDP csomag az MT-től a huzalos csomóponthoz



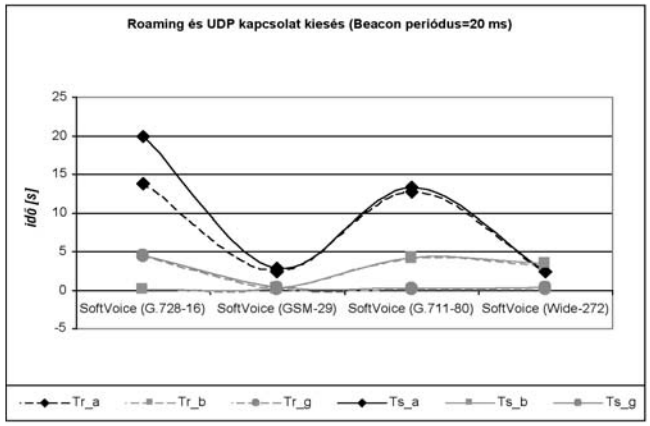
7. ábra A streaming viselkedése (Tb=20 msec)



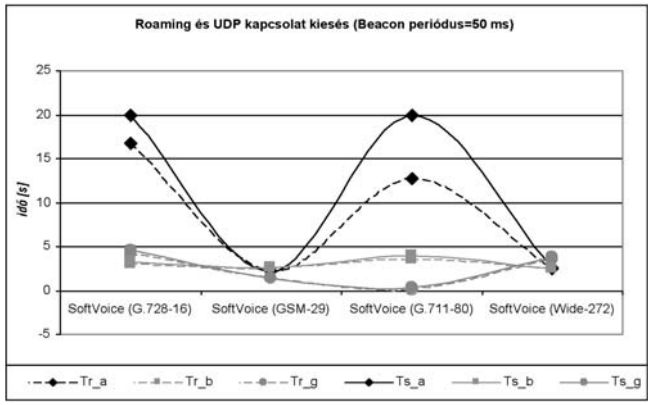
8. ábra A streaming viselkedése (Tb=50 msec)



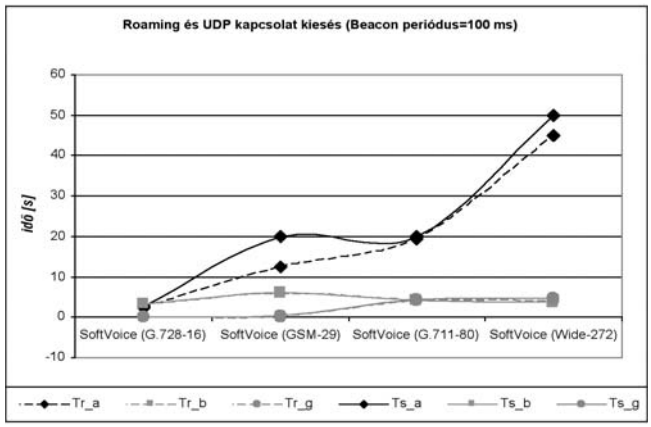
9. ábra A streaming viselkedése (Tb=100 msec)



10. ábra Az IP telefon viselkedése (Tb=20 msec)



11. ábra Az IP telefon viselkedése (Tb=50 msec)



12. ábra Az IP telefon viselkedése (Tb=100 msec)

jelenségnek számít. A T_b nagyon kis értékre vétele sem lehet jó a gyakorlatban, mivel beltéri környezetben a többutas terjedés miatt a túlzott érzékenység cellaváltásokat okoz, ami a TCP kapcsolat gyakori kiesését jelenti.

• IP telefon kapcsolat esetén adott hangkódolási technikánál a cellaváltási időre a beacon periódus csökkentése 100 msec értékről 50 msec, majd 20 msec-re a cellaváltási időt a 0,1-44,5 sec értékről 0,1-12,5 sec értékekre csökkenti. Az UDP kapcsolat kiesés a 0,2-49,8 sec értékről a 0,2-19,9 sec értékekre csökken. Ez is a T_b=20 msec érték előnyét jelzi.

• Épületen belül az IEEE 802.11 technológiák különbözőképpen reagálnak a beacon periódusra. Streaming forgalom esetén az IEEE 802.11a hosszabb ideig állítja vissza a kapcsolatot. Utána az IEEE 802.11b következik, és legelőnyösebb tulajdonságokkal az IEEE 802.11g rendelkezik beltéri cellaváltás esetén.

• IP telefon szolgáltatásnál az IEEE 802.11a nagyon nagy késleltetéseket produkál, nagy sávszélességű hangkapcsolat esetén le is szakad a szolgáltatás. Az IEEE 802.11g a legjobb reakcióidőt biztosítja, így a szolgáltatás kiesése 4 sec alatti. Ez még elviselhető ritka esemény lehet mozgó IP telefonos környezetben, ha a felhasználók erről előzetes értesüléssel rendelkeznek.

• A streaming sávszélesség igényétől függően a műsor kiesési idő is eltérő viselkedést mutat. A 150 kbps-os NSV műsor T_b=20 msec esetén a legkevésbé függ a rádiós technológiától, viszont T_b=50 msec esetén éppen a 150 kbps-os NSV műsor függ leginkább a rádi-

ós technológiától. $T_b \leq 50$ msec esetén a 80 kbps-os és az 500 kbps-os NSV műsorok kevésbé függnek a rádiós technológiától.

• Az IP telefon kapcsolat $T_b \leq 50$ msec esetén a GSM hangkódolásnál mutatja a legkisebb kiesést. Ez a GSM technológia mobil viszonyokra optimalizált tulajdonságából adódik. Annak ellenére, hogy a GSM minőségben gyengébb, mint a G.728, mégis jobban illeszkedik a cellaváltás okozta környezetváltozáshoz. $T_b \leq 50$ msec esetén a G.711 nagyon függ a rádiós technológia cellaváltási mechanizmusától. Ez a PCM hagyományos huzalos környezetre kialakított tulajdonságából adódik.

• Cellaváltás befejezése után a streaming kapcsolat folytatása nagy beacon periódusidő esetén későn, 4-11 sec késleltetéssel történik. Ezzel ellentétben $T_b \leq 50$ msec esetén az új cellába váltás után a TCP kapcsolat 3 sec késleltetés után folytatódik. Ez az adott technológia Ts-Tr időkülönbség értékekből figyelhető meg.

• IP telefon esetén a cellaváltás utáni UDP forgalom folytatásának késleltetése IEEE 802.11b/g rádiós technológiák esetén minden hangkódolási technika esetén 0,5 sec alatt van. Az IEEE 802.11a viszont az MT új cellába érkezése után még az UDP forgalom folytatását is jelentősen (3-7 sec) késlelteti.

• Az IEEE 802.11a rádiós technológia a streaming számára T_b=50 msec értékre mutatja az összességében legelőnyösebb tulajdonságait. Az IEEE 802.11g pedig a T_b=20 msec értékre képes legelőnyösebb adatkapcsolati szolgáltatást nyújtani a streaming részére.

• Az IP telefon számára hangkódolási technikától függetlenül bármilyen beacon periódusra az IEEE 802.11g rádiós technológia a legjobb, ezt követi az IEEE 802.11b, majd a legkedvezőtlenebb viselkedést az IEEE 802.11a mutatja.

• Az IP telefon esetén a cellaváltásból származó adatkapcsolati szintű kimaradás miatt a hangkódolási technikák rugalmassági sorrendje csökkenő sorrendben a következő: GSM, Wideband, G.711, G,728.

5. Összefoglalás

Az cikkben elemeztük az IEEE 802.11a, 802.11b és 802.11g WiFi átviteli technikákon működő multimédiás (streaming, IP telefon) alkalmazások jellemzőit beltéri cellaváltás közben. A TCP típusú mérésekhez Nullsoft Video formátumú, különböző sávszélességű streaming jelfolyamokat indítottunk egy beltéri környezetben gyalog mozgó notebook irányába. Az UDP típusú mérésekhez IP Softphone futott az előzetesen említett notebook gépen, miközben egy másik, huzalos IP telefonnal beszélgetést folytatott. A leggyakoribb hangkódolási mechanizmusokra készültek a mérések.

Ezek alapján megállapítható, hogy a bázisállomás beacon periódus ideje erőteljesen befolyásolja a cellaváltás folyamatát. A különböző IEEE 802.11 rádiós technológiák eltérő módon viselkednek TCP, illetve UDP forgalom esetén. Ugyancsak különböző hatást gyakorol ezekre is a beacon periódus értéke. Mozgó beltéri vezeték nélküli streaming terminál számára 150 kbps esetén az IEEE 802.11g szabvány 20 msec értékű beacon periódus idővel a legelőnyösebb. Mozgó vezeték nélküli IP telefon számára gyengén terhelt IEEE 802.11g beltéri rádiós környezetben jó minőségű szolgáltatás vehető igénybe. A cellaváltás legjobb esetben 2-3 sec szolgáltatás kimaradást okozhat, amit a felhasználók előzetes értesítése esetén elfogadhatónak tarthatnak.

A GSM hangkódolási mechanizmus a legrugalmasabban viszonyul a cellaváltás hatására bekövetkező adatkapcsolati szintű szolgáltatás kimaradására, amit a wideband kódolás követ, annak ellenére, hogy sávszélesség igénye egy nagyságrenddel nagyobb, mint a G.711, G.728 esetén.

A későbbiekben gyors konvergenciájú cellaváltású, illetve 250 msec alatti szolgáltatás kiesést biztosító szállítási rétegbeli mechanizmusok kialakítására van szükség ahhoz, hogy mobil vezeték nélküli beltéri környezetben a multimédiás szolgáltatások folyamatosan elfogadható minőségben működőképesek legyenek. Ugyancsak értékelést kell végezni a H.323/SIP típusú mobil IP videokonferencia szolgáltatásra vonatkozóan is.

Irodalom

[1] Zoltán Gál, Andrea Karsai, Peter Orosz:
„Evaluation of IPv6 Services in
Mobile WiFi Environment”,
Selected Papers of Info-Communication-Technology,
Volume LX., 2005, pp.47–54.

[2] Dodd, Annabel Z.:
The Essential Guide to Telecommunications

[3] Newton, Harry:
Newton’s Telecom Dictionary,
http://www.harrynewton.com/

[4] Justin Frankel:
„Nullsoft Video (NSV) Format 2.1 Specification”,
http://ultravox.aol.com/NSVFormat.rtf

[5] Jonathan Davidson:
„Voice over IP Fundamentals”,
http://www.ciscopress.com/

[6] Cisco Documentation DVD Home Page:
„Voice/Data Integration Technologies”,
http://www.cisco.com/univercd/cc/td/doc/
cisintwk/ito_doc/voicdata.htm

[7] WiFi Alliance:
„Wi-Fi Certified for WMM- Support for Multimedia
Applications with Quality of Service in Wi-Fi Networks”,
http://www.wi-fi.org/files/uploaded_files/
wp_1_WMM%20QoS%20In%20Wi-Fi_9-1-04.pdf

[8] SpectraLink Co.:
„White paper: Deploying netlink wireless telephones,
best practices”,
http://www.spectralink.com/files/literature/
NetLink_Best_Practices_122105_01.pdf

[9] 3Com Co.:
„White paper: Deploying 802.11 Wireless LANs”,
http://www.3com.com/other/pdfs/products/
en_US/wireless_lans_wp.pdf

Ügyfélazonosítás és -hitelesítés az európai e-közigazgatásban

SIKOLYA ZSOLT

Informatikai és Hírközlési Minisztérium
zsolt.sikolya@ihm.gov.hu

Kulcsszavak: e-közigazgatás, azonosságkezelés, személyhitelesítés, interoperabilitás

Az ügyfelek azonosítása és hitelesítése kiemelt kérdés az e-közigazgatási eljárások során. Az európai országokban – köztük Magyarországon – alkalmazott megoldások és modellek nagyon eltérőek, és nem vagy csak korlátozottan tudnak együttműködni egymással. Ez még az egyes országokon belül gyakran így van. A cikk vázolja és röviden értékeli a leggyakoribb megoldásokat. Bemutatja az Európai Bizottság legutóbbi döntését arra nézve, hogy 2010-re a tagországok minden szinten biztosítsák az e-közigazgatási azonosságkezelés együttműködési képességét.

1. Bevezetés

Az információs társadalom megvalósításának világszerte az egyik kulcsterülete az elektronikus közigazgatás. Már a múl század utolsó éveiben felismerték, hogy az infokommunikációs eszközök alkalmazása a közigazgatásban soha nem látott lehetőségeket teremt a szolgáltató típusú, ügyfélbarát, (költség)hatékony, innovatív, nyitott, átlátható közigazgatás létrehozásához.

Az Európai Unió eEurope 2002, majd eEurope 2005 cselekvési tervében kiemelt helyet kapott az e-közigazgatás, de hasonló szerepe lesz az i2010 programban is. A közigazgatási eljárásoknak, szolgáltatásoknak meghatározó szerepük van az alapvető jogbiztonság megteremtésében, és ez a jogbiztonság, valamint a személyes adatok védelme, a visszaélések elkerülése az esetek jelentős részében csak úgy garantálható, ha a szolgáltató valamilyen mértékben és hitelességgel azonosítja az ügyfelét. Ez igaz mind az ügyek hagyományos, tehát személyesen vagy papíron történő, mind pedig az elektronikus úton történő intézésére is.

Az alábbiakban áttekintést adunk arról a sokszínűségről, amely az Európai Unió országainak megoldásait, hitelesítési modelljeit jellemzi. Ebben a sokszínűségben sajátos helyet foglal el a „magyar út". Végül kitérünk arra, hogy – felismerve a határokon átívelő szolgáltatások szükségességét – milyen összeurópai tervek vannak az együttműködésre.

2. Fogalmi alapok

A következők során szerepel az azonosítás (identification) és a hitelesítés (authentication) fogalma, és mivel a különböző források nem egységesen értelmezik ezeket, elöljáróban megadjuk a két fogalomnak a továbbiakban használt értelmezését, melyet [1]-ből vettünk át:

Azonosítás:
Arra vonatkozó információ megszerzésének folyamata, hogy kinek állítja magát a kérelmező.

Hitelesítés (személyé):
Egy személy állított azonosságáról való bizonyosság megszerzése.

Nagyon fontos, hogy a személy hitelességének (entity authentication) fogalmát megkülönböztessük az adat (vagy dokumentum) hitelességének (data authentication) fogalmától, amely utóbbit az adat sértetlenségének és eredetének bizonyosságaként értelmezzük [2].

3. Ügyfélazonosítás az Európai Unió országaiban

Mielőtt az elektronikus azonosítás/hitelesítés európai gyakorlatát áttekintenénk, érdemes néhány szót szólni a hagyományos ügyintézésről. A hagyományos út esetében évtizedek sőt bizonyos értelemben évszázadok során alakult ki a jól bevált gyakorlat. Ennek során két fő típussal találkozunk. Az egyik esetben elegendő, ha az ügyfél a kérelemben azonosítja magát az erre alkalmas adatainak megadásával, és a kérelmet aláírja. Ilyenkor a hatóság „elhiszi" az állított azonosságot.

Az aláírás csak a dokumentum hitelesítésére szolgál, hiszen a hatóságnak általában nincs aláírásmintája, ezért ellenőrizni sem tudná az aláírás valódiságát; az aláírás csak egy esetleges későbbi jogvita során bizonyíthatja a kérelem eredetét és sértetlenségét. A másik esetben személyes megjelenésre van szükség – legkésőbb az eljárás végső, érdemi fázisában –, és a kérelmezőnek személyazonosítására alkalmas hatósági igazolvánnyal kell igazolnia személyazonosságát.

A tagországokban nincs egységes gyakorlat arra nézve, hogy milyen adatokat használ a közigazgatás az ügyfelek azonosítására – akár hagyományos, akár elektronikus ügyintézés során. Ez a megállapítás sok esetben az országokon belül is igaz. Míg a természetes személyazonosító adatok használatát illetően sok hasonlóság van (név, születési adatok), abban már éles a különbség, hogy használ(hat)nak-e egységes személyazonosító kódot vagy sem.

Vannak országok (pl. Észtország, Belgium), ahol az egységes kód használata megengedett és általános – esetleg nem is csak a közigazgatásra kiterjedően –, vannak országok (pl. Németország, Magyarország), ahol néhány jól meghatározott csoportra vannak felosztva az ügyek, és az egyes csoportok más-más személyazonosító kódot használhatnak, és végül vannak olyan országok (pl. Egyesült Királyság), ahol gyakorlatilag minden hivatal más azonosító kódot használ. Az is jelentős mértékben kihat az azonosításra – de főleg a hitelesítésre –, hogy van-e az országnak központi népesség-nyilvántartása (az Egyesült Királyságnak például nincs). A személyazonosító kódok és a központi nyilvántartás kérdése elsősorban az egyes országok adatvédelemről való felfogásán múlik, amely annak ellenére jelentős különbségeket mutat, hogy az EU-nak van adatvédelmi irányelve, és azt természetesen minden tagország beépítette saját jogrendjébe.

Az Európai Unió elsődleges jogát képező, az európai közösség létrehozásáról szóló szerződés [3] 3. cikkében felsorolt közösségi tevékenységek azonban nem terjednek ki a közigazgatásra, a 18. cikk szerint pedig az útiokmányokra, személyazonosító igazolványokra, a tartózkodási engedélyekre vagy bármely egyéb ilyen okmányra vonatkozó rendelkezések nem tartoznak közösségi hatáskörbe.

4. Hitelesítési módszerek

Az elektronikus dokumentumok hitelesítésének jól kialakult jogi és szabványosítási háttere van az Európai Unióban – gondolunk itt elsősorban az EU elektronikus aláírásra vonatkozó irányelvére [4] és a meglévő számos nemzetközi (ETSI, IETF stb.) szabványra. (Ennek ellenére még hiányoznak a teljes mértékben átjárható megoldások.) Ugyanakkor a személyhitelesítésnek nincs nemzetközi jogi háttere, a gyakorlata országonként – és sokszor az egyes országokon belül is – eltérő, nincsenek rá általánosan elfogadott szabványok.

A legfejlettebb országokban, ahol korán elkezdődött el az e-közigazgatás terjedése, különösen jellemző volt az a természetes fejlődés, hogy az egyes hivatalok saját megfontolásaik alapján, különösebb összehangolás nélkül alakították ki elektronikus ügyintézési rendszereiket, és azok ügyfél-hitelesítési megoldásait. Az újonnan csatlakozott országok (pl. Észtország, Magyarország), ahol egyébként is jelentős hagyományai voltak a centralizációnak, már sokkal inkább törekedtek arra, hogy – legalább országukon belül – egységes megoldást alakítsanak ki az e-közigazgatásban, de természetesen az utóbbi években az élenjáró országok is sorra alakítják ki a sok egyedi megoldás helyett vagy mellett egységes, illetve együttműködésre (interoperabilitásra) képes ügyfél-hitelesítési koncepciójukat, megoldásukat.

Uniós szinten – amint azt később látni fogjuk – csak a legutóbbi időkben fogalmazódott meg határozott szándék arra nézve, hogy meg kell teremteni a tagországok személyhitelesítési interoperabilitását, legalább is a közigazgatást illetően.

Az e-közigazgatás elterjedésének kezdetén szinte kizárólag a felhasználói név és jelszó szolgált személyhitelesítésre, és ma is ez a legelterjedtebben használt módszer – még a legfejlettebb tagországokban is. Egyetlen titkos információ, a jelszó feltételezetten kizárólagos ismeretén alapul, ezért egyfázisú (single-factor) hitelesítésnek nevezik. A megoldás javára egyszerűsége, ingyenessége szól, nincs szükség például kártyaolvasó vásárlására, telepítésére sem.

Közismert ugyanakkor, hogy a megoldás mennyire sérülékeny, akár kémprogramokkal, akár megtévesztéssel milyen könnyen megszerezhetők a jelszavak, és ezáltal ellophatóvá válik a személyazonosság. Ezért egyre több helyen (pl. Belgiumban) teszik biztonságosabbá a módszert egyszer használatos jelszó alkalmazásával, amihez általában valamilyen segédeszközt (jelszólista, RSA SecurID, más csatorna: például sms stb.) használnak.

Egyre inkább – bár a kívánatosnál lényegesen lassabban – terjed a nyilvános kulcsú infrastruktúra (PKI) használata. Ez egy magán és nyilvános kulcspár, az azokkal végrehajtott kriptográfiai eljárás, illetve egy megbízható harmadik fél által kiállított tanúsítvány alkalmazásán alapul. A módszer azonos az elektronikus aláírásnál alkalmazottal, de itt általában nem egy, az aláíró által ismert dokumentumot kódolnak a magánkulccsal hitelesítés céljából, hanem egy véletlenszerű, nem „visszajátszható” adatot (kérdés-válasz – challenge-response – módszer). A tanúsítvány legegyszerűbb esetben tartalmazza a személyazonosításra alkalmas adatokat (kódot) – olyan országokban, ahol ez megengedett (pl. Belgium, Észtország, Szlovénia), az egységes személyazonosító kódot.

A bevezetőben már említettük, hogy a személyhitelesítést meg kell különböztetnünk az dokumentumhitelesítéstől (aláírástól). Más a céljuk, a felhasználásuk, és teljesen más joghatások fűződnek hozzájuk [5]. Az aláírás egy jól kezelhető jogi fogalom, amellyel az aláíró vállal – letagadhatatlan módon – felelősséget az aláírt dokumentumban foglaltakért. Személyhitelesítés viszont egy folyamat, amelyre olyan esetekben kerül sor, amikor a hatóságnak kell felelősséget vállalnia azért, hogy ne jusson valaki illetéktelenül például hatósági igazolvány vagy érzékeny adat birtokába. Ha valaki átjut a személyhitelesítésen, joggal hajthat végre olyan cselekményeket, amelyekre ezzel jogosultságot szerzett. Ha mindkét célra PKI-tanúsítványt használnak, a két tanúsítvány az esetek túlnyomó többségében különböző.

Külön kell szólnunk Ausztria egészen sajátos, és igen jól kidolgozott megoldásáról. Az osztrák e-közigazgatási törvény által előírt „Bürgerkarte” koncepcióban nincs külön hitelesítő (autentikációs) tanúsítvány. Ausztriában csak szektorspecifikus ágazati azonosítók használata megengedett; a személy ágazati azonosítóinak származtatására használt egységes forrásazonosítót az e-aláírás nyilvános kulcsához kapcsolja egy,

a forrásazonosítót kibocsátó hatóság aláírásával ellátott adatrekord, és a „beléptetéskor” szükséges ügyfélhitelesítéshez egy „nem visszajátszható” kérelmet iratnak alá az ügyféllel. A személyazonosság megállapításához a hatóság számára szükséges ágazati azonosító kódot az aláíró nyilvános kulcshoz hitelesen hozzákapcsolt forrásazonosítóból számítják ki egy egyirányú algoritmussal.

A titkos magánkulcsot sok esetben (pl. Dánia, Svédország) a számítógép memóriájában tárolják, ami megint csak sérülékeny megoldás, viszont nem igényel speciális eszközt. Sokkal inkább alkalmas a személyazonosság kompromittálódásának megelőzésére az a módszer, amikor biztonságos csipkártyán generálódik a titkos kulcs, és azt soha nem hagyja el. A csipkártyához való hozzáférést PIN-kóddal védik: így alakul ki a kétfázisú (two-factor) hitelesítés, amelynek használatához egyrészt rendelkezni kell a biztonságos eszközzel, másrészt ismerni kell a PIN-kódot.

Csipkártyát részben egy-egy ágazat (egészségügy, oktatás stb.) szolgáltatásainak igénybevételére bocsátanak ki az országok (pl. Franciaország, Németország), részben pedig univerzális céllal. Ez utóbbiaknak van olyan típusa (Ausztria, Észtország, Belgium, Finnország, Olaszország, legújabban Spanyolország), amely mind fizikai személyazonosító dokumentumként, mind e-közigazgatási szolgáltatások igénybevételére használható, de van olyan is, amely csak ez utóbbira (pl. Egyesült Királyság, Olaszország). Meg kell jegyeznünk, hogy létezik olyan csipkártyás hitelesítés is, amely nem PKI technológiát használ.

A hitelesítésnek van egy olyan fajtája, amely az ügyfél valamilyen tulajdonságának közvetlen érzékelésén, mérésén alapul (biometrikus hitelesítés), de ennek a közigazgatási szolgáltatások elektronikus igénybevételére történő alkalmazása még csak egyes országok (Spanyolország, Szlovénia stb.) tervei között szerepel. Egyelőre csak a csipkártya elérésére használt PIN-kód helyett tervezik használni.

5. Hitelesítési modellek

Az ügyfél-hitelesítés valamilyen elektronikus „igazolvány” bemutatásán alapul. Ilyen igazolvány lehet például a jelszó, a PKI-tanúsítvány, a biometrikus adat. Hitelesítési modellnek azon szervezeti és eljárási hátteret nevezzük, amely az ügyfél regisztrációjához, az igazolvány kibocsátásához, az igazolványnak az ügyfélhez való kapcsolásához, az igazolvány visszavonásához stb. tartozik. A modellnek az ügyfélen és a közigazgatási szolgáltatás nyújtóján kívül még legalább a hitelesítő szervezet a szereplője.

Alapvetően három fő típusra oszthatjuk az EU-ban jelenleg használt modelleket, Az egyik modellnél a szolgáltató és a hitelesítő szervezet ugyanaz. Ilyen majdnem minden országban található; ez jellemző a szigetszerű rendszerekre. A másik megoldásnál egy központi hitelesítő szervezet hitelesíti az ügyfeleket több – esetleg minden – szolgáltató szervezet számára. Ezt használják többek között a sokféle szolgáltatás igénybevételére alkalmas – például személyi azonosító – csipkártyák és a magyar ügyfélkapu esetén.

Végül kezdenek elterjedni az osztott, illetve szövetséges (federated) modellek. Ezek lényege az, hogy az ügyfelek megválaszthatják, hogy mely hitelesítő szervezetet bízzák meg elektronikus azonosságuk igazolásával (hitelesítésével), az alkalmazás-szolgáltatók pedig megállapodásokat kötnek a hitelesítőkkel, hogy elfogadják hitelesítésüket, és így végül úgynevezett bizalmi körök alakulnak ki, amelyeken belül „szövetséges” (egyezményes) alapon működik a személyhitelesítés.

Adatvédelmi szempontból fontos, hogy ennél a modellnél az ügyfél akár esetenként is dönthet arról, hogy mely hitelesítő szervezetet választja, és hogy az milyen hitelesítési információt adhat át az alkalmazásszolgáltatónak. A skandináv országokban pl. a bankok hitelesítését is elfogadják a közigazgatásban, Magyarországon pedig bármelyik, adott feltételeknek eleget tevő hitelesítés-szolgáltatóét.

Míg a szigetszerű modellnél nincs szükség interoperabilitásra, a központi megoldásoknál pedig az egységesség a modell jellegénél fogva biztosított, addig a szövetséges modellek különösen igénylik a szabványosítást. Jelenleg három nemzetközi szabványosítási kezdeményezés van erősen elterjedőben [6]: a Liberty Alliance, a Microsoft/IBM és az OASIS rendszere. A francia kormányzat a Liberty Alliance szabványait alkalmazó kísérleti projektet futtat, és 2007-től be kívánja vezetni a szövetséges hitelesítés használatát a kormányzati portálon.

6. A magyar megoldás

A közigazgatási hatósági e-ügyintézés szabályait a 2005. november 1-jén hatályba lépett, a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény (Ket.) és annak végrehajtási rendeletei állapítják meg [7-9].

Az elektronikus hatósági ügyintézés során a kérelem benyújtásának elsődleges módja a fokozott biztonságú aláírással ellátott kérelemnek a központi rendszeren keresztül vagy közvetlenül a hatósághoz történő eljuttatása. Ha szükség van az ügyfél hitelesítésére, úgy azt az elektronikus aláíráshoz kapcsolódó, a hitelesítés-szolgáltató számára kötelezően előírt viszontazonosítás útján kell elvégezni.

A viszontazonosítás során lényegében az ügyfélnek a hatóság és a hitelesítés-szolgáltató nyilvántartásában szereplő természetes azonosítóit hasonlítja össze a hitelesítés-szolgáltató. A jogszabályok az ügyfél hitelesítés-szolgáltatónál szükséges regisztrációjával szemben a minősített e-aláírással egyenértékű követelményeket támasztanak. A regisztrációnak személyesen kell történnie az ügyfél személyazonosságának személyazonosításra alkalmas (arcképes) okmány alap-

ján a megfelelő közhiteles nyilvántartásban történő ellenőrzésével. Ezzel tehát a jogosulatlan azonosságszerzés szempontjából legdöntőbb mozzanattal, a regisztrációval szemben a legmagasabb biztonsági elvek érvényesülnek.

Az elektronikus aláírásnak személyhitelesítésre történő felhasználása szokatlan, de nem egyedülálló a nemzetközi gyakorlatban (lásd Ausztria), a viszontazonosításra viszont egyáltalán nincs példa más országokban. A nemzetközi együttműködésben külön problémát jelenthet, hogy a magyar megközelítés egy piaci szereplő, a hitelesítés-szolgáltató számára ír elő kötelező jelleggel az uniós e-aláírási irányelvtől idegen szolgáltatást (természetesen csak a közigazgatási célú tanúsítványokat kibocsátóktól).

A Ket. rendelkezései szerint az elektronikus aláírással nem rendelkező ügyfelek számára a központi rendszer biztosítja az elektronikus ügyintézés lehetőségét. Ilyenkor egy úgynevezett ügyfélkapun keresztül történik a belépés – lényegében egy felhasználói név és jelszó megadásával. Ezt megelőzően egy okmányirodában regisztrálnia kell az ügyfélnek, amely ugyanolyan szigorú személyazonosítással történik, mint az elektronikus aláírás esetén.

Az ügyfélkapun történő beléptetést követően a hatóság információs rendszere nem kapja meg az ügyfélről a központi rendszerben tárolt természetes személyazonosító adatokat, hanem egy, az elektronikus aláírásnál használttal analóg viszontazonosítási folyamattal ellenőrizheti le az ügyfél vélt személyazonosságának valódiságát.

A Ket. és végrehajtási rendeletei egyenértékűként kezelik a két ügyfél-hitelesítési módszert, és nem teszik lehetővé, hogy ágazati jogszabály mérlegelje, hogy melyik használatát engedélyezi. Egyedül abban van választási lehetőség, hogy a hatóság alkalmazzon-e hitelesítést (viszontazonosítást), vagy esetleg csak fogadja el azt, amit az ügyfél magáról állít. Bizonyos esetekben azonban kötelező a viszontazonosítás, pl. ha az ügyfél személyes adathoz, illetve adó-, bank-, biztosítási vagy értékpapírtitokhoz kíván hozzáférni.

A magyar e-ügyintézés szabályozásában meg kell említeni még egy különleges rendelkezést, bár az nem az ügyfél-hitelesítéshez, hanem a dokumentum-hitelesítéshez kapcsolódik. Eszerint a folyamatos párbeszédre épülő ügyintézés – beleértve az ügyfélkapun történő, jelszavas belépést is – alapesetben önmagában biztosítja a kapcsolat tartama alatt végzett egyes eljárási cselekményeknek az azonosított ügyfélhez rendelését. Az eljárási cselekményekbe bele kell érteni többek között valamely dokumentum beküldését is. Ez azt jelenti, hogy egy jelszavas belépéssel történő adóbevallás tartalmát érintő esetleges jogvita során az ügyfélnek kell bizonyítania azt, hogy az általa vélt bevallást küldte be, amely elektronikus aláírás nélkül meglehetősen reménytelen vállalkozás.

Tehát egy kicsit sarkosan fogalmazva a magyar jogrendszer a jelszavas ügyfél-hitelesítéshez (is) a letagadhatatlanság vélelmét rendeli, míg – amint azt korábban láttuk –, az elektronikus aláírást használja ügyfél-hitelesítésre (is), ami épp a fordítottja a nemzetközileg kialakult gyakorlatnak.

7. Páneurópai törekvések

Az Európai Bizottság eEurope E-közigazgatási Alcsoportja 2005-ben kidolgozta az i2010 e-közigazgatási stratégiáját [10], melyet 2005. novemberben a manchesteri miniszteri e-közigazgatási konferencián tettek közzé. Azóta ennek cselekvési terve is elkészült [11]. A tervnek öt fő iránya van, amelyből az egyik az e-azonosítással és -hitelesítéssel, valamint az elektronikus dokumentumok hitelességével foglalkozik. A stratégia a legfontosabb tennivalók között megjelölte, hogy

- 2010-re legyen olyan megbízható e-azonosítás minden európai ügyfélre az adatvédelem figyelembevételével, melyet minden tagország saját felelősségében old meg, és elismer,
- ennek megalapozására készüljön el egy világos terminológia,
- legyen megoldva a meghatalmazás, közvetítés, szerepkezelés.

Az első feladat végrehajtása során messzemenően figyelembe kell azt venni, hogy számos ország már jelentősen előrehaladt saját e-közigazgatási ügyfél-hitelesítési rendszerének megvalósítása terén. Ezek a megoldások jelenleg nem vagy csak korlátozottan átjárhatóak, és mivel már hatalmas összegeket ruháztak be megvalósításukra, nem lehet szó arról, hogy a meglévő megoldásokat lecseréljék valamilyen páneurópai egységes megoldásra.

A jogszabályi szintű egységesítés akadályáról már szóltunk. Mindezek miatt a tervek szerint az egyes tagországok saját kompetenciájukban valósítják meg e-közigazgatási személyhitelesítési rendszerüket, de el kell ismerniük egymás hitelesítését. Az átjárhatóságot a szövetséges modell alkalmazásával, és a hozzá tartozó szabványosítással, illetve szabványok átvételével kell biztosítani. Fontos szempont, hogy többszintű legyen a modell, azaz tegye lehetővé a különböző biztonsági és hitelesítési igényekhez igazodóan a hitelesítés különböző szintjeinek használatát. Azt majd csak a későbbi vizsgálatok döntik el, hogy ehhez szükség van-e egy nemzetek fölötti uniós infrastruktúra felállítására, vagy az országok közötti kölcsönös elismerés lesz a járhatóbb út. Ugyancsak fontos biztosítani az uniós adatvédelmi irányelv maradéktalan érvényesülését.

Az egyes országok igényein túl ki kell elégíteni a páneurópai közszolgáltatások hitelesítési igényeit is. Ezzel a kérdéssel elsősorban az Unió IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens) programja foglalkozik, amely korábban már elkészítette e-hitelesítési irányelveit, 2007. közepére egy e-azonosítási interoperabilitási stratégiát, 2007. végére pedig egy közös specifikációt kíván elkészíteni.

Az európai törekvések között fontos megemlíteni az Európai Szabványügyi Szervezet, a CEN keretében folyó munkákat. 2005-ben elkészült egy anyag egy – nemcsak közigazgatási célokat szolgáló – interoperábilis e-azonosítási architektúráról [1], és 2006-ban kívánja véglegesíteni a TC 224 WG15 munkacsoport az európai lakossági azonosítókártya szabványát.

8. Összefoglalás

Az egyes európai országok – köztük Magyarország – közigazgatásai által alkalmazott ügyfél-azonosítási és -hitelesítési megoldások, modellek jelentősen eltérnek egymástól, sőt többnyire az egyes országokon belül sem egységesek, ezért a jelen helyzetben nem vagy csak nagyon korlátozottan lehet létrehozni határokon átnyúló e-közigazgatási szolgáltatásokat.

Az Európai Unió ezért az i2010-hez kapcsolódó e-közigazgatási stratégiájában és cselekvési tervében kiemelt helyen kezeli az együttműködési képesség megteremtését a különböző tagországok e-hitelesítési rendszerei között. Ezeket a törekvéseket jelentős európai szabványosítási kezdeményezések is támogatják.

Irodalom

[1] Architecture for a European interoperable eID system within a smart card infrastructure, CEN Workshop Agreement, 2005. CWA 15264-1, ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eAuth/cwa15264-01-2005-Apr.pdf

[2] Common Terminological Framework for Interoperable Electronic Identity Management, Consultation paper, MODINIS-IDM Project, 2005. https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/GlossaryDoc

[3] Szerződés az Európai Közösség létrehozásáról, http://www2.datanet.hu/im/Primleg/EUSz-EKSz_EAKSz_HU_04-05-01.htm#_Toc63341811

[4] Az Európai Parlament és a Tanács 1999/93/EK Irányelve az elektronikus aláírásra vonatkozó közösségi keretfeltételekről, 1999. http://ccvista.taiex.be/Fulcrum/CCVista/hu/31999L0093-HU.doc

[5] Myhr, T.: Regulating a European eID. A preliminary study on a regulatory framework for entity authentication and a pan-European Electronic ID for the Porvoo e-ID Group, http://porvoo7.fjarmalaraduneyti.is/media/Porvoo7/Thomas_Myhr.doc, 2005.

[6] Windley, P. J.: Digital Identity, O'Reilly, 2005.

[7] A közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló 2004. évi CXL. törvény, http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0400140.TV

[8] Az elektronikus ügyintézés részletes szabályairól szóló 193/2005. (IX. 22.) Kormányrendelet, http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0500193.KOR

[9] A közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó követelményekről szóló 194/2005. (IX. 22.) Kormányrendelet, http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0500194.KOR

[10] Signposts towards eGovernment 2010, http://europa.eu.int/information_society/activities/egovernment_research/doc/minconf2005/signposts2005.pdf

[11] i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All, COM (2006) 173 final, http://europa.eu.int/information_society/activities/egovernment_research/doc/highlights/egov_action_plan_en.pdf

Autentikációs és autorizációs infrastruktúrák

BAJNOK KRISTÓF

MTA Sztaki, ITAK
kristof.bajnok@sztaki.hu

Kulcsszavak: autentikáció, autorizáció, identitás menedzsment, föderáció, biztonság

Egy intézmény alapvető érdeke, hogy az általa nyújtott szolgáltatásokhoz, illetve bizalmas információkhoz csak megfelelő azonosítás után férhessenek hozzá a felhasználók. Heterogén felhasználási környezetben hatékony azonosítást és jogosultság-ellenőrzést úgy lehet megvalósítani, ha erre önálló infrastruktúrát, middleware-t alkalmazunk. A cikk bemutatja ennek fontosságát és vázol néhány, más országokban már általánosan elterjedt identitás szövetségi (föderációs) modellt.

1. Bevezetés

Az informatikai rendszerek terjedésével és jelentőségük növekedésével együtt a felhasználók azonosítása és jogosultságaik megfelelő ellenőrzése alapvetően fontossá vált. Az informatikai biztonsággal kapcsolatos számtalan kutatásból azonban megállapíthatjuk, hogy sok esetben a biztonság legnagyobb veszélyeztetője maga a felhasználó. Lehet ugyan a mai tudományos vélekedés szerint többé-kevésbé védett rendszereket készíteni, de a biztonság sok esetben rugalmatlanságot, nehéz kezelhetőséget jelent, ami rendkívüli módon növelheti a költségeket; másfelől a felhasználó munkájának nehezítése bonyolult azonosítási eljárásokkal végső sorban éppen magát a megcélzott biztonságot áshatja alá. Ezért óriási nyomás nehezedik az iparra és a kutatókra, hogy olyan azonosítási megoldásokkal álljanak elő, amelyek egyszerre képesek megvalósítani a következő – olykor egymásnak ellentmondó – követelmények optimálishoz közeli kompromisszumát: *kriptográfiai megbízhatóság; a felhasználó számára egyszerű használat; rugalmasság, könnyű karbantarthatóság; szabványosság, kompatibilitás; költséghatékonyság.*

A cikk bevezető jelleggel – és a téma szerteágazósága miatt messze nem teljeskörűen – ismerteti az autentikációs és autorizációs infrastruktúrákban (AAI) gyakrabban használt eljárásokat, valamint vázolja az intézmények közötti megállapodások (föderációk) elterjedtebb modelljeit.

2. Autentikációs middleware

Kezdetben az alkalmazásokat saját azonosítási funkcióval szállították, azonban ez súlyos problémákat vetett fel. Egyrészt a megfelelő erősségű hitelesítési eljárást implementálni kellett (minden egyes alkalmazásban), másrészt számtalan felhasználói adatbázis jött létre, melyek konzisztenciáját nagyon nehéz volt biztosítani. Ez utóbbi problémát leginkább úgy lehetett kiküszöbölni, hogy a felhasználói információkat valamilyen központi adatbázisban (NIS, SQL, illetve címtárak) tárolták. A címtárakat először az ITU X.500 szabványa írta le (amely lekérdezéshez a DAP – Directory Access Protocolt definiálta), elterjedt és könnyen hozzáférhető implementációja azonban csak az LDAP-nak (Lightweight Directory Access Protocol [1]) készült el. A címtár lekérdezések szabványosításának jelentős előnye a hagyományos adatbázisokhoz képest éppen maga a *szabványosság*, azaz,, hogy a kliens bármelyik gyártó szerverétől (elvileg) pontosan ugyanúgy tud adatokat lekérdezni.

A központi felhasználó-adatbázisokban (vagy azokhoz kapcsolódóan) nem csak az azonosításához szükséges adatok tárolhatók, hanem – több más adat mellett – a felhasználó jogosultságai is, akár alkalmazásonként külön-külön. Ha az adatbázis elé megfelelő felhasználói felületet készítünk, akkor megoldható, hogy a felhasználók hozzáadása/törlése, illetve jogosultságainak beállítása ne a rendszergazda feladata legyen, hanem részévé váljon az intézmény humánerőforrás-kezelési és belső házirend (policy) kezelési folyamatainak. Ha az intézmény alkalmazásai központi felhasználó-adatbázist használnak, és ezt az adatbázist a humánerőforrás és a házirend nyilvántartásáért felelős adminisztrátorok tartják karban, akkor *identitás-menedzsmentről (Identity Management)* beszélhetünk.

Az intézményi identitás-menedzsment bevezetése alapvetően fontos az informatikai biztonság szempontjából is. Ugyan nagyon kellemetlen (és pazarló), ha egy új munkatárs azért nem tudja megkezdeni a munkát, mert még nem kapott jogosultságot a megfelelő alkalmazásokhoz, ennél sokkal nagyobb károkat tud okozni egy elbocsátott dolgozó, akinek nem szűnik meg azonnal a hozzáférése az üzletileg kritikus rendszerekhez.

3. Webes Single Sign-On

Egyre több helyen használnak belső vállalati környezetben webes alkalmazásokat. Azonban hiába van központi felhasználói adatbázis, az azonosítást min-

den egyes alkalmazásnál külön-külön el kell végezni. Sok esetben ez a felhasználótól újabb és újabb közreműködést kíván. (A felhasználó szempontjából a több faktoros azonosítás még további gondot okozhat, ha az azonosítási módszer PIN-kód, esetleg idő alapú token megadását követeli meg – de még az ujjlenyomatolvasó túl gyakori használata is kényelmetlenné válik előbb-utóbb.) E problémákat általában úgy lehet megoldani, ha az azonosítást különválasztjuk az alkalmazástól, tehát az azonosítást nem az alkalmazásban végezzük el, hanem egy dedikált azonosító (login) szerveren.

A webes alkalmazásokhoz kidolgozott Single Sign-On (WebSSO) megoldások működésének alapjául a HTTP protokoll szabványos elemei szolgálnak: az átirányítás (redirect) és a sütik (cookie). Számos WebSSO szoftver létezik, például Pubcookie, CAS, A-Select stb. Az azonosítás menetét szemlélteti az *1. ábra*.

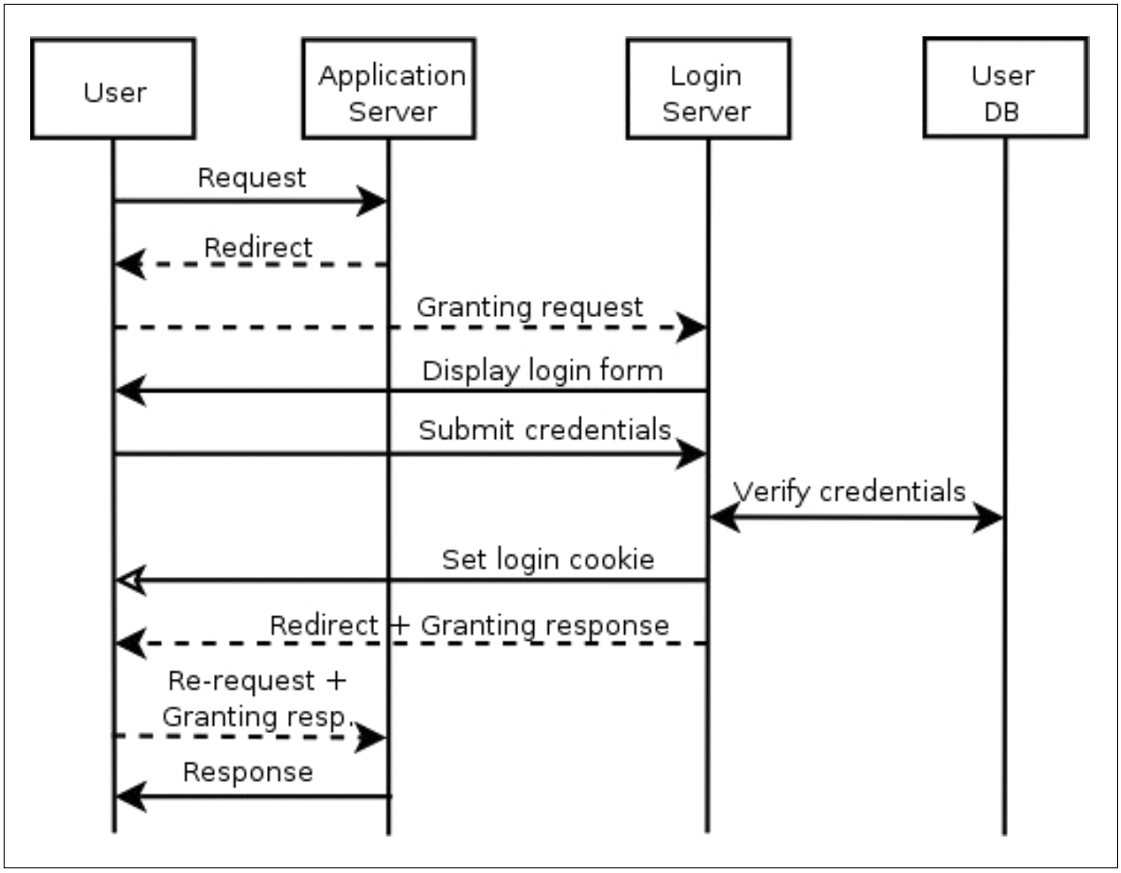
A felhasználó az azonosító adatait mindig a megbízhatónak tekintett login szervernek adja meg. Iső lépésként a webes alkalmazás előtt álló webszerver modul észleli, hogy még a felhasználónak nincs érvényes környezete (security context), ezért átirányítja a login szerverhez. Ez elvégzi az azonosítást, majd sikeres esetben készít egy úgynevezett feljogosító (granting) üzenetet az alkalmazás számára, majd ezt eljuttatja a webszerver modulnak. (Természetesen gondoskodni kell arról, hogy a granting üzenet ne legyen visszajátszható, ezért a válasz tartalmazza a requestben található véletlen elemet is.) A webszerver ezt ellenőrizve engedélyezi a hozzáférést az alkalmazáshoz.

Fontos megjegyezni, hogy ez a módszer csak a felhasználó azonosítást (autentikációt) oldja meg, a jogosultság kezelés (autorizáció) továbbra is az alkalmazás feladata marad. A magát már azonosított felhasználó „beazonosítása” (azaz az autorizációhoz, illetve az alkalmazás használatához szükséges további adatok lekérdezése) a granting üzenetből kinyerhető azonosító alapján történik. (Hasonlóan működnek a HTTP Basic autentikációt használó webes alkalmazások is: ott a webszerver az azonosítás után a felhasználónevet a REMOTE_USER változóban adja át.) Ez azt is jelenti, hogy az alkalmazásnak a felhasználó attribútumaiért közvetlenül a felhasználó-adatbázishoz kell fordulnia.

Amennyiben a felhasználó másik alkalmazáshoz fordul, az ugyanúgy a login szerverre irányítja át, ám ezúttal a login szerver (a korábban beállított süti alapján) észleli azt, hogy a felhasználó már azonosította magát, ezért az azonosító adatok elkérése nélkül kiállítja a granting választ. Így a második autentikációhoz már nincs szükség a felhasználó közreműködésére.

Mivel a legtöbb WebSSO megoldás (memóriában tárolt) sütiket használ, ezért az alkalmazásból történő kijelentkezés megvalósítása korántsem egyszerű. Vannak szoftverek, amelyek lehetővé teszik az alkalmazásonként történő kijelentkezést, azonban számos esetben csak a böngészőből való kilépéssel (vagy a sütik törlésével) lehet kijelentkezni.

A WebSSO – noha tényleg egyszerűsíti a felhasználó számára az autentikációt – biztonságossága leginkább a böngészőben tárolt cookie-k biztonságán múlik. Fontos észrevenni, hogy a login szervernél érvé-



1. ábra

Webes SSO alkalmazás (PubCookie) működésének folyamata [2]

nyes munkamenetünket tároló süti nem védhető visszajátszás ellen, ezért annak lehallgathatatlanságáról gondoskodni kell. Sajnos a böngészőket érintő hibák egy része kihasználható a cookie-k ellopására is, azonban ezek a hibák – WebSSO-tól függetlenül – minden olyan alkalmazást érintenek, amelyeket webböngészőn keresztül veszünk igénybe (hiszen így tetszőleges sessiont el lehet lopni).

A WebSSO megoldások előnye, hogy nagyon olcsón, minimális költséggel kialakíthatók úgy, hogy a legtöbb alkalmazáson csak kismértékben kell változtatni. (A webszerver autentikációs moduljait használni képes alkalmazások például változtatás nélkül működhetnek.)

Az azonosítás biztonsága növelhető azáltal, ha a login szerver valamilyen erős autentikációs mechanizmust (például hardver tokenes megoldást) alkalmaz. Mivel ekkor a mechanizmust csak a login szerver számára kell implementálni, ezért a WebSSO megkönnyítheti az erősebb autentikáció bevezetését az intézményen belül, illetve jelentősen csökkentheti a bevezetés költségeit.

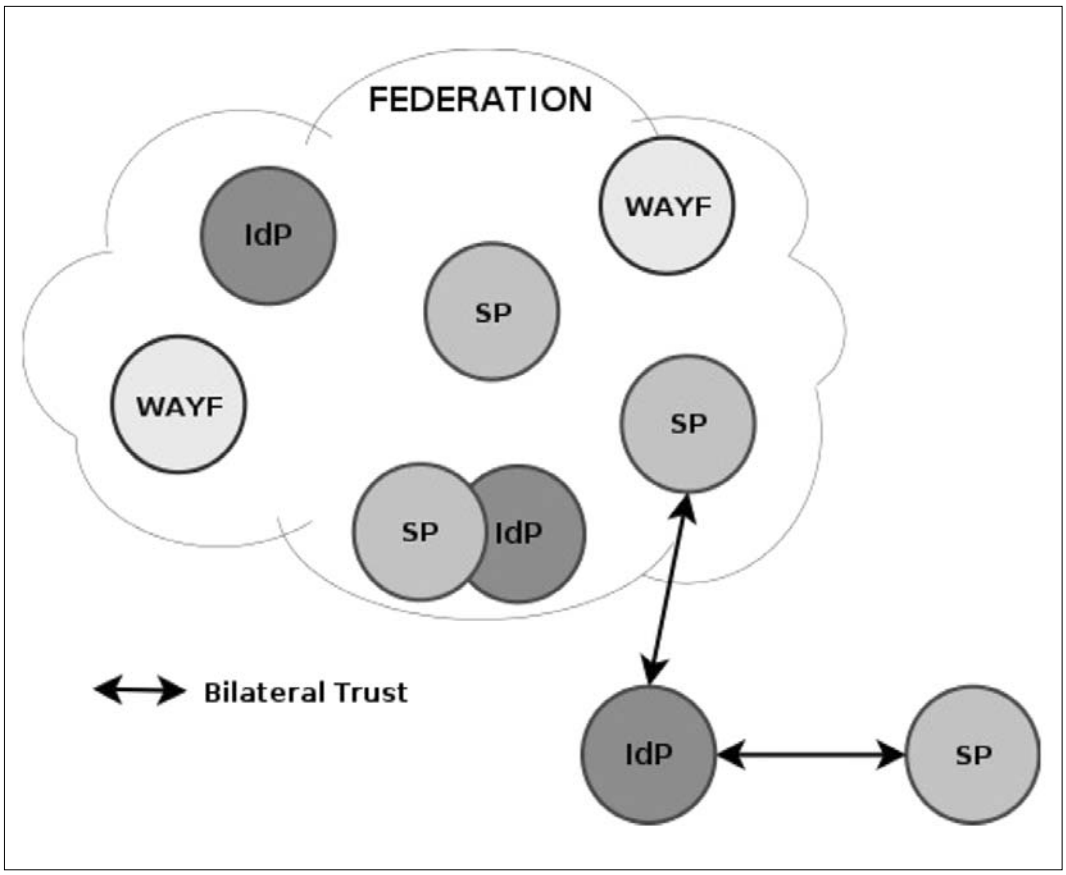
4. Föderációk

A cikk elején szót ejtettünk arról, hogy egy intézmény informatikai biztonságának alapja a megfelelő identitás-menedzsment. Gyakran előfordul azonban, hogy egy projekt megvalósításában több intézmény dolgozik együtt, és a munka során közösen használnak erőforrásokat. Más intézmények dolgozóinak saját adatbázisunkba való felvétele viszont számos problémát és nehézséget okozhat, hiszen például az egyik intézmény nem biztos, hogy értesíti a másikat arról, ha elbocsát egy, a közös projekten dolgozó munkatársat. Szintén a „befogadó” intézményt terheli a felhasználói panaszok kezelése (jelszóváltoztatás, bejelentkezési problémák), ezen kívül a felhasználónak új azonosító adatokat (felhasználónév/jelszó, chipkártya stb.) kell használnia.

A megoldást az jelentheti, ha a két intézmény szövetségre (Federation) lép egymással, és kölcsönösen *megbíznak* egymás identitás-menedzsmentjében. Nagyon fontos megérteni, hogy ez a „bizalom” nem elsősorban informatikai megoldásokon, hanem jogi kötelezettségvállalásokon alapszik. A megállapodás során a felek számtalan dolgot rögzíthetnek: az identitás-menedzsmentben használt eljárásokat, az alkalmazható autentikációs metódusokat, a felhasználóról kiadott attribútumok alkalmazásának feltételeit vagy akár rendelkezésreállási paramétereket. Természetesen a szövetségkötés nem csak kétoldalú lehet, hanem kettőnél több intézmény is együttműködhet.

Mielőtt a föderációk részletesebb ismertetését tárgyalnánk, érdemes észrevenni, hogy a „nem-digitális” világban is több helyen használnak bizalomra épülő föderációkat. Amennyiben A ország megbízik B ország „identitás-menedzsmentjében”, akkor B ország polgárai a B ország által kiállított azonosító okmányukkal (útlevelükkel) utazhatnak A-ba.

Természetesen előfordulhat, hogy két ország nem bízik meg egymásban: ekkor vízumot kell használni, a vízumot ugyanis mindig a fogadó állam (nagykövetsé-



2. ábra

Föderációs topológia. A nyilak kétoldalú (föderáción kívüli) bizalmat jelentenek

ge) állítja ki. A különbség világos: a vízum kiállítás körülményes és drága, ellenben nem szükséges hozzá bizalomra épülő kapcsolat.

Egy föderációban levő szolgáltatásokat funkciójuk szerint általában három osztályba sorolhatjuk. Vannak az *Identitás Szolgáltatók (IdP, Identity Provider)*, amelyek a felhasználó azonosítását végzik, illetve esetlegesen adatokat közölnek a felhasználóról a *Tartalomszolgáltatók (SP, Service Provider)* számára, amelyek közvetlenül a felhasználó számára nyújtanak (azonosítást igénylő) szolgáltatást.

Egy intézmény általában működhet egyszerre IdP-ként és SP-ként is. E két szolgáltatáson kívül lehetnek még olyan alkalmazások, amelyek a Föderáció működtetését segítik elő. Amennyiben egy Föderációban több egyenértékű IdP vesz részt, szükség van olyan alkalmazásra, melynek segítségével a felhasználó Identitás Szolgáltatója kiválasztható. Ez történhet implicit módon (például a felhasználónév hordoz információt az IdP-ről), illetve lehetséges olyan speciális alkalmazás használata is, amely első látogatáskor megjeleníti a felhasználó számára az elérhető Identitás Szolgáltatókat. Ezt a szolgáltatást *Home Location* szolgáltatásnak nevezzük, de elterjedt a „Where Are You From?" (WAYF) elnevezés is.

A Föderációban résztvevő elemek kommunikációjához általában szükség van *metaadatokra*, amelyek többek között tartalmazzák a szerverek közötti biztonságos adatkapcsolathoz szükséges PKI tanúsítványokat is.

4.1. SAML

Mivel egy Föderációban résztvevő intézmények általában szabadon dönthetnek arról, hogy milyen szoftvermegoldást alkalmaznak, szükség van arra, hogy az egyes elemek közti kommunikáció szabványos módon történjen.

2001-ben az informatikai ipar legnagyobbjai (Hewlett-Packard, Sun, Intel, Novell, Entrust, RSA stb) elkezdték kidolgozni a biztonsági kommunikáció nyílt szabványát, amelyet 2002-ben az OASIS szabványosítási szervezet *SAML (Security Assertions Markup Language* [3]) néven elfogadott. A szabvány jelenlegi, 2.0-ás verzióját 2005 márciusában fogadták el, ez jelentős újításokat hozott a korábbi, már működő rendszerekben használt 1.1-es verzióhoz képest. Funkcionális újítások mellett az új verzió leginkább azért érdekes, mert jelentős lépéseket tesz annak érdekében, hogy képes legyen integrálni meglévő megoldásokat (pl. Shibboleth, Liberty, ill. nagy gyártók Identity Management termékei) és szabványokat (WS-Security), így várható, hogy az AAI elemek kommunikációjának egyfajta „lingua franca"-ja lesz. Ez okból is érdemes a szabvánnyal részletesebben foglalkozni.

A SAML XML alapú keretrendszert definiál, amely autentikációs és jogosultsági adatok, valamint attribútumok szabványos kommunikációját teszi lehetővé. A keretrendszer tartalmazza az egyes elemek XML sémáját, valamint protokollokat és profilokat ír le. Mivel a SAML XML alapú, ezért így számos átviteli módszerhez illeszthető (binding).

Egy SAML üzenet legkisebb egysége az entitásra vonatkozó *állítás (statement)*, amely vonatkozhat autentikációra (Authentication Statement), a felhasználó valamely attribútumára (Attribute Statement), illetve valamilyen autorizációs döntésre (Authorization Decision Statement). Az állítás hordozhat paramétereket is, így például leírható, hogy az autentikált entitás milyen módszerrel lett azonosítva.

Egy SAML *igazolás (Assertion)* egy vagy több állítást tartalmazhat, kiegészítve a hitelesség ellenőrzését lehetővé tevő paraméterekkel: azonosító, kiállító (Issuer), kiállítás dátuma, „célközönség" (audience) stb. (Magyarítási megjegyzés: az angol „assertion" szó szinonímája a „certificate"-nek, amit a szakirodalom bevett módon tanúsítványnak fordít. Mivel tanúsítvány alatt általában X.509 tanúsítványt értünk, a félreértések elkerülése végett a cikkben az „assertion"-re magyarul az „igazolás" szót használjuk.)

Föderált környezetben az entitás megnevezése komoly problémákat vethet fel. Adatvédelmi okok miatt sok esetben tilos (és biztonsági megfontolások alapján sem célszerű) az entitásnak az IdP rendszerében érvényes azonosítóját átadni az SP számára, így legtöbbször egy felhasználói munkamenetre érvényes ideiglenes azonosítót (transient opaque identifier) alkalmaznak.

Az igazolás a hitelesítés érdekében opcionálisan tartalmazhat digitális aláírást is. A digitális aláírásra a szabvány a W3C XML Signature szabványának használatát írja elő. (Pontosabban az ebben definiált „enveloped signature" aláírási eljárást.) Felmerülhet a kérdés, hogy miért nem kötelező a digitális aláírás használata? A válasz az, hogy számos esetben már hitelesített a kommunikációs csatorna – például kölcsönös SSL hitelesítéssel –, így szükségtelen az egyes igazolásokat külön-külön aláírni.

SAML üzeneteket többféle módon továbbíthatunk az elemek között, a szabvány részletesen foglalkozik az egyes hordozó protokollokkal (bindings). Az alapvető üzenettovábbítási mód a SOAP (Simple Object Access Protocol), melyet leggyakrabban HTTP felett használnak. A szintén gyakran használt HTTP POST csatolásnak akkor van jelentősége, amikor a felhasználót – például az azonosítási eljárás során – át kell irányítani egyik kiszolgálóról a másikhoz. A csatolás lényege, hogy a webszerver olyan weboldalt állít elő, amely egy HTML form-ot tartalmaz, amelyet a felhasználó böngészője egy apró JavaScript kód segítségével automatikusan elküld a fogadó kiszolgálóra. A HTML form része egy rejtett változó, amely a tényleges SAML üzenetet tartalmazza.

A HTTP POST csatolás nagyvonalúan bánik a felhasználó sávszélességével, hiszen ekkor a teljes SAML üzenetet le kell tölteni a forrástól, majd azt el kell küldeni a célállomásnak. Ennek kiküszöbölésének érdekében definiálja a SAML az *Artifact* fogalmát, amely valójában egy hivatkozást, referenciát jelent az eredeti

SAML üzenetre. Artifact binding használatakor a felhasználó böngészője csak a (sokkal kisebb méretű) referenciát adja át a célállomásnak, majd az Artifact Resolution Protocol segítségével közvetlenül (általában SOAP segítségével) kérdezi le az eredeti SAML üzenetet.

5. Föderációs modellek

Alapvetően kétféle föderatív modellt különböztethetünk meg. *Központosított föderációnak* nevezzük azt a modellt, amelyben csak egyetlen identitás-szolgáltató található, minden más intézmény tartalomszolgáltató. Ilyen például a Microsoft Passport és a magyar elektronikus közigazgatás azonosítási rendszere, az Ügyfélkapu.

Mivel a központosított modellekben minden identitással az egyetlen IdP rendelkezik, annak megbízhatósága és helyes működése a teljes rendszer biztonsága szempontjából kritikus. Központosított föderációk esetén az egyes tartalomszolgáltatók nincsenek egymással összakapcsolva, köztük adatcsere nem történik.

Elosztott föderációról beszélhetünk akkor, ha egy föderáción belül több identitás-szolgáltató is működik. Ilyenkor az IdP-k jellemzően egyenértékűek, a hozzáférés szabályozása (autorizáció) az SP-knél történik.

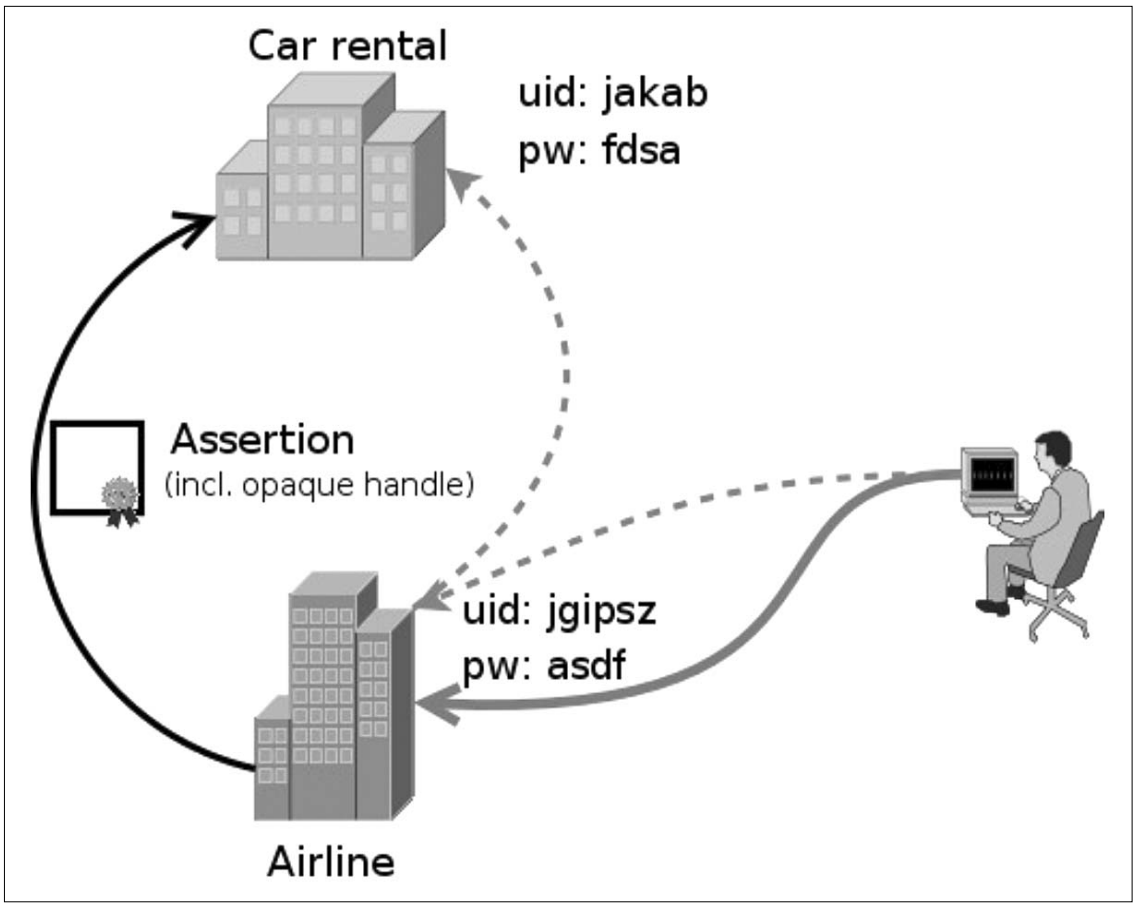
5.1. Liberty Alliance

A Liberty Alliance [4] projekt 2001-ben indult, korábban nem létezett nyílt szabványokra épülő identitás menedzsment federációs megoldás. Létrehozói elsősorban ipari cégek: Sun Microsystems, Hewlett-Packard, IBM, Intel, Oracle stb. A modell szerint a felhasználó különböző fiókokkal (account) rendelkezik különböző tartalomszolgáltatóknál, így mindegyik tartalomszolgáltató képes őt azonosítani, azonban az azonosító adatok szolgáltatónként különbözők lehetnek. A Liberty lehetőséget ad arra, hogy a felhasználó a különböző azonosítóit *összekapcsolja*, majd az SP-k szolgálatatásait egyetlen szolgáltatónál történő azonosítás után vehesse igénybe, tehát SSO-t biztosít. Lényeges megjegyezni, hogy ez az összekapcsolás kizárólag a felhasználó közreműködésével jöhet létre. Autorizáció kizárólag az egyes szolgáltatóknál található adatok alapján történik, adatcsere a szolgáltatók között csak annyi lehetséges, amennyi az összekapcsoláshoz, illetve az elosztott autentikációhoz szükséges.

5.2. Shibboleth

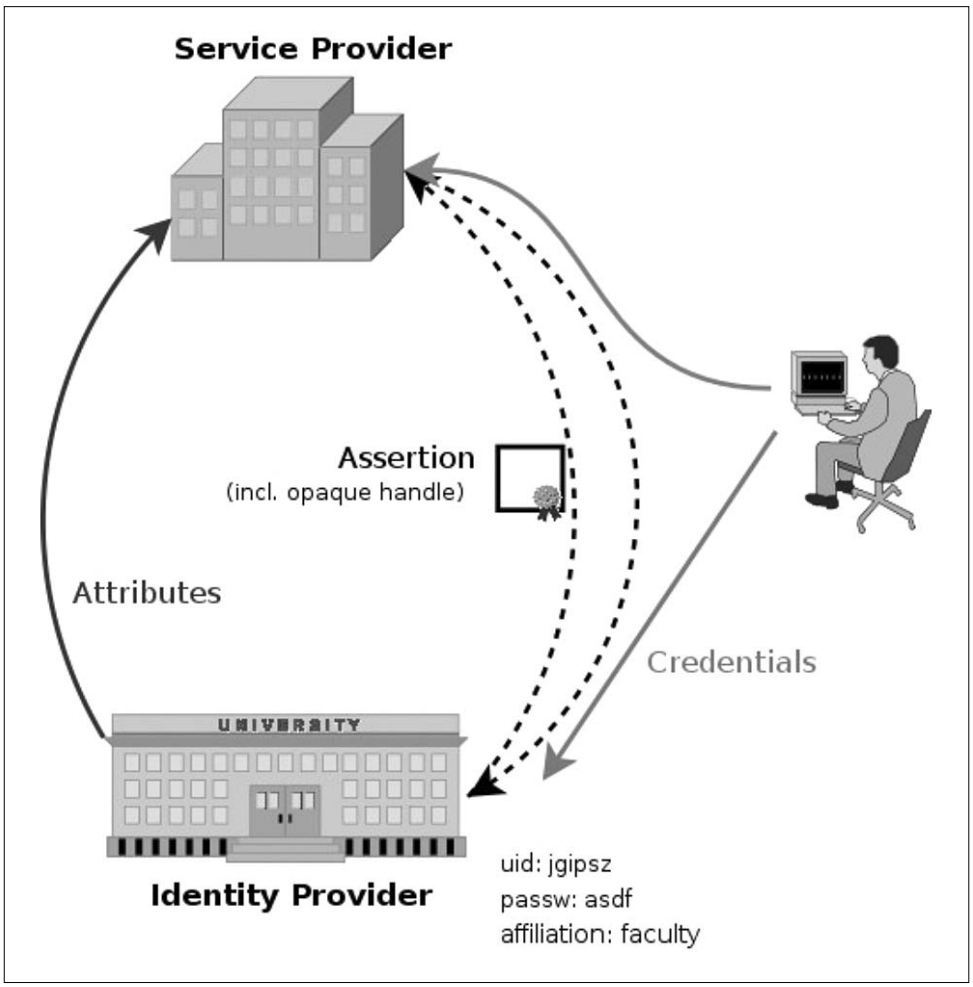
A Shibboleth projektet [5] az amerikai Internet2 indította. A Shibboleth egy elosztott autentikációs és autorizációs rendszer, ahol az erőforrásokhoz történő hozzáférés az identitás-szolgáltatótól kapott attribútumok alapján történik. A felhasználó úgy vehet igénybe szolgáltatásokat a föderáción belül, hogy csak egyetlen identitása van az „anyaintézménynél” (home institution).

A felhasználó első lépésben egy védett erőforráshoz fordul, azonban a Shibboleth webszerver-modulja átirányítja őt azonosítás céljából az identitás-szolgálta-



3. ábra

Liberty föderációs modell. Az autókölcsönző szolgáltatásait a légitársasághoz történő bejelentkezés után vehetjük igénybe



4. ábra
Shibboleth föderációs modell.
A szaggatott vonalak HTTP átirányítást jelölnek.

tóhoz. Azonosítás után az IdP kiállít egy SAML Assertion-t, amelyet (a böngészőn keresztül) eljuttat az SP-nek. Ezen a ponton a felhasználó azonosítottnak tekinthető.

Az autorizációs szakaszban az SP (az igazolásban található tranziens azonosító alapján) adatokat kér a felhasználóról. Mivel az adatcsere során személyes adatok utaznak, az IdP-nek lehetősége van arra, hogy tartalomszolgáltatónként, vagy akár felhasználónként *attribútum kiadási szabályzatot (Attribute Release Policy, ARP)* definiáljon. Az SP a kapott adatok és az erőforráshoz tartozó attribútum elfogadási szabályzat (Attribute Acceptance Policy, AAP) alapján engedélyezi vagy megtagadja a hozzáférést.

Mivel a Shibboleth általában tranziens azonosítókat használ, legjellemzőbb alkalmazási területei azok, ahol nem szükséges a felhasználó pontos kilétét megállapítani, hanem valamilyen jellemző csoporthoz tartozás alapján (például tanár egy bizonyos intézményben, hallgató egy adott kurzuson stb.) engedélyezzük a hozzáférést. Tipikusan ilyen terület lehet az e-learning illetve a hozzáférés olyan elektronikus gyűjteményekhez, melyek előfizetői nem az egyes felhasználók, hanem intézmények.

Az autorizációra szolgáló attribútumok használatának feltételeit a föderációs szerződés szabályozza (jogi eszközökkel). A Shibboleth-ben lehetséges ugyan állandó azonosítót is használni, azonban ekkor tisztázni kell, hogy ez milyen – a felhasználó privát szféráját érintő – adatvédelmi kérdéseket vet fel.

6. Összefoglalás

Az autentikációs és autorizációs infrastruktúra lényege, hogy az azonosítási és jogosultság-ellenőrzési feladatokat az alkalmazásoktól elkülönítve, szabványos illesztési módszerek felhasználásával végezzük.

Ilyen infrastruktúra létrehozásának akkor is lehet létjogosultsága, ha egyetlen intézményen belül használjuk, mivel a Single Sign-On egyszerűsíti a felhasználó számára az autentikációt, és megfelelően alkalmazva, magát az intézményi informatikai biztonságot is növelheti.

Várhatóan egyre több olyan projekt indul majd, melyben több intézmény közösen használ erőforrásokat. Ilyen esetekben a föderált identitás-menedzsment jelentősen csökkentheti a felhasználókhoz kapcsolódó költségeket.

Irodalom

[1] Lightweight Directory Access Protocol, RFC 3377, http://www.rfc-editor.org/rfc/rfc3377.txt
[2] PubCookie: http://www.pubcookie.org/docs/how-pubcookie-works.html
[3] OASIS Security Services Technical Committee: Security Assertion Markup Language (SAML) Schema and Specifications, http://docs.oasis-open.org/security/saml/v2.0/saml-2.0-os.zip
[4] Liberty Alliance: http://www.projectliberty.org/
[5] Shibboleth: http://shibboleth.internet2.edu/

Személyes adatok védelme és az AAI rendszerek

dr. Rátai Balázs

Informatikai- és Kommunikációs Jogi Kutatóintézet, Pécs
balazs.ratai@carneades.hu

A személyes adatok védelméhez való jogot az Alkotmány 59. paragrafusa rögzíti. Az Alkotmánybíróság a személyi szám alkotmányellenességét kimondó 15/1991-es határozatában aktív személyiségvédelmi jogként értelmezte az adatvédelemhez való jogot és leglényegesebb tartalmát abban határozta meg, hogy az emberek külső kényszerektől mentesen saját maguk jogosultak rendelkezni személyes adataik feltárásáról és felhasználásáról.

A személyes adatok kezelésének legfontosabb törvényi kereteit ma az 1992. évi LXIII. tv. határozza meg. Ebben a törvényben került meghatározásra, hogy mi számít személyes adatnak, valamint az, hogy milyen kötelezettségekkel jár az, ha valaki mások személyes adatait kezeli.

Az AAI rendszerek üzemletetése alapvető céljuknál fogva személyes adatok kezelésével jár együtt, ezért egy AAI rendszer létrehozásakor már a rendszertervezési fázisban érdemes foglalkozni azzal a kérdéssel, hogy az adatvédelmi előírásokat miként tudja majd teljesíteni az AAI rendszer üzemeltetője.

Az AAI rendszerek által kezelt személyes adatok három nagyobb csoportba oszthatók:

A) autentikációs adatok (többnyire természetes személyazonosító adatok),
B) autorizációs (jogosultsági) adatok,
C) a rendszer működése során keletkező adatok.

A három adatkör közül az első azokat az adatokat takarja, amelyek lehetővé teszik a felhasználók személyének azonosítását, azaz a „Ki a felhasználó?” kérdésre adnak választ.

Az autorizációs adatok azt a kérdést válaszolják meg, hogy mire jogosult az adott felhasználó.

A harmadik csoport pedig azon adatokat takarja, amelyek az AAI rendszerek működése során keletkeznek és az adatvédelmi törvény személyes adat meghatározásából adódóan személyes adatnak tekintendők. Az alábbi táblázat néhány példát tartalmaz a három adatkörbe sorolható személyes adatokra vonatkozóan.

Az AAI rendszerek tekintetében az adatvédelmi szabályozás által támasztott adatvédelmi követelmények és ezek teljesítésének hogyanja természetesen az AAI rendszer által kezelt személyes adatok körétől, mennyiségétől függ és nyilvánvaló összefüggésben áll azon szolgáltatások sajátosságaival, amelyek igénybevételét az AAI rendszer segíti. Ebből adódóan nagyon nehéz általánosságban meghatározni azt, hogy milyen módon kerülhető el a jogosulatlan adatkezelés.

Ennek ellenére érdemes néhány ökölszabályt szem előtt tartani egy AAI rendszer létrehozása és üzemeltetése során:

A) Törekedni kell arra, hogy minél kevesebb személyes adat tárolására és továbbítására kerüljön sor.
B) A rendszer működése során keletkező személyes adatok tárolására a lehetőségekhez képest egyáltalán ne, vagy csak rövid ideig kerüljön sor.
C) Az autentikációs és autorizációs adatok kezelésének szükségességét rendszeres időközönként felül kell vizsgálni.

Autentikációs adatok	Autorizációs adatok	Másodlagosan keletkező adatok
– név	– igénybe vehető szolgáltatások	– igénybevett szolgáltatás
– lakcím	– egyéb olyan jellemzők, amelyek a szolgáltatás igénybevételére való jogosultságot megalapozzák	– szolgáltatás igénybevételének időpontja
– életkor		– szolgáltatás igénybevételének helye
– azonosító		– szolgáltatás használatának időtartama

Hálózati köztes rendszerek

HORVÁTH GÁBOR

ELTE Informatikai Igazgatóság
hg@ludens.elte.hu

Kulcsszavak: hálózatmenedzsment, hálózati incidenskezelés és eszköznyilvántartás, konfiguráció- és szűrőlista-karbantartás

Az utóbbi pár évben a hálózatos szakemberek munkája egyre inkább megváltozott. Az egyre több szolgáltatás miatt egyre több szervert és konfigurációs fájlt kell karbantartani. Hogyan tudjuk csökkenteni ezt az adminisztrációs terhet? A sok kicsi, nem dokumentált script használatának nincsen sok értelme. Mit értünk middleware rendszer alatt és hogyan tudjuk használni a hálózatmenedzsment egyes területein?

1. Bevezetés

Bizonyára sok számítógéphálózat üzemeltető és tervező kolléga érzi úgy, hogy valami változik, nem pusztán a kapcsolatok sávszélessége és a hálózati berendezések csomagtovábbító képessége növekszik, hanem az elvárt szolgáltatáspark és a munkafolyamatok szerkezete változik lassan és biztosan, nem a legkellemesebb irányba. Mik ennek a változásnak a mozgatórugói, pontosan hogyan zajlik le és miket tehetünk a munkánk szakmai színvonalának megóvása érdekében? Hol találkoznak a hálózattal a sokat emlegetett middleware rendszerek, mit nyújtanak nekünk és milyen veszélyeket jelent, ha nem valódi middleware rendszert állítunk üzembe?

2. A probléma

A 90-es évek hálózati rendszergazdái (azon informatikus szakemberek, akik nagyvállalatok gerinchálózati infrastuktúráját működtetik) elsősorban a fizikai kapcsolatok létesítésére és fenntartására összpontosítottak, a gyors és megbízható csomagtovábbítás általában elegendő volt a felhasználói / megbízói elégedettséghez.

A hálózatos szakember munkaidejének jelentős részében célberendezések (router, switch) installálásával, cseréjével, felügyeletével foglalkozott és azokat a problémákat oldotta meg előszeretettel, amik ezen a szinten igényes szakmai megoldásokkal kezelhetők voltak (például vonalszakadás, router fizikai meghibásodás). Ami a lokális hálózat egyik portján „beesett", azt minél gyorsabban megpróbáltuk a megfelelő kimeneti porton kiadni, függetlenül annak tartalmától, valamint azzal sem foglalkoztunk, hogy mit tud vele kezdeni a címzett.

A szolgáltatási helyzet azonban változott, ami a hálózatüzemeltetőktől is más megközelítést kívánt. A változás főbb komponensei:

1. A számítógépes hálózat még az oktatói és kutatói területen is kinőtte a „hobbilevelezés" besorolást és az intézmény napi életének elengedhetetlen része lett. A dolgozók (és az intézmény vezetése) egyre inkább „közműként" tekint a hálózatra, elvárja a nagy rendelkezésre állást a teljes szolgáltatási területen, elvárja a szűk keresztmetszetek megszüntetését. Emiatt minden kulcsfontosságú berendezést, szervert minimum duplikálni kell, az automatikusan működésbe lépő redundancia valamint a terhelésmegosztó megoldások a hálózattervezés alappillérei lettek.

2. A gyakorlatban a hálózat „haszonélvezői", a jóhiszemű felhasználók nem tudták magukat (és gépeiket) megvédeni az Internet irányából rájuk leselkedő veszélyektől. (Valljuk be, a személyi tűzfalak és VPN kliensek installálása nem is várható el például a középkori történelem professzorától.) A hálózatosok tehát elkezdtek tűzfalakat és szűrőlistákat konfigurálni, megvédeni a felhasználókat a rosszindulatú forgalomtól.

3. Egyre több olyan hálózati entitás jelent meg, ami adatot termelt vagy igényelt. A legtöbb hálózatban már működik valamilyen hálózatmonitorozó, szolgáltatás-figyelő program, amiknek aktuális konfiguráció szükséges, és a keletkező adatokat fel kell dolgozni.

4. Több olyan „kényelmi" szolgáltatás vált a felhasználás részévé, ami eredetileg nem volt a kiszolgálás része, de nagyon kellemesek, mint a DHCP vagy a wireless hozzáférés. Ezek azonban saját konfigurációs komponensekkel rendelkeznek.

Mindezeknek van egy markáns és megkerülhetetlen hatása: a hálózatos rendszergazdáknak egyre több adatot kell egyre több helyre (általában konfigurációs fájlba) beírniuk. Ezeket a konfigurációkat konzisztensen, ellentmondásmentesen kell vezetni, a növekvő követelményeknek megfelelően egyre kisebb reakcióidővel. Ha például a felhasználó igényel egy új hálózati végpontot, akkor ennek adatait (IP-, VLAN-, hardware Ethernet cím, végponti azonosító) a DHCP és DNS szerverekbe fel kell venni, a megfelelő switch portot VLAN-ba kell helyezni, a router szűrőlistákba, firewall-adatbázisokba be kell jegyezni stb. Mindezek nagyon gondos és mennyiségileg jelentős adminisztrációt igényelnek, ami nem tekinthető igényes szakmai munkának.

3. A megoldás lehetőségei

A hálózatos szakemberek joggal érzik úgy, hogy munkidejükben túl sok a mechanikus munka, automatizálható adminisztráció, keveset tudnak a tervezéssel, mérnöki problémákkal foglalkozni. Ugyanakkor pazarlás is a „drága" mérnököket text konfigurációs fájlok karbantartására használni. A probléma megoldására a következő megoldások kínálkoznak:

a) Vegyünk fel kevésbé képzett, szerződéses munkatársakat a konfigurációs fájlok karbantartására. Nem túl jó megoldás, mivel a hálózati komponensek jogosultsági rendszere általában nem támogatja az ilyen irányú feladatmegosztást, tehát a munkatárs gyakran teljes jogosultsággal tud „garázdálkodni". Ezenkívül a módosításokat továbbra is ember végzi, aki tévedhet, fáradt lehet, elgépelhet stb.

Rövidítések és fogalmak jegyzéke

DHCP – Dynamic Host Configuration Protocol:
Lehetővé teszi, hogy mindazokat az adatokat, amik a hálózatra kapcsolódáshoz és a forgalmazáshoz szükségesek (pl. IP-cím, DNS szerver címe stb.) ne az egyes számítógépeken, hanem központi szerveren tároljuk.

Firewall – tűzfal:
Egyszerűbb változatai a hálózati csomagok szűrésével, bonyolultabb megoldásai a hálózati kapcsolatok nyilvántartásával és a bennük folyó kommunikáció követésével próbálják meg a nemkívánatos forgalmat azonosítani és eltávolítani. Nagy sávszélességű változatai általában célberendezések. A személyi tűzfal (personal firewall) egy olyan program, ami a gazdagépet védi a megengedett kapcsolati mintázatok megtanulása után.

IDS – Intrusion Detection System:
Olyan célberendezés, ami a hálózati forgalom megadott minták szerinti figyelésével a rosszindulatú használatot próbálja meg valós időben jelezni. A logfile elemző rendszerek utólag azonosítják a gyanús hálózati tevékenységet.

Router – forgalomirányító:
A csomagok továbbküldési irányának kiválasztásához nem csak a saját konfigurációját, hanem más forgalomirányítók elküldött irányítási adatait is felhasználja.

SNMP – Simple Network Management Protocol:
A hálózati entitások tulajdonságainak szabványos lekérdezésére és módosítására kifejlesztett kapcsolati felület. Használata – több műszaki ok miatt – csak a lekérdezés területén terjedt el.

VLAN – Virtual Local Area Network:
Virtuális helyi hálózat – A helyi hálózat fizikai struktúrájának további tagolását lehetővé tevő eszköz, amivel a hálózaton terjedő csomagok halmazokba sorolhatók.

VPN – Virtual Private Network:
Virtuális magánhálózat – Lehetővé teszi, hogy egy hálózat egy tagját (vagy részhálózatát) egy – általában titkosított – kapcsolaton keresztül egy másik hálózat tagjaként (tagjaiként) használjuk.

b) Irjunk „okos" script-eket, amik konzisztens módon elvégzik a szükséges konfigurációs módosításokat. Ez egy sok helyen alkalmazott és (kisebb cégeknél) jelenleg is működő megoldás. A következő problémák vannak vele:

– A script-ek dokumentáltsági foka (a legtöbb helyen) alacsony. Aki már „örökölt" ilyen programot szabadságolt kollégájától, és hibát kellett keresnie benne, az nem lelkesedik annyira ezért a megoldásért.
– A remek hálózatos mérnökök (tisztelet a kivételeknek) nem túl igényes programozók, a hibakezelés, portolhatóság, erőforrás-takarékosság nem jellemzői ezeknek a mágikus script-eknek.
– Az üzemeltetési környezet, a gerinchálózat felépítése folyamatosan változik. Ezeket az adatokat a script-ek „beépítve" tartalmazzák, nincsen törzsadatbázis vagy topológia adatbázis. Például egy új router üzembe állítása esetén a script-eket egyenként kell megtanítani az új interfészekre, ismét csak fájlokat editálunk, nagy fegyelemmel és odafigyeléssel...

c., Vásároljunk olyan programot, ami ezt a terhet leveszi a vállunkról. De ez nem annyira egyszerű dolog, mint amennyire az eladói oldal beállítja. Mit is kell tudnia egy ilyen programnak? Az biztos, hogy valahol a sok hálózati entitás között áll, adatokat cserél velük, azokat tárolja, ellenőrzi, átalakítja, továbbítja. Az ilyen alkalmazásokat nevezzük köztes rendszernek, middleware-nek.

4. A hálózati middleware funkciói

1) Kapcsolatot tart fent a hálózati entitásokkal, adatcserét folytat velük. Ezen entitások jelentős része nem rendelkezik olyan kapcsolati interfésszel, amin ez az adatcsere univerzálisan megtörténhet, általában a middleware oldalnak ismernie kell a másik fél saját adattárolási vagy kapcsolati formátumát. (például a SNMP erre a célra nagyon nehézkesen és korlátozottan alkalmazható csak, különösen problémás a hálózati eszköz konfigurációjának módosítása ezen a módon.)

Milyen hálózati komponensekről van szó?

– Hálózati célberendezések, router-ek, switch-ek. A berendezés saját formátumában szűrőlistákat, interfész- és port konfigurációkat kell előállítani és a berendezésre tölteni azokat. Le kell kérdezni konfigurációs beállításokat és interface/port állapotokat, számlálókat.
– Hálózatbiztonsági célberendezések, tűzfalak, IDS-ek, VPN koncentrátorok. Szűrőlistákat, konfigurációs beállításokat kell előállítani a részükre, jelzéseket kell kezelni.
– Hálózati szolgáltató szerverek, DHCP szerver, DNS szerver, authentikációs szerverek stb. Konfigurációs adatokat, bejegyzéseket kell aktualizálni. Delegált zónák, külső szervezetek esetében zónalekérdezés is szükséges.

2) Felhasználói felületet biztosít a rendszer „humán” komponenseinek:
– Hálózatos mérnökök.
Bizony ők is a rendszer komponensei, reguláris felületet kell biztosítani nekik a „kézi” módosítások elvégzésére, az általános szabályok (pl. szűrési policy) felvitelére. Ezen a felületen kell kezelni a berendezések és fizikai konfigurációk változását (kábelkönyv).
– Operátorok, helpdesk.
Ők azok, akik a felhasználói igényeket, módosítási kérelmeket felviszik a rendszerbe, az érdeklődő felhasználót tájékoztatják. A hálózati middlewarenek tehát ügykezelő funkcionalitással is kell rendelkeznie.
– Felhasználók.
Sok esetben (pl. letiltott gépek listája) meg kell adni a közvetlen lekérdezés lehetőségét.
Zárt felhasználói kör esetében a közvetlen ügyfelvitel (DNS bejegyzés igénylése) lehetőségét is érdemes biztosítani. Ekkor a hálózat üzemeltetői csak engedélyezik a folyamat lefutását és a konfigurációs módosulások életbe lépését.
Az emberi kapcsolati interfésznek a web felület kézenfekvő, mivel a szükséges kliens már a legtöbb desktop gépen rendelkezésre áll. Természetesen nem „sportszerű” egy bizonyos web böngésző használatát előírni.

3) Karbantartja a saját adatbázisát. A hálózatról rendelkezése álló információk alapján eldönti, hogy a beérkezett kérések kiszolgálhatók-e, az adatokon tartalmi ellenőrzést is végez. A módosulások átvezetése után eldönti, mely komponenseknek szükséges a változásokat továbbítani. Lehetőséget biztosít a törzsadatok (kapcsolattartók, berendezés adatok) karbantartására, a hálózati topológia lekérdezésére. Lehetőleg kapcsolatot tud létesíteni a cég saját törzsadattáraival (pl. LDAP kapcsolat).

4) Kapcsolatot tart fent a „társrendszerekkel”, hálózatfigyelő, szolgáltatás-monitorozó alkalmazásokkal (pl. MRTG, Nagios), illetőleg a cég saját, speciális hálózati alkalmazásaival. Részükre konfigurációkat, topológiai információkat továbbít, fogad állapot- és terhelési adatokat.

5. Hogyan működik a hálózati middleware?

A hálózati middleware működését érdemes néhány gyakorlati példán keresztül megismerni.

1. példa: Végponti igénykezelés

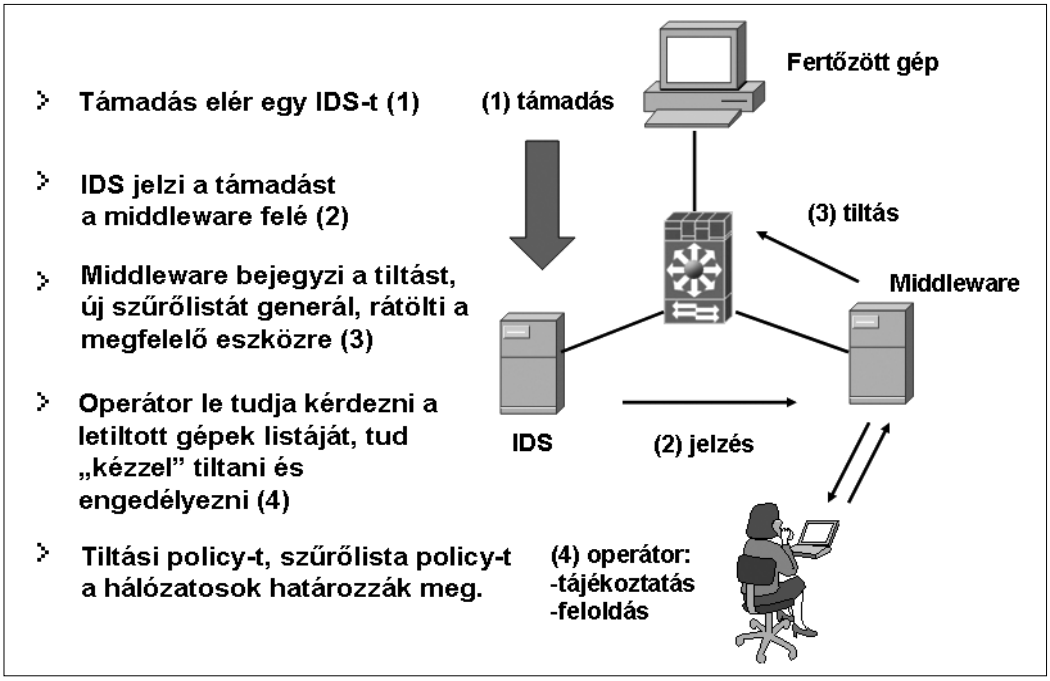
– A felhasználó a végpont bekötési (vagy módosítási) igényét annak jellemző adataival egy web felületen (web form) felviszi a middleware-be. (Vagy papír/fax/e-mail alapú igénylőlapot ad le, ekkor az adatok rögzítését az operátor végzi.)

– A middleware az adatok formai és tartalmi ellenőrzése (például szabad-e az IP cím, létezik-e az igényelt végpont) elkészíti az ügyet, értesíti a szükséges fizikai beavatkozást (pl. patchkábel csatlakoztatást) végző munkatársat.

– Ha a technikus (a fizikai módosítások elvégzése után) lezárja az ügyet, a middleware elvégzi a DNS módosítást, a kiszolgáló port VLAN-ba helyezését, az esetleges DHCP bejegyzést, a router/firewall szűrőlista módosítást (hogy az új gép az intézményen kívülre is tudjon forgalmazni). Az adatbázis a név, IP cím, végpont új állapotát és kapcsolati adatait tartalmazza.

– Természetesen ismerjük a várakozó és a teljesített ügyek számát.

DNS vagy VPN igénylés esetén fizikai beavatkozásra nincs is szükség, a 3. lépés pusztán a folyamat lefutásának engedélyezéséből áll.



1. ábra

Fertőzött felhasználói gép szűrése hálózati middleware-en keresztül

2. példa: Hálózati incidenskezelés

– A hálózat egy komponensét támadás éri egy fertőzött gépről. Erről tájékoztathatja a middleware-t maga a támadott komponens, de egy IDS vagy egy logfile elemző alkalmazás is.

– A middleware a saját topológiai képe alapján megállapítja a beavatkozási pontot (router szűrőlista, firewall szűrőlista), elkészíti az új szűrőlista szabályokat és rátölti a megfelelő eszközre.

– A letiltott gépek listája és az indokok lekérdezhetők (publikus web felületen is).

– A támadó gép „fertőtlenítése" után az operátorok a kezelői felületen feloldják a korlátozást, a middleware ismét engedélyezi a gép forgalmazását.

3. példa: Eszközgazdálkodás

– Eszközvásárlás esetén a szállítólevél alapján megtörténik az eszköz felvitele a middeware adatbázisába. Az eszköz raktárba kerül.

– Miután a technikus kiviszi az eszközt helyszínre és beszereli, könyveli a middeware kábelkönyvi moduljában, hogy mely rackszekrény melyik pozíciójába került, milyen konfigurációban (milyen kártyákkal, modulokkal) és milyen kábeles kapcsolatokkal rendelkezik.

– A lekérdező felületek pontosan informálnak arról, hogy milyen típusú eszközből mennyivel rendelkezünk és azok hol vannak. Hogyan épülnek fel a rackszekrények, milyen eszköznek milyen másikkal van fizikai kapcsolata.

Természetesen a berendezés adatok származhatnak egy raktári rendszerből is, az aktuális fizikai konfiguráció nyilvántartására azonban az alkalmatlan, mert például azt sem tudja eldönteni, hogy mely kártya mely slot-ba illeszthető be. Ezek a middleware eszköztulajdonság adatbázisával dönthetők csak el.

4. példa: Hálózatfelügyelet

– Gyakori probléma, hogy az installált hálózat- vagy szolgáltatás monitorozó alkalmazást nem látjuk el topológiai információkkal, ezért egy hiba esetén sok riasztást kapunk, amiből egy a valódi hiba, a többi annak következtében fellépő másodlagos jelenség, amire a mérnök nem kíváncsi. Ezek a másodlagos riasztások kiszűrhetők, ha a middleware a monitorozó alkalmazásnak „el tudja magyarázni" a hálózat felépítését.

– Ha felveszünk egy új hálózati tartományt, egy új router interfészt, akkor milyen komfortos, ha ezeket mindjárt a monitorozó, terhelésmérő alkalmazás (pl. MRTG) is megismeri.

– A middleware-ben a módosítások tematikusan és időrendben visszakereshetők. Nem kell tehát hosszan vallatni a kollégákat, ha pár napig nem vettünk részt az operatív hálózatkonfigurálási munkában.

Fenti példák jól illusztrálják a hálózati middleware rendszerek közös tulajdonságát, a nagyfokú flexibilitást, nyitottságot, a többi rendszerrel való kommunikációs hajlamot.

6. A piac jelenlegi állapota

Ha hálózati middleware-t szeretnénk vásárolni, nehéz helyzetben vagyunk! A jelenleg kapható programrendszerek főbb kategóriái:

– Vannak olyan programrendszerek, amik a teljes funkcionalitást biztosítják. Ezek azonban komplex informatikai irányítási rendszerek, amik megvásárlása, bevezetése, az informatikai szegmens működésének „átszabása" komoly terhet jelent. Kisebb cégek esetében nehéz ehhez forrást és motivációt találni. Ezek a rendszerek általában tartalmazzák a kapcsolati komponenseket (törzsadattár, kábelkönyv, ügykezelő, hálózatmonitor és felderítő komponensek stb.) A rendszer zárt, a kapcsolati felület más rendszerekkel license köteles (ha létezik egyáltalán). Itt tehát nem middleware alkalmazásról van szó, hanem olyan zárt világról, ami megpróbálja maga megoldani a felmerülő feladatokat.

– Vannak kisebb programok, amik a fenti funkcionalitás egy részét biztosítják és megfizethetőek a kisebb ügyfeleknek is. Bevezetést, pilótavizsgás specialistát nem igényelnek. Ezek azonban általában jól működő hálózatmonitorozó, hálózatfelderítő programokból alakultak ki, a tapasztalat szerint az adatbázis és az alkalmazás-logika zárt, az alkalmazás tervezésekor egyáltalán nem volt szempont a sokoldalú kapcsolódási lehetőség. Ne hagyjuk magunkat áltatni: kis kozmetikázással és színes marketingmunkával ezekből sem lesz middleware.

– Most jelennek meg a piacon az igazi hálózati middleware-ek első generációi. Ezen rendszerek adatbázisait, alkalmazás-logikáját, kapcsolati felületeit a fent vázolt céloknak megfelelően tervezték, és alapkövetelmény az egyedi igények (ügyfél modulok) támogatása is dokumentált interfészeken keresztül. Itt fontos szempont a gyártófüggetlen támogatás. Ha egy hálózatmonitorozó alkalmazást a beleépített néhány middleware funkcióval együtt „komplex hálózatmenedzsment rendszerként" adnak el nekünk, akkor valószínűleg keresztet vethetünk arra, hogy más gyártótól származó vagy saját fejlesztésű rendszereinket elegáns módon ezzel összekapcsoljuk. Amennyiben egy gyártó hálózatmonitorozó, beavatkozó rendszere nem választható el a middleware komponenstől (nem installálható és használható külön az egyik vagy a másik) akkor az valójában nem is middleware alapú megoldás, csupán felszínes mutáció az aktuális marketingszlogenek meglovagolására.

7. Összefoglalás

A jelenleg elérhető hálózati middleware rendszerek még csak szárnyaikat bontogatják. Installálásuk, feltöltésük az induló adatokkal még nehézkes, csak kevés adatbáziskezelőhöz, hálózati entitás-típushoz tartalmaznak kész kapcsolati modulokat. Megéri azonban kipróbálni őket és figyelemmel kísérni lendületes fejlődésüket, mert az univerzálisnak szánt, de zárt rendszereket sok területen hamarosan fel fogják váltani.

Köztéka – Könyvtári és adatfeldolgozó program kistérségek részére

SIMON ANDRÁS

MTA SZTAKI ITAK
andras.simon3@uni-corvinus.hu

Kulcsszavak: könyvtár, könyvtárgépesítés, Internet, katalógus

A könyvtárak közötti együttműködés mára általánosan elterjedt gyakorlattá vált. Különösen fontos megoldani, hogy a földrajzilag egymástól elkülönülő, de szervezeti, gyűjtőköri, vagy szakmai szempontokból összetartozó könyvtárak hálózatban együtt tudjanak működni, a szolgáltatások, a szervezeti működés, az adatfeldolgozás, és a gyarapítás terén is. Fontos hogy az egy térséget képviselő adott esetben hasonló vagy éppen különböző feladatokat ellátó illetve gyűjtőkörű könyvtárak esetében ez az integrált könyvtári alkalmazással is támogatva legyen. Az MTA SZTAKI által kifejlesztett és forgalmazott Kistéka könyvtári rendszeren alapuló Köztéka alkalmazás erre kínál megoldásokat a különféle szakmai, fenntartói, vagy területi alapon szerveződött könyvtári hálózatoknak, különös tekintettel a Kistérségi társulásokban részt vevő községek közművelődési könyvtáraira, és azok honlap, webes kereső és portál szolgáltatásaira.

1. Bevezetés

A könyvtári számítógépes rendszerek tervezése során, különösen akkor, ha újonnan kifejlesztett alkalmazásról van szó, nem elég a meglévő igényeket számba venni, és azok kielégítésére modelleket állítani fel, hanem a könyvtári világban a közeljövőben várható igényeket is fel kell tudni mérni, át kell tudni tekinteni, sőt a számítástechnikai, szoftverfejlesztési eszközök és majdani lehetőségek ismeretében ezen igényeknek éppen irányt is tudni kell szabni, felmutatva a jövő alkalmazási területeit a könyvtáros közvéleménynek. Ilyen, tulajdonképpen a könyvtárgépesítés új eszközei és lehetőségei és a könyvtár automatizálási rendszerek tervezői és fejlesztői által nyújtott lehetőségek kapcsán előállt elvárás a könyvtárak közötti időtől és tértől független együttműködési modellek alkalmazása [1].

2. Együttműködés – új igények, új lehetőségek

Az egyes különféle szakmai földrajzi, vagy igazgatási szempontból összetartozó könyvtárak közötti együttműködés mára nemcsak általánosan elterjedt gyakorlattá vált, de egyenesen követelmény szintre is emelkedett. Egyre fontosabb megoldani, hogy a földrajzilag egymástól elkülönülő, de szervezeti, gyűjtőköri, valamint szakmai szempontokból összetartozó könyvtárak hálózatban is együtt tudjanak működni, a szolgáltatások, a szervezeti működés, az adatfeldolgozás, és a gyarapítás terén egyaránt. Az ezzel kapcsolatos szakmai és szervezési feladatok mellett a könyvtár automatizálási alkalmazásoknak is megoldásokat kell kínálniuk ezekre a feladatokra.

A szakmai elvárásokon túl egyébként éppen a könyvtári szoftverek nyújtotta egyre szélesebb lehetőségek is ösztönzően hatottak a könyvtári együttműködési tevékenységre, itt is, mint a modern társadalomban annyi más alkalommal, a kínálati oldal teremtette meg, építette fel a keresleti oldalon az igények tekintélyes részét. A könyvtári együttműködés és annak technikai támogatása mindamellett természetesen nem öncél, hanem elsősorban a felhasználók igényeinek jobb és gyorsabb kielégítését szolgálja.

Fontos tehát, hogy az egy térséget képviselő illetve adott esetben hasonló vagy éppen különböző feladatokat ellátó illetve gyűjtőkörű könyvtárak esetében ez az együttműködés integrált könyvtári alkalmazással is messzemenően támogatva legyen.

3. Együttműködési modellek

Az együttműködésnek számos szintje van:

- Közös keresőfelület felkínálása
- Bibliográfiai rekordok beszerzése egymástól
- A szerzeményezés és apasztás összehangolása
- Közös besorolási adatállományok, elsősorban közös tárgyszó és szerzői adatbázis építése
- Közös alkalmazás használata önálló adatbázissal
- Közös adatbázis használata
- Közös adatbázis használata mozgó helyszínekről (könyvtárbuszokból)

A szakmai tapasztalatok azt mutatják, hogy a közös adatbázis használati modell csak akkor működőképes, ha a könyvtárak irányítása és a könyvtári munka egy központban összpontosul. Ellenkező esetben a különféle szempontokat jóformán lehetetlen lesz egyeztetni, és közös összehangolt irányítás hiányába az együttműködés kudarcra van ítélve.

A közös keresőfelületeket számos alkalmazás kínálja fel, emellett a közös keresőfelület birtokában megfe-

lelő munkaszervezési döntések meghozása után a szerzeményezési és apasztási munkát is össze lehet hangolni. Ami a bibliográfiai és besorolási rekordok egymástól való átvételét illeti, itt az az általános tapasztalat, hogy a rekordok mozgása általában egyirányú, ráadásul döntően nem horizontális, hanem vertikális pályán mozog, tehát az azonos rangú és jellegű könyvtárak nem egymástól, hanem a náluk magasabb szinten álló könyvtáraktól veszik át a rekordokat, ahol a könyvtári munkaerő inkább rendelkezésre áll, ezért az egyes rekordokat elkészítésük gyorsasága és magas szakmai színvonala, miatt érdemes átvenni. Ezért az egymástól való rekord átvétel könyvtári hálózatok esetében csak akkor intenzív, ha az illető könyvtárak gyűjtőköre nagyon hasonló, és munkaerő és szakmai tekintély szempontjából valamelyik könyvtár a többi számára értékes adatforrásul szolgál.

A bibliográfiai rekordok cseréje mellett a besorolási rekordok átvétele is inkább felülről lefelé halad, ezért a közös besorolási állományok építése helyett a nagyobb könyvtáraktól való besorolási rekord átvétel a célravezető megoldás. Igény esetén ennek technikai támogatását – a besorolási rekordok letöltési lehetőségének biztosítását az adó, és betöltésének lehetőségének biztosítását a fogadó oldalról – kell megadni.

Úgy gondoljuk tehát, hogy a könyvtárak szakmai és anyagi érdekeit az szolgálja leginkább, ha olyan alkalmazást készítünk, mellyel lehetővé tesszük, hogy hálózatban együttműködő könyvtárak azt közösen, de mégis külön-külön adatbázisokat építve használhassák, egymástól és a fölöttük lévő könyvtáraktól bibliográfiai illetve besorolási rekordokat átvéve, illetve a könyvtárosaiknak és olvasóiknak közös lekérdező, kereső felületet felkínálva. Így legalább részben mentesülnek az alkalmazás telepítésének, üzemeltetésének, és a megfelelő körülményeknek a biztosításának terheitől, mégis élvezve a saját külön bejáratú rendszer előnyeit.

4. Pénzügyi és szervezeti lehetőségek, technikai megoldások

Különösen fontos itt, hogy a közös alkalmazást a fenntartó egyszerre valamennyi érintett könyvtár számára megvásárolhassa, illetve a valamilyen módon együttműködő könyvtárak azt kedvezőbben szerezhessék be. A rendszer egy kiszemelt szerveren futhat. Mivel együttműködésről van szó, mód van egy nagy kapacitású számítógép beszerzésére, és a megfelelő szakmai színvonalú és kielégítő biztonságot nyújtó rendszerfelügyelet biztosítására. Adott esetben a szerver nem is feltétlenül van az alkalmazást használó könyvtárak, vagy fenntartójuk birtokában, ráadásul a forgalmazó saját központi gépén is képes ilyen szolgáltatás biztosítására.

Az MTA SZTAKI által kifejlesztett és forgalmazott Kistéka könyvtári rendszeren alapuló Köztéka alkalmazás erre kínál megoldásokat a különféle szakmai, fenntartói, vagy területi alapon szerveződött könyvtári hálózatoknak, különös tekintettel a Kistérségi társulásokban részt vevő községek közművelődési könyvtáraira, és azok honlap, webes kereső és portál szolgáltatásaira.

Egyrészt igény esetén egy az ügyfél által kijelölt gépre képes telepíteni egy Köztéka alkalmazást, ahol az ügyfél által kívánt könyvtárak adatbázisai építhetők, másrészt maga is kínál Köztéka alkalmazásokat nagy teljesítményű hardver eszközeire, szervereire, és hálózati rendszerére telepítve és magas szintű szakmai felügyelettel ellátva azokat.

5. A Köztéka rendszer bemutatása

A Köztéka a már évek óta forgalmazott Kistéka könyvtári rendszer olyan változata, ahol egy alkalmazás több adatbázist is képes kezelni, melyek adott esetben több szerveren külön-külön is helyet foglalhatnak.

5.1. Keresőfelület

Az alkalmazás rendelkezik közös lekérdező felülettel, melyet az olvasók és a könyvtárosok webes felületen az interneten keresztül elérhetnek, és azonosítás nélkül használhatnak. Mind az olvasó, mind a könyvtáros az együttműködésben résztvevő könyvtárak tetszőleges körét, így adott esetben kizárólag a saját könyvtárát kiválasztva folytathat keresést, illetve elérheti kizárólag a saját könyvtárának keresőfelületét is. A sikeres keresést követően megnézheti az illető példányok lelőhely adatait, a részt vevő könyvtár elérhetőségét, és adott esetben a megtalált dokumentumra vonatkozó igénylést, előjegyzési, félretételi, vagy könyvtárközi kölcsönzési kérést küldhet saját könyvtárába, magát mint olvasót olvasójegy számával és e-mail-címével azonosítva. Amennyiben a keresés előtt csak a hozzá földrajzilag közel eső könyvtárakat választotta ki, természetesen személyesen is elmehet az illető könyvtárba, ahol a dokumentumot megtalálta [2].

A könyvtáros, amennyiben úgy dönt, letilthatja megjelenését az együttműködés közös keresőfelületén. Ekkor rekordjai, és adatbázisa csak a saját közvetlen keresőfelületen érhetők el.

A WEB alapú OPAC modul lehetővé teszi a megszokott keresési eljárások, (csonkolás, maszkolás, kombinált keresés, Boole operátorok, különféle adatelemek böngészése) alkalmazását és a találatok többféle megjelenítését.

5.2. Feldolgozói felület

Minden könyvtáros saját feldolgozói felülettel rendelkezik, jelszóval azonosítva lép be, és módosítási, törlési stb. jogokkal kizárólag saját adatbázisában rendelkezik. Módja van viszont a résztvevő más könyvtáraktól közvetlen átvételi technikával rekordokat cserélni. A rekordcserét mások számára engedélyezheti, vagy letilthatja.

A feldolgozói felület egyéb tekintetben maradéktalanul egyezik az MTA SZTAKI által forgalmazott Kistéka legújabb verziójával. A könyvtár bibliográfiai állománya

mellett az olvasói nyilvántartása is el van különítve. Az együttműködésben résztvevő könyvtárakba az illető olvasóknak külön-külön be kell iratkozniuk [3].

Az adatcsere a fentebb említett okok miatt döntően adatátvételt jelent, és a nagyobb könyvtári adatbázisokból, idegen könyvtár gépesítési alkalmazások által támogatott keresőfelületekről való letöltéssel történik. Ezt a munkát a Köztéka támogatja mind a bibliográfiai, mind pedig a besorolási rekordok esetében, MARC illetve Z3950 formátumokban. Emellett lehetőség van szabványos kézi adatbevitelre is, mind a bibliográfiai, mind a besorolási, példány és olvasói adatok esetében is.

A katalogizáló modul lehetővé teszi könyvek, vagy bármilyen más dokumentumtípus bevitelét. A legfontosabb adatok (szerzők, nyelvek, kiadók, tárgyszavak) ellenőrzött háttérállományba kerülnek és a későbbi címleírások elkészítéséhez felhasználhatók. A katalógus szerkezete a HUNMARC szabvány előírásait követi. A beépített import funkció felgyorsíthatja a katalogizálási munkát: a Köztéka fogadni tudja a KELLÓ vagy a Magyar Nemzeti Bibliográfia rekordjait, az esetlegesen már meglévő rendszer (pld. ISIS) rekordjai egyszerűen és gyorsan áttölthetők.

A Köztékával katalogizálhatók elektronikus dokumentumok is, a tényleges dokumentumok a rekordhoz kapcsolhatók. Az elektronikus dokumentum az olvasói OPAC felületen közvetlen linkkel elérhető és megjeleníthető. A katalogizálási munkafolyamatok tervezésekor figyelembe vettük az érvényes magyar szabványokat és előírásokat. A rekordok a bevitel egyszerűsége mellett is teljes mértékben szabványosak és megfeleltethetők más rendszerek rekordjainak.

6. Gyakorlati alkalmazások

A Köztéka forgalmazása során örömmel tapasztaljuk az óriási érdeklődést már a termék bevezetésének első hónapjaiban is.

6.1. Kitelepített Köztéka

A Szatmári Római Katolikus Püspökség számos könyvtárat üzemeltet, saját püspökségi könyvtárát, melyben a történelem viharait átvészelt jelentős múzeális állomány is található, illetve az általa fenntartott oktatási intézmények könyvtárait. Ezeket célszerű hálózatba kötnie, és közös felületet felkínálnia, mely a püspökség többnemzetiségű volta miatt négy nyelvű (magyar, német, román, angol). A szerver a püspökségen van, ezt érik el a többi könyvtárból, így a helyi katolikus iskola könyvtárából, de például Nagykárolyból, az ottani katolikus iskolából is. Webes alkalmazás lévén kliensek telepítésére nincs szükség, mind a kereső, mind a feltáró felület bármely hálózatba kötött munkaállomásról könnyen elérhető.

6.2. A SZTAKI központi gépén elérhető Köztéka

Az MTA SZTAKI nagyteljesítményű szervereinek egyikén több Köztéka alkalmazást is üzemeltet. Egy ilyet például a magyar orvosi könyvtárak számára. A hasonló gyűjtőkörű, és hasonló beszerzési politikát folytató könyvtárak könyvtárosai és olvasói számára igen érdekes az adott esetben közösen használható lekérdező felület, emellett a könyvtárosok a jó hálózati lehetőségeket és a szerver hatalmas kapacitását kihasználva kényelmesen használják rendszerüket, nem törődve azzal, hogy az adatbázis nem náluk található. Nincs gondjuk így az üzemeltetésre, a mentésre, nem kell segítséget kérniük, az amúgy általában igen elfoglalt kórházi rendszergazdáktól, és nehézségeiken a forgalmazó is könnyen tud segíteni, mert adatbázisukhoz közvetlenül is hozzáfér.

Szükség esetén az adatbázisok, mely természetesen a könyvtárak tulajdonát képezi, szabványos formában a megrendelően átadhatók.

7. Összefoglalás

A korunkban igen divatos könyvtári együttműködések, különösen a kistérségi könyvtári együttműködések számára igen jó gépesítési megoldást jelent tehát a Köztéka használatba vétele.

Lehetőséget kínál a könyvtárosnak hogy tértől és időtől függetlenül és más könyvtárak munkatársaival együttműködve használja saját rendszerét, az olvasóknak pedig keresési lehetőséget nyújt szélesebb könyvtári összefogások által felépített adatbázis csoportokban is. Olyan alkalmazást kínál a könyvtári világnak, mely a könyvtári szolgáltatásokat a modern internetes környezetben is elérhetővé és a különféle korszerű adat és tartalomszolgáltatók által nyújtott eszközökkel versenyképessé teszi.

Irodalom

[1] Lengyel Monika:
„Rendszerváltás” a hazai könyvtárakban –
divathullám vagy kényszer?,
TMT 2003 50/8.

[2] Koltay Tibor:
Információs kultúra:
múló divat, vagy alapvető készségek együttese?,
Networkshop 2006, Miskolc.

[3] Fejős László:
Kistéka: lehet, hogy az év kiskönyvtári programja?,
Könyvtári Levelezőlap, 2002 december.

eleMEK –
Metaadat-kezelő és szolgáltató digitális gyűjteményekhez

PERLAKI ATTILA

perlaki@kvtlinux.lib.uni-miskolc.hu

Kulcsszavak: metaadat, digitális dokumentum, XML, platformfüggetlen, Java, GNU GPL, WWW

Az „eleMEK" a digitális dokumentum-gyűjtemények platformfüggetlen, Java- és webalapú moduláris metaadat-kezelő eszköze. Kifejlesztésének alapötlete a Magyar Elektronikus Könyvtár (MEK) digitális dokumentumainak kezelési tapasztalataira alapozva született meg. A mindennapi használat problémái, a helyi nem kompatibilis, nem szakszerű, hiányos és elérhetetlen metaadatokkal szembesülve döntöttek a fejlesztők egy metaadat-szerkezet és annak kezelőjének kifejlesztéséről, a helyi gyűjtemények kezelői számára. Emiatt az „eleMEK" használata és módosítása is engedélyezett a GNU GPL alapján. A cikk a kifejlesztés néhány döntését és az eszköz jelenlegi állapotát ismerteti. Reményeink szerint ezzel új felhasználók és fejlesztők csatlakozhatnak.

1. Bevezetés

A metaadatok az egyre növekvő információhalmazban való eligazodásunkat segítik, a kategorizálást, a keresést teszik könnyebbé. Ezek a könyvtárakban váltak tudománnyá, s alakultak ki igen összetett adatstruktúrákká, ám a mindennapi életben is számos esetben alkalmazzuk őket egyszerűbb formáikban. Ahogy azonban egyre több az információ, a megszokott leírók szegényessé, használhatatlanná válnak. Az eleMEK egy hazai fejlesztésű segédeszköz digitális gyűjtemények metaadatainak kezelésére, erre alapuló rendszerek fejlesztéséhez.

A cikkben az eleMEK rövid bemutatására kerül sor az alkalmazás során leggyakrabban felmerülő kérdések alapján, melyek több általános metaadat-kezelési témát is érintenek. A kérdések és válaszok a probléma ismertetésétől a cél meghatározásán és az eszköz kifejlesztését érintő főbb döntések okain át a használatig vezetnek, nem csak a lehetséges felhasználók, hanem a továbbfejlesztés iránt érdeklődők figyelmére is számítva. Az eleMEK ugyanis nem csak szabadon hozzáférhető segédeszköz, de a GPL alapján módosítható is.

2. Metaadat-kezelés

2.1. Miért segédeszköz?

Az eleMEK nem szokásos szoftvercsomag abban az értelemben, hogy feltelepíti a felhasználó és használja, mint egy „fekete dobozt". Hasznosabb úgy tekinteni rá, mint egy szabadon továbbfejleszthető szoftvereszköz-készletre, amelyből nem szükséges minden elemet felhasználni, amit pedig felhasználunk, azt saját rendszerünkbe, szolgáltatásunkba építjük bele, hasznos „elemként". A neve is erre a gondolatra vezethető vissza.

2.2. Miért van rá szükség?

Metaadat az is, amit egy operációs rendszer gépünkön őrzött állományainkról szolgáltat, ha listázási parancsot adunk ki. Operációs rendszertől függnek a részletek, de általában legalább két szintről kapunk információt:

– Megtudjuk, hogy melyik meghajtón, könyvtárban (directory, folder) vagyunk, ennek mi a neve, elérési útja, mekkora helyet foglal és esetleg azt is, mikor hoztuk létre.
– Megtudjuk a benne tárolt állományok neveit, méretüket, létrehozási dátumait, jogosultságait, esetleg egy kisebb képi ikont is – vagy közvetlenül, vagy egy-két kattintás után.

A lényeg tehát, hogy nem magát az adatot, hanem az adatról szóló adatokat kaptuk meg (az operációs rendszerek eddigi fejlődési sajátosságai miatt meglehetősen korlátozottakat). Ez alkalmas korlátozott keresésekre (például keresem a 2004-es adóbevallásom tábláit), kategorizálásra (kiválogatom azokat a fotókat, amiket télen készítettem), de általában csak emberi segítséggel megy, automatikusan nem.

Ennek az oka az, hogy a szükséges további metaadatok jó részét a fejünkben tároljuk még mindig (például tudom, hogy a digitális fényképezőgépem DSC betűhármassal kezdődő állományneveket állít elő, tehát a sok kép közül valószínű, bár nem biztos, hogy ezek általam készítettek). Alaposan elgondolkodva bizonyára előnyösebb lenne, ha nem nekünk kellene megjegyezni hogy egy-egy állománynév, állománytípus, vagy egy-egy könyvtár mit is azonosít, hanem tetszőleges, vagy legalábbis a mainál sokkal bővebb leírásokkal láthatnánk el anyagainkat.

Ha az állománynév nem mond semmit, ma csak az egyenkénti „belenézegetés" marad lehetőségnek. Ami pedig több tízezer állománynál már reménytelen feladatnak tűnik. Több százmillió gép gépenként több tízezer nyilvánosságnak szánt adatánál biztosan az.

A több tízezer állomány a legutóbbi évekig olyan mennyiség volt, ami még kisvállalatokat sem mindig fenyegetett. Egy magánszemély csak gyűjtőként szembesült a katalogizálás problémáival. Egy (vállalati) kiskönyvtár néhány száz kötetével is „fejből” elboldogulhatott a sok év rutinjával rendelkező könyvtáros. Ennek azonban már vége, egyetlen digitális fényképezőgép is több száz fotót tud egy kártyán tárolni, amit másodpercek alatt lehet „átönteni” a számítógépre, majd onnan akár az internetre. Visszafelé pár nagyságrenddel még több állomány kerülhet a gépre. A „hova is tettem azt a képet, szöveget?” kérdés egyre nehezebben megválaszolható.

2.3. Mi az ismert megoldás?

A könyvtárak már jóval a digitális gyűjtemények kora előtt ismerték és használták a metaadatokat, ha nem is éppen így hívták őket. Ha rátekintünk egy katalógus cédulára, azon a legfontosabb információkat általában hamarabb megtaláljuk, mintsem a polcok közti bolyongással – már amennyiben egyáltalán kint van a könyv és nem raktárban. Megtudjuk a szerzőt és a pontos címet, a kiadót, a kiadás dátumát, néhány azonosítókódot, a témakört, néhány kulcsszót és a könyv megtalálását segítő információt. Ha publikációt keresünk, általában annak rövid összefoglaló leírását is olvashatjuk, mely segít dönteni, valóban ezt keressük-e? Ráadásul a katalóguscédula csak az egyik, tulajdonképpen a legegyszerűbb és legszegényebb metaadat a könyvtárak által használtak közül.

Talán érthető, hogy amikor a digitális gyűjtemények metaadat-kezelésének problémáját megoldani kívánták, elsősorban a könyvtárak tapasztalataira építettek, ám ennek mutatkozott néhány árnyoldala is.

Az egyik, hogy a könyvtáraknál kialakult összetett leírási szabályok egyrészt túl bonyolultak voltak más irányú felhasználáshoz, másrészt sok esetben nem voltak megfelelően illeszthetők az adott problémákhoz. Alkalmas szabvány nem lévén a helyi jellegű megoldások szaporodtak el, és az ezek közti adatcsere gazdaságosan gyakorlatilag kivitelezhetetlen volt. Hozzájárult még ehhez, hogy míg a könyvtárakban szakképzett személyek végezték a leírásokat, addig a digitális gyűjteményeknél elemi hibákkal és hiányosságokkal terhelt metaadat-bázisok születtek.

Ezenközben pedig a digitális tartalmak (nem csak könyvek!) robbanásszerűen szaporodnak, s sajnos vesznek el a digitális kásahegyben, hiába a félelmetesen jónak tűnő és adatbányászati eszközöket is bevető webes keresők egyre elképesztőbb teljesítményei.

2.4. Nincs túl késő?

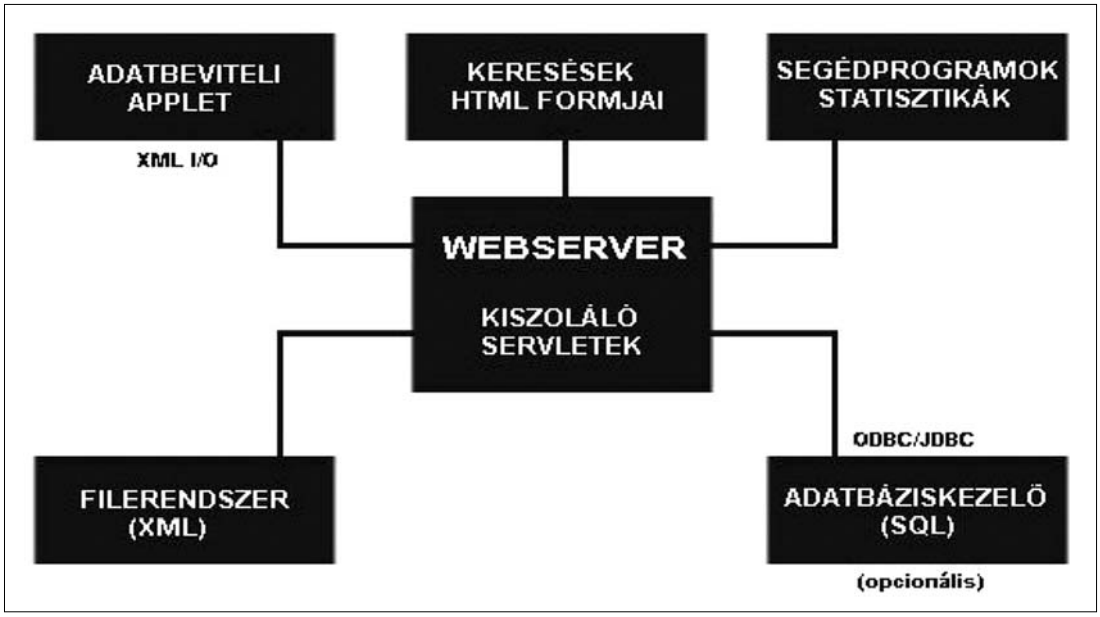
Be kell ismerni, hogy általában véve is az interneten elkésettnek látszik a metaadat-kezelés szabványosított bevezetése. Túl sok leíratlan digitális dokumentum került már fel, melyek közt legfeljebb a teljes szövegű keresőkkel van valami remény megtalálni a keresett információt, rendezettségről szó sincs. Az internet hőskorában még léteztek elképzelhetetlen munkaigénnyel létrehozott tematikus katalógusok, ezeket azonban, ha csak nem speciális célúak, az adattömeg szó szerint maga alá temette.

Márpedig az a dokumentum, ami nincs meg, gyakorlatilag nem is létezik, hiába készült el.

3. Szoftver

3.1. Miért indult el az eleMEK fejlesztése?

Az utólagos katalogizálás az erre váró anyag mennyiségétől függően vagy felesleges erőfeszítésnek tűnik (mert kevés az anyag, „úgy is tudom, mi hol van”), vagy reménytelennek (“ki fog tizenkétezer képet átnézni és egyenként leírni?”). Mégis, valami ilyesmire (és egy kis további rendszeres pluszmunkára) szeretné az eleMEK rávenni az érdeklődőket, cserébe sok felhasználónak sok-sok idejét megtakarítva a kereséskor. Valamint esélyt nyújt arra, hogy a keresés eredménnyel járjon.



1. ábra

Az eleMEK webszerver köré épülő eszközei

A Magyar Elektronikus Könyvtár (MEK) 1994 óta gyűjti a tapasztalatot a digitális gyűjtemények kezelésében és szolgáltatásában. Itt merült fel a gondolat, hogy a nagy központi szolgáltatás mellett egy felhasználóknál üzemeltethető eszköz is kerüljön megvalósításra. Az egyik fontos cél az, hogy az egymással nem kompatíbilis helyi, sokszor ötletszerűen összeállított, különféle formátumokban és rendszerekben tárolt metaadatok „közös nevezőre" legyenek hozhatók, amely nélkül gyakorlatilag nem lehet információt cserélni, keresni.

Az eleMEK legfontosabb alkotó eleme ezért nem valamiféle program, hanem maga az adatszerkezet, amelyhez, mintegy „szerszámosládaként" csatlakozik a programcsomag.

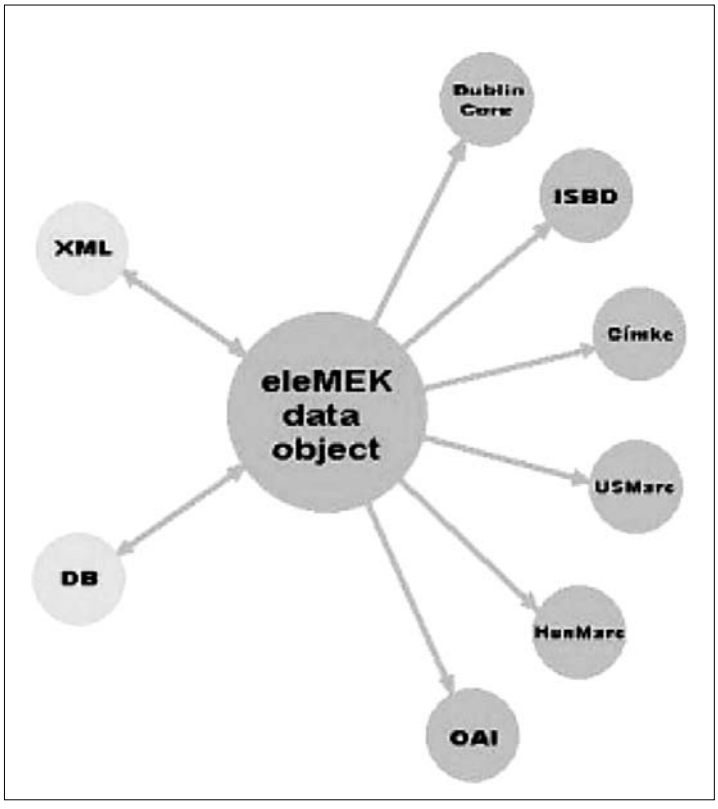
3.2. Mit találunk a szerszámosládában?

Az eleMEK szoftvereszközei *(1. ábra)* a felhasználó szemszögéből a következő részekre bonthatók:

– adatrögzítés és módosítás,
– keresők, listázók,
– import, export és archiváló eszközök,
– ellenőrző, karbantartó és statisztikai eszközök.

A keresők kivételével, amelyek webes felület alá tartoznak, az eszközök lényegében a metaadatokat reprezentáló XML állományok (és igény szerint adatbázistáblák) kezelésére szolgálnak, beleértve a statisztikák készítését is. Az egész csomag felépítése annak figyelembevételével készült, hogy minden eleme igény szerint helyettesíthető legyen, az adatok akár egy szövegszerkesztővel is olvashatók, módosíthatók legyenek.

2. ábra Az eleMEK belső és külső adattípusai



3.3. Miért XML?

Az XML szabványú adatrögzítés ma már egyfajta elvárás, amelyet komoly általános célú és ingyenesen is hozzáférhető szoftverek támogatnak, ugyanakkor mentes a korábbi szigorúan kötött szabványos formátumok korlátaitól és az egyedileg megalkotott nem szabványos formátumok hozzáférhetőségét akadályozó tényezőktől. Megköveteli, hogy a célnak megfelelő „nyelvtant" definiáljuk és hozzáférhetővé tegyük, ugyanakkor szerkezeti megkötései alig vannak. Ez különösen szoftver-objektumok tárolásakor hasznos, amelyek összetettségüknél fogva például relációs adatbázis-kezelőkbe nehezen képezhetők le.

Az eleMEK adatszerkezete kétszintű, mindkét szintjén elhagyható és kötelező részekkel, melyek egyediek és ismételhetők is lehetnek. Ez áttekinthető és XML-ben jól megvalósítható. Figyelemmel az eddig felmerült kimeneti formátumokra *(2. ábra)*, a konverziók általában egyszerűek, legfeljebb közepesen bonyolultak, a beépítetteken (pl. DublinCore, USMARC) kívül könnyen írhatók hozzá újabbak, akár valamilyen programozási nyelven (C, Java, PHP), akár az XML konverziók saját eszközével, az XSL-lel. Az eleMEK kódja jelenleg Java.

3.4. Miért Java?

A cél a platformfüggetlenség volt. A legelterjedtebb operációs rendszerekre a Javát futtató környezet, a JRE ingyenesen letölthető, a programnyelv korai éveiben bírált erőforrásigény pedig ma már alapszintű kiépítéssel rendelkező PC-k esetén sem számottevő. A kód az 1.4-es verziójú Java képességeire épül, jelen pillanatban már az 1.5-ös tölthető le, valószínűleg az eleMEK elkövetkezendő kiadásai már ehhez alkalmazkodnak az ebben a verzióban bevezetett számos előnyös nyelvi fejlesztés miatt. Ez persze attól is függ, kik hajlandóak a csomagot fejleszteni. A lehetőség adott, mivel a csomag GNU GPL alapján terjeszthető és módosítható.

3.5. Miért GPL?

A cél a már fentebb is említett információcsere elősegítése, amit egy teljesen szabadon hozzáférhető és továbbfejleszthető nyílt eszközzel célszerű elérni. Az egyetlen összetevő, amit a kompatibilitás fenntartása érdekében az eredeti fejlesztő kézben szeretne tartani, az adatszerkezet.

A GPL tehát annak, aki nem csak használni, de továbbfejleszteni is szeretné a csomagot, lehetővé teszi, hogy a forráskódot megtekinthesse, módosíthassa, s ezt akár terjeszthesse is.

4. Alkalmazás

4.1. Mi kell hozzá?

A csomag feltételez néhány összetevőt a működő operációs rendszeren – és szolgáltatási igény esetén – az élő hálózati kapcsolaton túl is. Ezek a következők:

– Java SDK, legalább 1.4-es verzió, 1.5 ajánlott. Java JRE csupán akkor elegendő, ha csak adatrögzítésre és konverziókra használjuk a csomag érintett részeit.
– Tomcat 4.0, vagy magasabb verziójú webszerver, amely a keresési szolgáltatásokat támogatja, Java Servlet Pages (JSP) kezelésére képes. Már meglevő webszerver mellé is telepíthető és üzemeltethető, ekkor általában a 8080-as porton.
– SQL adatbázis-kezelő, JDBC csatolóval. Ez körülbelül 1000-1500 tételig, tehát kis gyűjteményeknél nem alapkövetelmény, a kereső tisztán állományalapú működésben is viszonylag gyors eddig a határig.

A használatbavételt célszerű úgy megkezdeni, hogy a fent említett komponensek már tesztelve felkerültek. A csomaghoz mellékelt dokumentáció kitér mind a Windows, mind a Linux alapú telepítés menetére, és a Tomcat webszerver alapbeállításain szükséges változtatásokra is.

Két olyan eleme van a csomagnak, ahol a kezelési felület alapvető fontossággal bírt. Az egyik az adatbeviteli eszköz, a másik a keresés.

4.2. Mennyire felhasználóbarát?

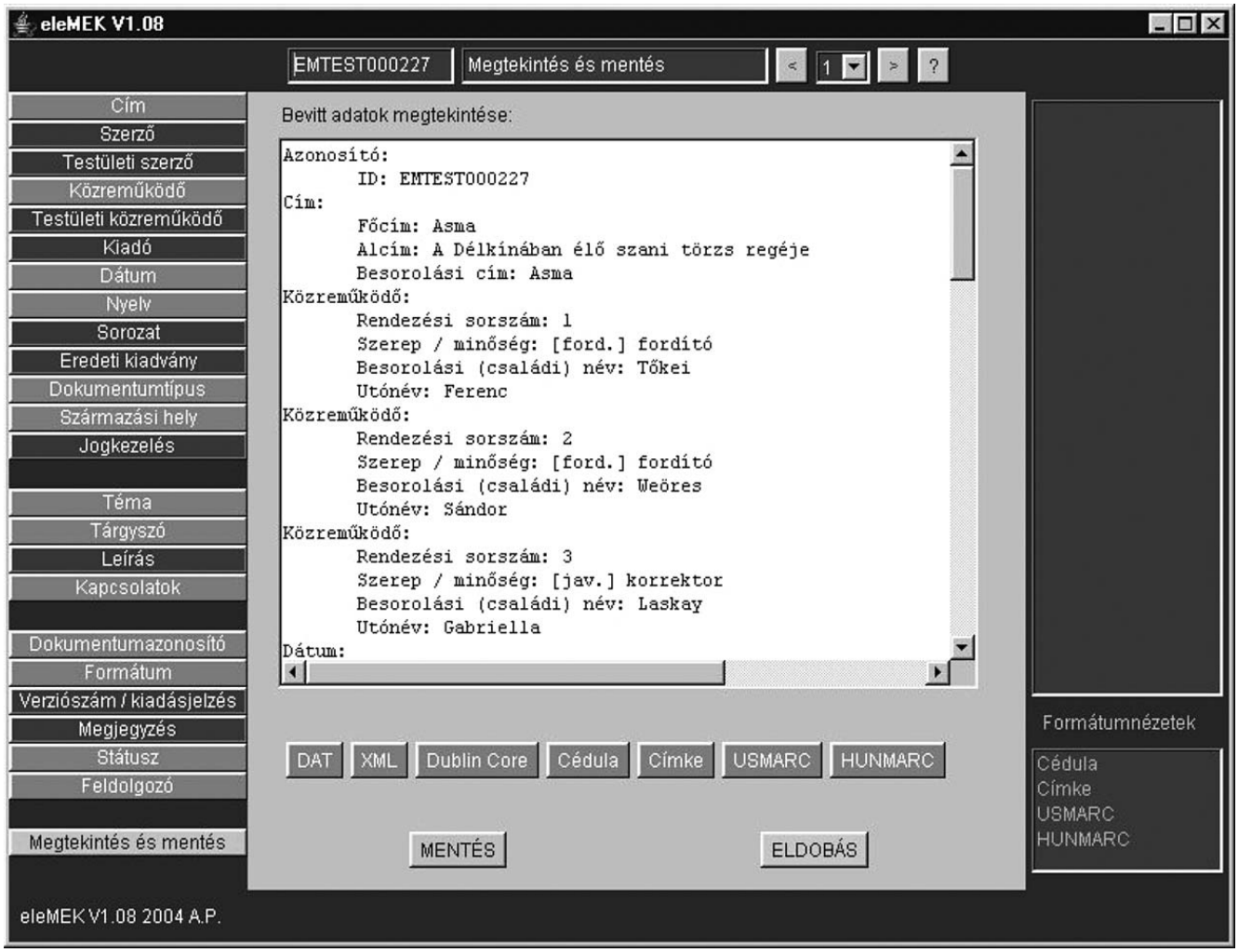
Az adatbevitelt egy Java applikáció végzi *(3. és 4. ábra)*, amit szükség esetén appletként is el lehet indítani, amennyiben a felvitelt egy központi gépről kívánjuk felügyelni. Ez egyben azt is jelenti, hogy a program grafikus környezetet igényel, Linux alatt karakteres terminál üzemmódban nem működik.

A feladata lényegében a metaadatok felvitele és a szükséges XML állomány előállítása, első közelítésben egy „felokosított” XML szerkesztő célprogram, azonban a beleépített tudás és az adatstruktúra összetettsége viszonylag bonyolult kódot eredményezett.

A felviteli folyamat egyszerű: ki kell keresni egy már létező metaadatot (ami akár importálással is a rendszerbe kerülhetett) és azt kell szerkeszteni, vagy újat kell létrehozni. Az adatfelvitel lapokra osztva történik, a néhány kötelező adat felvitele és rögzítése után bármikor megszakítható és később folytatható. A felvitel során bármikor a „nézet lapra” lehet kapcsolni és a felvitt adatokat többféle formátumban ellenőrizni.

A program több adatmezőt „listás”, illetve „indexes” meghatározással kezel, ami azt jelenti, hogy ezekhez a beviteli felületen (jobb oldalt) értéklisták kérhetők és a bevitel csupán választás és kattintás. A különbség,

3. ábra
Az eleMEK adatbevitelének „Megtekintés és mentés” képernyője



hogy a „listás” mezők csak választhatók, ezek értékeit csak az eleMEK adatait karbantartó „adminisztrátor” módosíthatja közvetlen javítással, vagy a mellékelt adminisztrátori eszközzel, míg az indexek a bevitel során automatikusan bővülnek, például új szerzői családnevekkel. Ugyanitt található még egy kicsiny ablak, ahonnan az aktuális adatlaphoz ajánlott tezauruszok hívhatók meg, on-line.

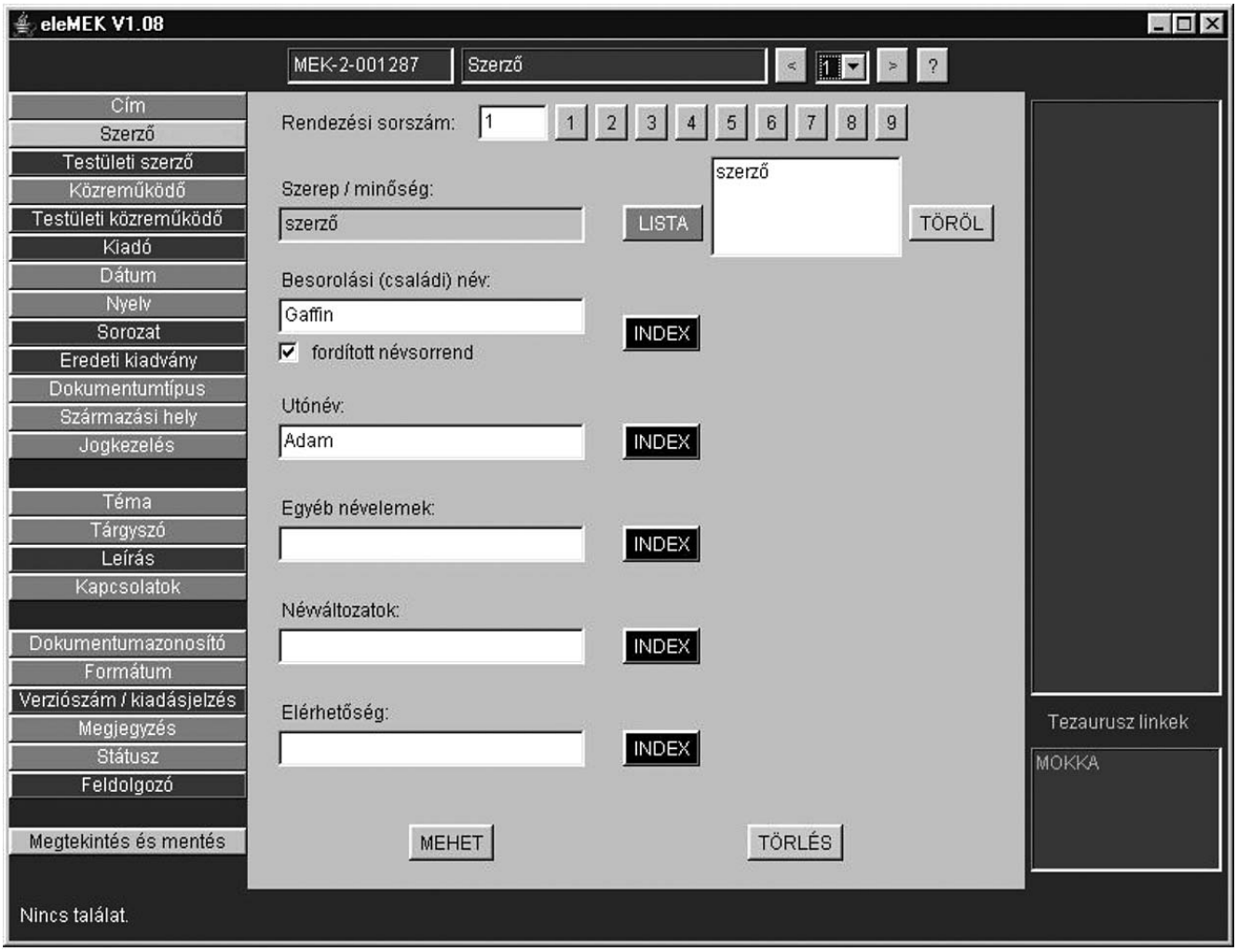
Ehhez a programhoz külön súgó tartozik (3. és 4. ábra, felső sor, kérdőjel), amelyet egy szakkönyvtáros állított össze, természetesen a csomagban ez is megtalálható. Ez azt jelenti, hogy a használatot mindenképpen tanulni és gyakorolni kell, ha a felhasználó pontos, jól kezelhető, szakszerű adatokat kíván rögzíteni.

A másik komponens, amelynél fontos a kommunikáció a felhasználóval, s aki ez esetben a szolgáltatást igénybevevő és nem az adatokat rögzítő, a keresés. Ez alapvetően más környezetben és megfontolások alapján került megvalósításra. Mindössze két webes „kérdőív”, illetve az eredménylisták alkotják a látható felületet, melyet az alkalmazó a maga képére alakíthat, s ezért gyakorlatilag a csomagban ennek a résznek a megjelenése alaphelyzetben purián. A két kérdőív egy úgynevezett gyorskeresést és egy olvasói, bővebben beállítható, paraméterezhető keresést (5. ábra) tartalmaz. Az eredményül kapott listán megjelenő adatok gyűjteményenként konfigurálhatók, tilthatók, vagy engedélyezhetők, illetve maga a keresés erre a listára még szűkíthető. Ennek a résznek a testre szabása tehát inkább weblap-készítői tapasztalatokat igényel.

4.3. Hogyan tovább?

Amíg olyan operációs rendszer nem kerül a kezünk alá, amely egyenesen megköveteli a mainál részletesebb metaadatok használatát, addig segédeszközökre szorulunk. Az ígéretek persze már évek óta elhangzanak, de messze vagyunk a hétköznapi, elterjedt használattól. Az eleMEK ebből a szempontból hiánypótló. Sajnos a tavalyi évben a fejlesztés hátterét biztosító NIIF forráshiány miatt kénytelen volt szüneteltetni a támogatást, a tervek és a még el nem készült kiegészítések „fiókban hevernek”. Ezek közül a periodikákat, dokumentum-csomagokat is kezelni képes, metaadatokat hierarchikus módon kezelő kiegészítés és az offline eleMEK emelhetők ki, utóbbi alkalmazható például CD-n kiadott digitális gyűjtemény elemeinek keresőrendszereként.

4. ábra
Az eleMEK adatbevitelének „Szerző” képernyője



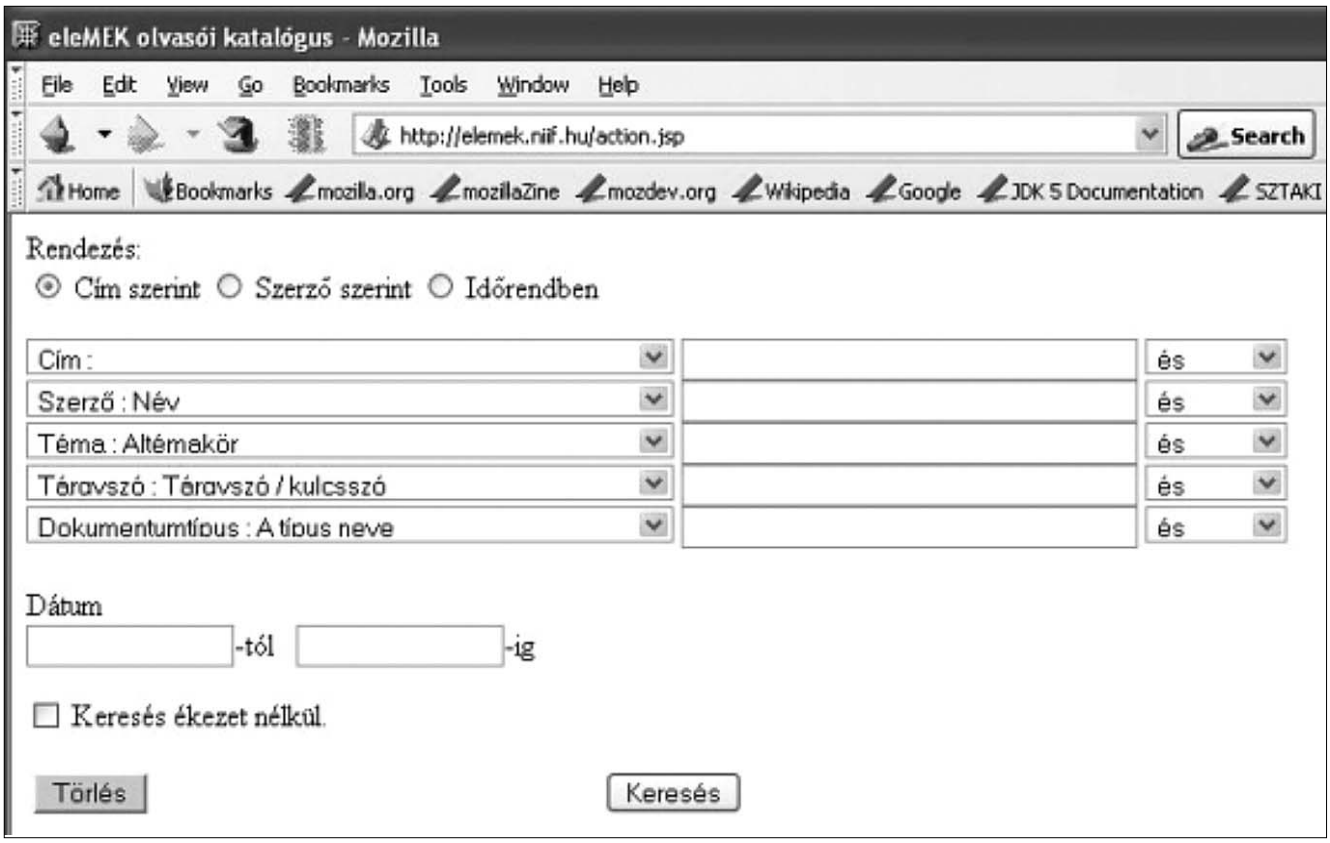
5. Összefoglalás

A digitális gyűjtemények metaadatainak kezelésére szolgáló eleMEK közkincs, egy nyílt eszköz-csomag, amit használni és fejleszteni lehet. Célját, hogy a metaadatokat könnyen kicserélhető, könnyen értelmezhető, szabványoknak megfelelő formában tárolja és szolgáltassa, mai formájában is teljesíti. Elterjedéséhez azonban nagyobb ismertség szükséges és annak felismerése, hogy sem az átlagos felhasználó számára megfizethetetlen és kihasználhatatlan nagy rendszerek, sem az egyéni ötleteken alapuló zárt fejlesztések nem alkalmasak a digitális tárolt tartalmak hatékony megtalálására, rendszerezésére.

Irodalom

[1] Drótos László:
eleMEK – Metaadat-kezelő rendszer digitális gyűjteményekhez,
TMT 2005/2
http://elemek.oszk.hu/ismertetok/elemek-cikk.htm
[2] Drótos László, Perlaki Attila:
Moduláris könyvtári rendszer elektronikus dokumentumgyűjtemények kezeléséhez: az eleMEK projekt,
Networkshop, Győr, 2004. április
http://elemek.oszk.hu/ismertetok/netwshp2004.htm
[3] Drótos László, Perlaki Attila:
eleMEK rendszerterv,
NIIF weblap (2004-től folyamatosan aktualizált)
http://elemek.niif.hu/rendszerterv/index.html
[4] Drótos László, Góczán Andrea:
eleMEK kitöltési útmutató,
NIIF weblap (2004-től folyamatosan aktualizált)
http://elemek.niif.hu/help/index.html

5. ábra Az eleMEK webalapú keresőjének „olvasói keresés" kérdőíve



Hálózatkihasználási kihívások a csillagászatban

HOLL ANDRÁS, SRÁGLI ATTILA

MTA Konkoly Thege Miklós Csillagászati Kutatóintézete
{holl, sragli}@konkoly.hu

Kulcsszavak: csillagászat, Internet

Az alábbiakban áttekintjük a hálózathasználat csillagászati gyakorlatát és lehetőségeit, nemzetközi kitekintéssel. Megvizsgáljuk a hazai helyzetet, azon belül is az MTA Konkoly Thege Miklós Csillagászati Kutatóintézete (CsKI) előtt álló kihívásokat. A csillagászat mint tiszta alapkutatás, valamint széles érdeklődést kiváltó tudomány, kiváló terepet jelent technológiák kipróbálására, műszaki-tudományos képzésre és ismeretterjesztésre. Több csillagászati alkalmazás is a figyelem középpontjába került az utóbbi években. Ezeken túl bemutatjuk a hazai csillagászati kutatás hálózathasználati lehetőségeit.

1. Kitekintés

A csillagászatnak erős nemzetközi kapcsolatrendszere van. Tiszta alapkutatásról lévén szó, a megfigyelési adatok hamar nyilvánosak lesznek: az égbolt minden nemzet kutatói számára hozzáférhető, ugyanakkor viszont a jelenségek folyamatos követése, illetve a teljes égbolt lefedése érdekében nemzetközi együttműködés szükséges. Az Internet hatalmas jelentőséggel bír az asztronómia művelői számára. Ez megmutatkozott az RFC 1017-ben is, ami a tudományos kutatás hálózati igényeit vette számba 1987-ben.

A csillagászat egyik nagy kihívást jelentő területe a hálózathasználatban az e-VLBI (Very Large Baseline Interferometry: nagy bázistávolságú rádió-interferometria). A VLBI mérésekhez egymástól minél távolabb (ha lehet, több ezer kilométeres távolságra) lévő rádióteleszkópokra van szükség. Az egyidejűleg végzett megfigyelések adatait korábban – atomórák időjeleivel együtt – mágnesszalagra vették, a szalagokat a kiértékelés helyére szállították, majd egy korrelátor segítségével összejátszották. A szalagok szállítása miatt az eredmények csak hetekkel a megfigyelés után születtek meg. Az e-VLBI esetében az adatok hálózati szállítása miatt az eredmények rögtön kiértékelhetők. Az Internet2 csillagászati bemutató alkalmazása 2004-ben egy e-VLBI kísérlet volt, amikor az Egyesült Államok, az Egyesült Királyság, Svédország, Hollandia és Lengyelország obszervatóriumait kötötték össze, helyszínenként 32 Mbit/s sávszélességgel. A brit rádiótávcsöveket összekötő e-Merlin hálózatot 150 Gbit/s folyamatos terhelésre építették ki, ugyancsak 2004-ben. Az e-VLBI ma 1 Gbit/s-os adatátvitel 24 órán keresztül való fenntartását igényli a hollandiai JIVE központtal, amit a GEANT hálózat biztosít európai rádióteleszkópok számára. A jövőre nézve az igények még merészebbek: 4-10 Gbit/s átviteli sebességekre lehet szükség.

Ugyancsak kihívást jelent a távoli helyeken (magas hegycsúcsokon, vagy éppen a világűrben) lévő obszervatóriumok hálózati összeköttetése. A Gemini Obszervatórium két megfigyelőhelyének (Hawaiiban és Chilében) 2002-ben 155 Mbit/s, illetve 77 Mbit/s sebességű kapcsolata volt az Internethez. A tervezett James Webb Space Telescope 600 GB-nyi adatot fog egy nap alatt termelni, amit tömörítve, egy 5.35 GB/nap kapacitású X-sávú rádiókapcsolaton kell majd a Földre lehozni – ez persze nem az Internet forgalmát növeli majd. Ám ezeket az adatokat a világ különböző részein dolgozó kutatókhoz hálózaton kell majd a Space Telescope Science Institute-ból eljuttatni! Nem a JWST lesz a legnagyobb adatforrás: a közeljövőben a Large Synoptic Survey Telescope egyetlen nap alatt 13 TB-nyi megfigyelési adatot „ont” majd.

A csillagászat és a rokon területek, mint az űrkutatás vagy az idegen intelligenciák keresése a világűrben igen népszerűek, jól használhatók a fizikai tudományok, illetve a számítástechnika népszerűsítésére. A népszerűség és a szabadon hozzáférhető adatok óriási oktatási lehetőséget jelentenek. Nem a SETI@Home volt az első elosztott hálózati számítási projekt, de talán a legismertebb. Ma a Berkeley Open Infrastructure for Network Computing keretében működik tovább. A Mars Pathfinder előre meghirdetett, Interneten közvetített leszállása olyan nagy érdeklődést keltett 1997-ben, hogy a NASA JPL 2 T3-as vonala nem bírta a terhelést.

Milyen ütemben bővül a hálózat sávszélessége, milyen ütemben nőnek az igények? A növekedés a számítástechnikában mindig exponenciális. A megfigyelő csillagászatban a detektorok (CCD-k) méretnövekedése, és persze számuk gyarapodása diktálja a sávszélesség-igényeket, az elméleti modellszámítások által létrehozott adatok mennyisége a processzorok sebességével, a tárolókapacitásokkal nő, növekedhet. A rendelkezésre álló sávszélesség Nielsen szerint kétévente duplázódik meg [1], Edholm és Eslambolchi a Moore-törvény szerinti növekedést állítanak [2]. Tanulságos lenne a csillagászati intézmények számára rendelkezésre álló sávszélesség növekedését megvizsgálni – ezt a CsKI tekintetében a következőkben meg is tesszük majd.

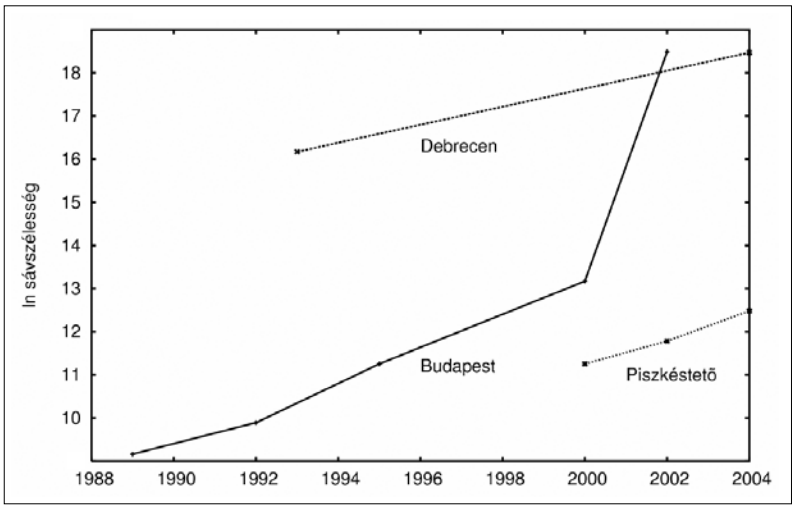
2. A CsKI hálózati kapcsolata

A CsKI-nek négy telephelye van: Budapesten, Debrecenben, Piszkéstetőn és Gyulán. Ezeket a telephelyeket hálózatnak kell összekötnie. Alapelvnek tekintjük, hogy a hálózat hiánya nem lehet a kis vidéki telephelyek üzemeltetésének akadálya, ellenkezőleg, a hálózatnak csökkentenie kell a távolság okozta problémákat, javítania kell a kutatás feltételeit. A hálózat fenntartása nem szabad, hogy teher legyen az intézeti költségvetésen, hanem éppenséggel megtakarítást kell eredményeznie a kommunikációs és utazási költségek terén.

A tudományos kutatás szükségleteinek kielégítése a legfontosabb szempont az Internethez való kapcsolódásban. Az erős nemzetközi kapcsolatrendszert tanúsítja, hogy a CsKI-ban készült tudományos publikációk jelentős részének van külső (sok esetben külföldi) társszerzője. Az Intézet a Wise Obszervatóriummal együttműködve kisméretű robot-távcsövet üzemeltet az izraeli Negev-sivatagban, és a HERSCHEL csillagászati mesterséges hold adatainak fogadására készül. A jelenleg üzemeltetett elektronikus adatbázisok – mint például a Nemzetközi Csillagászati Unió megbízásából kiadott Information Bulletin on Variable Stars nevű elektronikus folyóirat, ami 1994-ben került fel a webre – megkövetelik a biztonságos hálózati összeköttetést.

A CsKI hálózati (WAN) története a budapesti telephely X25-ös kapcsolatával kezdődött (1989), ha nem számítjuk a korábban az Intézethez tartozó Bajai Obszervatórium távoli terminál-kapcsolatát a SzTAKI nagyszámítógépével. A budapesti központ 1992-ben kapcsolódott az Internethez: egy 19.2 kbit/s sebességű bridge kapcsolta össze a KFKI RMKI hálózatával – az RMKI-nek ekkor már a CERN-en keresztül volt Internet-kapcsolata. 1995-ben 64 kbit/s-os bérelt vonal kapcsolta a HUNGARNET-hez az intézeti lokális hálózatot, majd 2000-ben a sávszélesség 512 kbit/s-re bővült. Végül 2002-ben a budapesti, Svábhegyen lévő obszervatórium sötét üvegszálas, Gigabites összeköttetést kapott az NIIF-től. A CsKI telephelyek hálózati összeköttetéseinek történetét az *1. ábra* mutatja be.

1. ábra A CsKI internet-kapcsolat sávszélesség-bővülése



3. A hálózathasználat lehetőségei

A következőkben áttekintjük azokat az új hálózathasználati lehetőségeket, melyek a Csillagászati Kutatóintézet számára a közeljövőben feltárulhatnak.

3.1. Megfigyelési adatok szállítása

B. Pirenne az European Southern Observatory (ESO, Európai Déli Obszervatórium) adattárolási és szállítási szükségleteit ötéves távlatban felmérve állítja, hogy az adatszállítás kívánatos eszköze mára a hálózat lett [3]. (A tárolás esetében a következtetés az, hogy merevlemezegységeken kell az adatokat őrizni.) A CsKI Piszkéstető–Budapest adatszállítási gyakorlata (a CCD kamerák megjelenésétől kezdve) előbb DAT mágneskazettákra, majd kivehető winchester diszkekre, illetve írható CD majd DVD lemezekre épült.

A CsKI jelenlegi adatforgalmi igényei a következőképp foglalhatók össze: Budapest: 2-20 GB/nap; Piszkéstető: 500 MB-15 GB/nap; Debrecen: 1 GB/nap; Gyula: 500 MB/nap. A svábhegyi és az egyetemi kampuszon lévő debreceni telephely üvegszálas kapcsolatai elegendő sávszélességet jelentenek az adatok fogadására. A vidéki obszervatóriumokban viszont nem kielégítő az Internet-kapcsolat sávszélessége. Áttekintve a jellemző megfigyelési programokat, Piszkéstetőn egy derült éjszaka 0.5/15 GB-nyi adat keletkezik, Gyulán a digitalizált Nap-képek mennyisége naponta nem haladja meg az 1 GB-ot. Ahhoz, hogy ezt az adatmennyiséget Budapestre illetve Debrecenbe szállíthassuk, és ez a kisebb sávszélességű oldal hálózati kapcsolatát naponta legfeljebb 2 órányit terhelje, mindkét kis obszervatóriumban legalább 1 Mbit/s (feltöltési) sávszélességre lenne szükség, Piszkéstetőn azonban a legtöbb adatot termelő megfigyelési programok kiszolgálásához néhányszor 10 Mbit/s kellene.

A svábhegyi intézetben a kihívást a HERSCHEL űrszonda adatainak (jelenleg tesztadatok, 2007-től valódi adatok) fogadása jelenti: itt akár 100 GB-os adatcsomagok letöltésére van szükség.

3.2. Távészlelés

A távészlelés alatt azt a lehetőséget értjük, hogy a csillagásznak nem kell a teleszkóp mellett lennie a megfigyelés során, hanem távolról irányíthatja azt. A mérés távvezérlése mellett (vagy helyett) igény lehet a távfelügyeletre, amikor a megfigyelő (például egy egyetemi hallgató) a távcső mellett van, de a mérések menetét egy másik kutató (oktatója) távolról követi, hogy beavatkozhasson, ha probléma adódik.

Létezik egy alacsony sávszélesség igényű változat is: a robotizált teleszkóp automatikus időbeosztó rendszerének csak a megfigyelési program leírását kell eljuttatni. Változócsillagok fotometriai megfigyelésénél nemcsak ez a leírás (mely tartalmazza többek között a megfigyelendő objektumok

listáját, a mérések kért időpontjait, prioritását), de maguk a mérési eredmények sem nagyméretűek. Ez esetben a robottávcső automata időbeosztó rendszerével való kommunikáció történhet e-mailen keresztül.

A szakirodalomban említett első távészlelési kísérletek egyikét S. Maran írta le 1967-ben: az Egyesült Államok-beli Kitt Peak obszervatórium 60 cm-es távcsövének távvezérlését oldották meg, egy modemes kapcsolaton keresztül. Az ESO-ban 1987-től végeztek kísérleteket La Silla-i (Chile) távcsövekkel, 64 kbit/s sávszélességű műholdas bérelt vonalon keresztül.

A modern távészlelés sem igényel nagy sávszélességet: a technológia alapja a vezérlő számítógép(ek) távirányítása, ami történhet X-Windows vagy VNC (Virtual Network Computing) [4] alapon. Az X-Windows esetében is lehetőség van viszonylag lassú vonalak használatára az NX technológia alkalmazásával. A CsKI-ban a svábhegyi távcsővel folyó megfigyelések távfelügyeletéhez a programban részt vevő kutatók otthoni kábelmodemes kapcsolata (~1 Mbit/s) alkalmasnak bizonyult *(2. ábra)*.

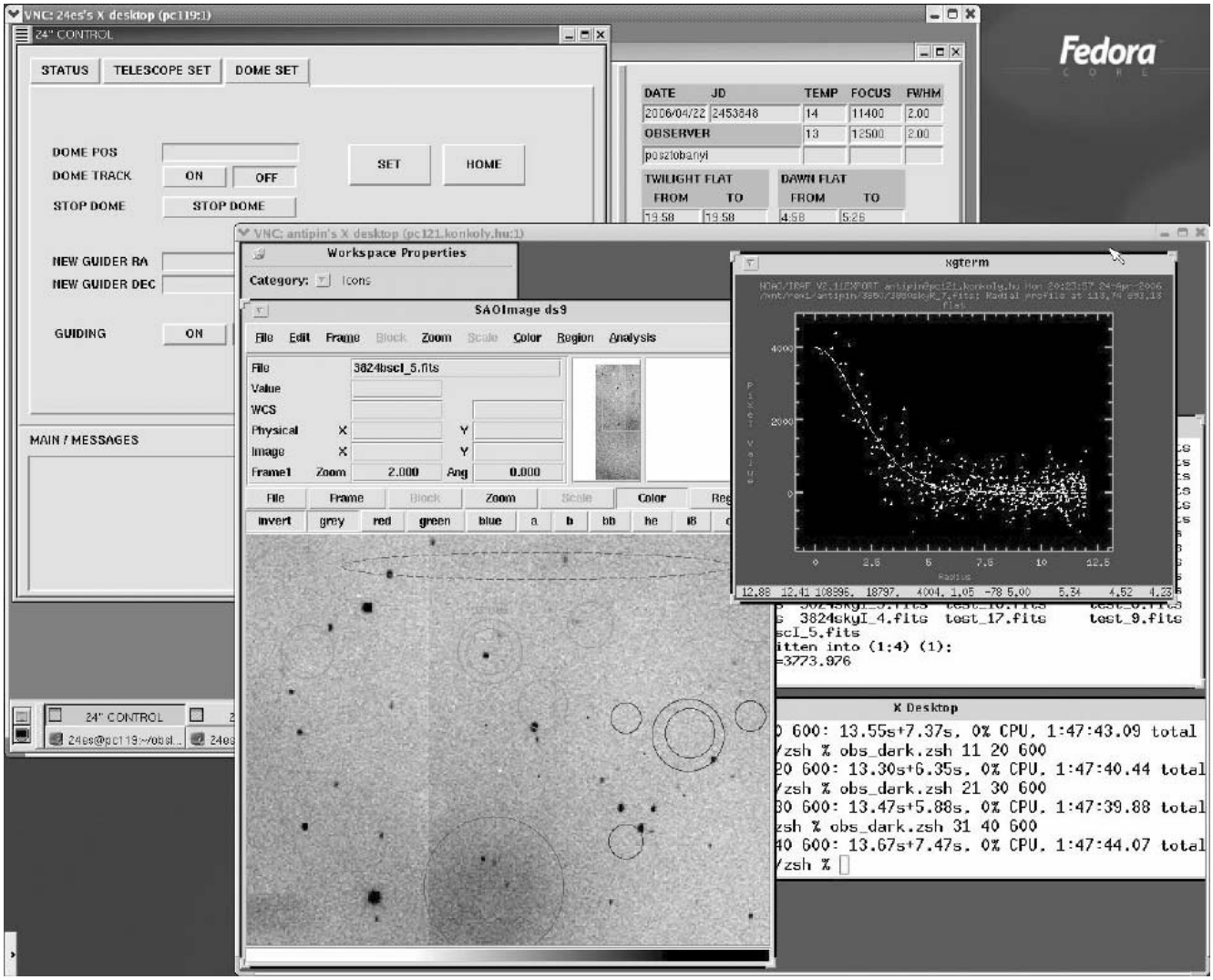
A távészlelés legnagyobb problémája az, hogy a berendezések nem mindig működnek tökéletesen, és hibák, elakadások esetén a vezérlő számítógép képernyője nem ad elég információt. (Az amperszag nem vihető át TCP/IP protokollok segítségével!) Ezért alkalmazzák a gyakorlatban a technikát inkább csak távfelügyeletre, vagy „közeli" távészlelésre, amikor a megfigyelő csak néhányszor 10 vagy 100 méterre van a teleszkóptól, fűtött helyiségben (esetleg egyszerre több távcsővel dolgozik). Távfelügyelet esetén a megfigyelő és a felügyelő között hangkapcsolat is van – de ez egyszerűen megoldható telefon segítségével is.

Az információhiány csökkentésére kísérleteket tervezünk webkamera alkalmazására. Itt problémát jelent az a tény, hogy a piszkéstetői, illetve svábhegyi megfigyelések sötétben zajlanak, és a jelenlegi webkamerák érzékenysége nem megfelelő. Hiba esetén a megfigyelés azonban megszakítható, a kupola megvilágítható.

3.3. Vagyonbiztonsági távfelügyelet

További lehetséges alkalmazás webkamerák alkalmazása biztonsági, vagyonvédelmi célokra. A távcsövek elhelyezésére szolgáló kupolákban sokszor nincs állandó személyzet, s többnyire elhagyatott helyeken állnak. A svábhegyi 60 cm-es távcső kupolájába több

2. ábra Így látja a távészlelést végző csillagász a távcsővezérlő és az adatfeldolgozó PC-k képernyőit



betörés történt már. Ezért adódik az informatikai hálózat, és esetleg akár a távészlelésnél használt kamerák biztonsági felhasználásának lehetősége.

Ahogy az előző pontban említettük, a megfigyelni kívánt helyiségekben a megvilágítás erőssége tipikusan 1 lux alatti (általában csupán néhány tized lux), és a jelenleg kereskedelmi forgalomban kapható webkamerák érzékenysége pedig a ~0.5-30 lux tartományban mozog, így ezek a kamerák e célra nem felelnek meg. Alkalmazhatók viszont a biztonsági kamerák, melyek egy része UTP csatlakozóval és beépített webszerverrel is rendelkezik.

Az általuk generált hálózati forgalom a kamera felbontásától (0.2-0.4 megapixel), a képfrissítési sebességtől (10-25 frame/s) és az alkalmazott tömörítési eljárástól (általában JPEG) függően változik, azonban – főként több kamera telepítése esetén – jelentős lehet (egy kamera használható képfelbontás és -frissítés mellett min. ~64 kbit/s sávszélességet foglal le).

3.4. Adatok tükrözése távoli helyszínre

Minthogy az adattárolás leginkább költséghatékony megoldása egyre inkább az adatok merevlemezen való tárolása, és a CsKI telephelyei közül a svábhegyi intézetnek és a Debreceni Napfizikai Obszervatóriumnak van nagy sávszélességű (üvegszálas) kapcsolata, felmerül az adatok biztonsági mentésének lehetősége a telephelyek között. Az adatbázisok tükrözése a rendelkezésre állási biztonságot növeli.

Az adatbázis-tükrözés sávszélesség-igénye erősen függ az alkalmazott technikától (időszakos, inkrementális mentés, részleges vagy teljes mentés, tranzakció alapú replika). E módszerek – a teljes mentés kivételével – használata esetén a sávszélesség-igény az adatok változásának, az adatbázis bővülésének mértékével arányos. Adatbázis-tükrözés jelenleg is történik a svábhegyi intézet és a KFKI között a PhysHun projekt keretében, az adatbázis mérete jelenleg kb. 100 MB.

Létezik egy technika a csillagászatban, ami lehetővé teszi az adatbázisok távoli *fail-over* redundanciájának megteremtését: ez a Strasbourg-i CDS csillagászati adatközpontban kifejlesztett GLU [5]. A technológia lényege, hogy a dinamikus weboldalakon az elosztott GLU rendszer segítségével képződnek az URL-ek. A központi GLU adatbázisba beavatkozva a meghibásodott webszerver adatait át lehet állítani a tartalék helyszín címére.

A hálózat lehetővé teszi a tárolóhely-kapacitások kihasználásának optimalizálását is: például egy több TB-os adattároló egység pillanatnyilag kihasználatlan kapacitásait a másik telephely igényeinek kielégítésére is fel lehet ajánlani.

3.5. Kisigényű telekonferencia, VoIP kommunikáció

Véleményünk szerint a telekonferencia alkalmazásának elterjedéséhez szükséges, hogy az NIIF által jelenleg alkalmazott technológiáknál olcsóbbak álljanak rendelkezésre. A CsKI-ban igény lenne az összintézeti értekezletek telekonferencia alapon való megrendezésére. Célszerű lenne megteremteni az intézet tudományos szemináriumainak, illetve az ELTE Csillagászati Tanszékén megrendezett országos csillagászati szemináriumok telekonferencia jellegű elérhetőségét is.

Ezek a rendezvények, ezek az intézmények nem feleltek meg az NIIF eddigi videokonferencia pályázatainak követelményeinek – olcsóbb megoldásokat kell keresni. Bár mind a svábhegyi, mind a debreceni telephelyen néhány km-es közelségben van NIIF telekonferencia csomópont, ezek használata túlságosan nehézkesnek bizonyult. Nem jó, ha a telekonferenciához utazni kell – lehetővé kell tenni azt a minden előadóteremben, vagy akár a kutatók íróasztalán. Úgy véljük, érdemes lenne kipróbálni olcsóbb technológiákat, amelyekkel kevesebb költséggel lehet az előadótermeket felszerelni, és a konferencia követésére, hallgatói hozzászólásokra pedig akár egy webkamerával felszerelt noteszgépnek is elegendőnek kell lennie.

A CsKI kisebb telephelyeinek VoIP elérésére az NIIF által jelenleg alkalmazott „hardveres” technológiáknál célszerűbbnek tűnik a „szoftveres” megoldások alkalmazása.

Szabad szoftverek széles skálája áll rendelkezésre Internetes telefonálásra (VoIP) illetve videokonferencia megvalósítására. A korábbi GnomeMeeting újabb változata, az Ekiga peer-to-peer kommunikációra (PC-PC, PC-telefon, telefon-PC irányokban), illetve kisebb, néhány fős csoportok számára ajánlott, hang- és videókapcsolatot biztosító, illetve azonnali üzenetküldő szoftver. Funkcionalitását tekintve szinte mindenben megegyezik az ismert Skype-pal, azonban azzal ellentétben szabad szoftver, valamint szabványos protokollokra épül (SIP, H323). Ez megkönnyíti a már létező infrastruktúrába való integrálását is (heterogén hálózatok, tűzfal, NAT).

Az Asterisk kiválóan alkalmazható szoftver intelligens telefonközpont (PBX) és SIP átjáró funkciókkal. Az NIIF VoIP hálózatába integrálva Asterisk szerverek és IP-telefonok jelenthetnek költségtakarékos kommunikációs lehetőséget a CsKI kis obszervatóriumainak.

A fizikai tudományokban külföldön elterjedt az AccessGrid technológia. Az AccessGrid csoportok közti költséghatékony videokonferenciára nyújt megoldást, szintén szabványos technológiák felhasználásával, szabad szoftverkomponensekkel (AccessGrid ToolKit). Multicast alapú kommunikációt használ, így csoportok között egyértelműen hatékonyabb, mint a PC-s VoIP szoftverek, ellenben hardverigénye miatt peer-to-peer vagy néhány résztvevős kapcsolattartásra kevésbé alkalmas.

3.6. Nagy adatbázisok hálózati szolgáltatása

Jelenleg a CsKI-ban a Svábhegyen ~2 GB, Debrecenben ~58 GB adat érhető el on-line. A svábhegyi 2 GB-nyi tárolt adatmennyiséget évente nagyjából 20-50-szer töltik le. A Svábhegyen (zömében analóg formában) fellelhető információs vagyon kb. 6-7 TB, mely évente kb. 1 TB-tal gyarapszik (teljes egészében digitális formában). A debreceni (analóg) információs va-

gyon is kb. 6 TB, az (analóg, de digitalizált) éves gyarapodás körülbelül 0.5 TB. Ezeket az információkat célszerű lenne elektronikus formában közzétenni.

Nehéz megbecsülni, hogy a teljesen digitalizált információmenynyiség mekkora adatforgalmat generálna – érzésünk szerint a teljes adatmennyiség 1-10%-át töltheték le évente. (A Space Telescope Science Institute MAST archívuma esetében egy év alatt nagyjából a tárolt összes adatmennyiséggel megegyező adatot töltenek le. A mi esetünkben ennek csak a töredékével számolunk.)

3.7. A Virtuális Obszervatórium kihívásai és lehetőségei

A csillagászat jelenlegi e-Tudomány projektjét Virtuális Obszervatóriumnak (VO) nevezik. Jellemzője a nagy égboltfelmérések adatbázisainak elérhetővé tétele, a nagy adatmennyiségeket kezelő eljárások, eszközök biztosítása és az ehhez szükséges szabványosítás. A felhasználók részére a VO a hálózati sávszélesség növelése nélkül tudja majd biztosítani nagy adattömegek használatát: az adatok feldolgozása a felhasználótól távol történik, hozzá csak a nagyságrendekkel kisebb méretű eredmények jutnak el, mint azt J. Gray, a Microsoft Research kutatója állítja [6]. Budavári T. nagy elosztott adatbázisok használatára ismertet egy alkalmazást [7].

Amennyiben a CsKI mint szolgáltató is megjelenik a VO-ban, a helyzet megváltozik. Az előző pontban említett nagy adatbázisok VO-keretekbe való integrálása az egyszerűbb, szabványos elérési lehetőségek, az adatok nagyobb láthatósága miatt a VO-n kívüli esethez képest növekedni fog. (A VO-technikák alkalmazása azt is jelenti, hogy a felhasználónak nem is kell tudnia arról, hogy azok az adatok, melyekre szüksége van, például éppen a CsKI-ban találhatóak meg, a VO (a GRID-es alkalmazásokhoz hasonlóan) gondoskodik arról, hogy az adatokat használhassa. Nem kell ismernie az adatok formátumát, nem kell rendelkeznie a feldolgozásukhoz szükséges programokkal – mindezt megoldja a VO.)

Lehetőség van a VO technikák alkalmazására a tudományos ismeretterjesztésben, tudománynépszerűsítésben, középiskolai oktatásban. Az *„outreach”* programok különösen az Egyesült Államokban népszerűek. A lényeg az érdeklődők bevonása tudományos programokba. A *„Hands on Universe”*-hez hasonló hazai program lehetne akár az, hogy a CsKI teleszkópjaival készült, hálózaton hozzáférhetővé tett felvételeken lehetne egyetemistáknak, középiskolásoknak, érdeklődőknek szupernóvákat vagy új változócsillagokat keresniük.

3.8. QoS igények

A csillagászatban a hálózat rendelkezésre állási követelményeit a felhasználók szokásai szabják meg. A kutatók sokat dolgoznak (mint a Sztrugackij fivérek fantasztikus tanmeséje címéből kiderül, „a hétfő szombaton kezdődik”). A mérések sokszor éjszaka folynak, távoli vagy akár űrobszervatóriumokban a nap minden órájában szükség van a hálózatra. A CsKI által szolgáltatott elektronikus szakfolyóirat, az IBVS számaira több külföldi adatbázisokból mutatnak linkek, mely linkeknek élniük kell. A 99,5%-os rendelkezésreállás megkövetelése reális igénynek tűnik.

A hálózattal szemben támasztott technológiai jellegű igényeket támasztó alkalmazások a CsKI-ban a Vo-IP, illetve videokonferencia, külföldi viszonylatban pedig az e-VLBI.

4. Összefoglalás

A csillagászat nagy sávszélességű Internet-kapcsolatokra tart igényt, cserében a társadalomnak népszerű szolgáltatásokat, oktatási lehetőségeket biztosít. Mint bemutattuk, e tudományág hazai művelőinek is vannak tervei a meglévő üvegszálas kapcsolatok kihasználására, és igénylik a kisebb telephelyek hálózati kapcsolatainak fejlesztését.

Irodalom

[1] Nielsen J.,
Processing power is increasing faster than bandwidth,
Alertbox, 1998. április 5.
http://www.useit.com/alertbox/980405.html

[2] Cherry, S.,
Edholm’s law of bandwidth,
IEEE Spectrum, 2004. július, p.58.

[3] Pirenne, B.,
Astronomical data storage and distribution
in the next five years,
ASP Conference Series, 2004., 314. kötet, p.525.

[4] Richardson, T. és szerzőtársai,
Virtual Network Computing,
IEEE Internet Computing, 1998., 2.1., p.33.

[5] Fernique, P., Ochsenbein, F., Wenger, M.,
CDS GLU, a tool for managing heterogeneous
distributed web services,
ASP Conference Series, 1998., 145. kötet, p.466.

[6] Gray, J.,
Computer Technology Forecast for
Virtual Observatories, MSR-TR-2000-102, 2000.

[7] Budavári, T., Szalay, S., Gray, J. és további szerzők,
Open SkyQuery – VO Compliant Dynamic Federation
of Astronomical Archives,
ASP Conference Series, 2004., 314. kötet, p.177.

A cikk Networkshop-os változata, sok URL-el:
http://www.konkoly.hu/staff/holl/miskolc/hollsrag.html

RFC1017 http://www.rfc-archive.org/getrfc.php?rfc=1017
GLU http://simbad.u-strasbg.fr/glu/glu.htx
Ekiga http://www.ekiga.org
AccessGrid http://www.accessgrid.org
Hands on Universe http://www.handsonuniverse.org
BOINC http://boinc.berkeley.edu/

Közösségi erőforrás-megosztás alapú számítási modell alkalmazása a gyakorlatban – SZTAKI Desktop Grid –

KORNAFELD ÁDÁM

MTA-SZTAKI, Párhuzamos és Elosztott Rendszerek Kutatólaboratórium
kadam@sztaki.hu

Lektorált

Kulcsszavak: dc-api, boinc, hierarchikus desktopgrid, közösségi erőforrás-megosztás alapú számítási modell, SZTAKI Desktop Grid

Számításigényes feladatok megoldásához a szuperszámítógépek mellett különböző grid technológiák is sikerrel alkalmazhatóak. Ezen technológiák kifejlesztésének fő célja a költségcsökkentés mellett az volt, hogy bárki felajánlhassa erőforrását a grid számára és bárki felhasználója lehessen a grid erőforrásainak. Ez az elképzelés azonban a mai napig nem valósult meg teljes mértékben. A grid technológiák fejlődése két külön úton indult meg. A clustergrid modellre épülő gridekben bárki hozzáférhet felhasználóként a grid erőforrásaihoz, de erőforrás csak megfelelő szakértelem birtokában ajánlható fel. Ezzel szemben a közösségi erőforrás-felajánláson alapuló számítási modellt alkalmazó gridekhez bárki felajánlhatja erőforrását, de a grid erőforrásait csak az azt felállító intézmény használhatja. Ez utóbbi modell némi módosítással mégis alkalmas lehet a grid technológiák eredeti koncepciójának megvalósítására. Jelen cikk a közösségi erőforrás-felajánláson alapuló számítási modell kiterjesztésének lehetőségét mutatja be a SZTAKI Desktop Griden keresztül.

1. Bevezetés

Napjaink tudományos kutatásai során gyakran merül fel igényként hatalmas mennyiségű információ feldolgozása, mely számítógépek segítsége nélkül szinte elképzelhetetlen. Olykor a rendelkezésre álló idő rövidsége teszi szükségessé minél nagyobb számítási teljesítmény alkalmazását. Remek példa erre az időjárás-előrejelzés, ahol a rendelkezésre álló mérési adatokból még azelőtt kell a jövőre nézve releváns következtetéseket levonni, mielőtt azok idejétmúlttá válnának.

A különböző grid technológiák az ilyen és ehhez hasonló igények kiszolgálását tűzték ki célul. Az eredeti elképzelés – miszerint bárki felajánlhat erőforrást a grid számára, valamint az igényeknek megfelelően bárki dinamikusan igényelhet erőforrást a gridtől – azonban nem valósult meg teljes mértékben. Napjainkban két jellemző irányvonalat figyelhetünk meg a grid technológiák fejlődésében. Az egyik irányvonal a clustergrid modellt alkalmazza, míg a másik elképzelés a Közösségi Erőforrás-felajánláson alapuló számítási modellre épülő desktopgrid architektúrát részesíti előnyben. Cikkünkben a desktopgrid architektúrát, annak kialakulását, a benne rejlő lehetőségeket és egy konkrét megvalósítását mutatjuk be.

2. A desktopgrid kialakulása

Számításigényes feladatok megoldásához kutatók már az 1970-es évek elejétől szuperszámítógépek kifejlesztésében látták a megoldást. A kifejlesztett szuperszámítógépek általában be is váltották a hozzájuk fűzött reményeket teljesítmény szempontjából, azonban mind kifejlesztésük, mind pedig üzemeltetésük rendkívül költségesnek bizonyult. Ennek megfelelően mind a mai napig nem teljesen triviális hozzáférni egy szuperszámítógép erőforrásaihoz. Elsősorban költségcsökkentés céljából felmerült az igény egy olyan architektúra kifejlesztésére, mellyel a nagy méreteket öltő költségek jelentős mértékben csökkenthetők, ugyanakkor a kifejlesztett rendszer számítási kapacitása továbbra is versenyképes marad a szuperszámítógépek körében. Ez az elképzelés vezetett a clustergrid architektúra kifejlesztéséhez.

A cél egy olyan grid szolgáltatás kifejlesztése volt, melyhez sok felhasználó hozzá tud férni. Ezt a grid szolgáltatást erőforrások hálózatba kapcsolásával hozták létre. Ahhoz, hogy egy erőforrás a grid részévé válhasson, egy előre meghatározott programcsomagot, úgynevezett middleware-t kell rá telepíteni. Egy ilyen middleware azonban annyira összetett, bonyolult rendszert alkot, hogy az üzemeltetés komoly szakértelmet igényel. Emiatt természetesen adódott, hogy magánszemélyek nem ajánlanak fel erőforrást, csak nagyobb intézmények (pl. egyetemi tanszékek), ahol egy szakértőkből álló csapat felügyeli a komplex, hardware és software komponensekből álló rendszert, ezáltal garantálva annak nagy rendelkezésre állását. Ilyen grid infrastruktúrákra példa a legnagyobb európai grid, az EGEE (Enabling Grids for E-SciencE [1]), és annak magyar virtuális szervezete a HunGrid. Ezekhez a gridekhez felhasználóként bárki hozzáférhet, aki rendelkezik megfelelő felhasználói tanúsítvánnyal, mely tanúsítványkezelő hatóságoknál igényelhető.

A kialakult clustergrid modell a fentebb tárgyalt okok miatt azonban nem alkalmas annak az igénynek a kiszolgálására, hogy bárki felajánlhassa erőforrását a grid számára. Bár a clustergrid modell alkalmazására összeállt intézmények számottevő erőforrásparkkal rendelkeznek, egyértelmű, hogy még nagyobb számítási teljesítmény összefogására nyílik lehetőségünk, ha le-

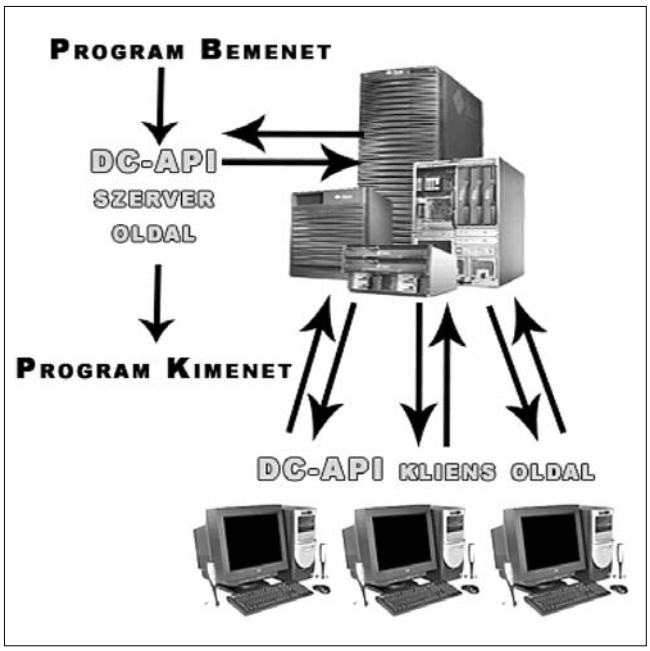
hetővé tesszük, hogy bárki és bármekkora erőforrást felajánlhasson a grid számára. Ez az elképzelés vezetett a Közösségi Erőforrás-felajánláson alapuló számítási modell kialakulásához, melynek sematikus rajza az *1. ábrán* látható.

A modellben a legkisebb építőelem a személyi számítógép (Desktop Computer). Erre utalva kapta a desktopgrid nevet a modellre épülő architektúra.

3. A desktopgrid architektúra

A legismertebb példa, a legelső desktopgrid architektúrájú grid a mind a mai napig futó SETI@Home [2]. A desktopgridek személyi számítógépektől kezdve a legkülönbözőbb erőforrásokat kapcsolnak össze egy központi szerver segítségével, jelentős számítási teljesítményre szert téve ez által. A saját erőforrását donorként felajánló számítógép tulajdonosnak mindössze egyetlen kliens programot kell telepítenie számítógépére, melynek a grid honlapján való rövid regisztrációt követően kapott címet megadva a felajánlott erőforrás máris a desktopgrid szerves részét képezi. A résztvevők számítógépein futó kliens program nem igényel semmilyen felhasználói beavatkozást az adott erőforrás felhasználójától. Ezáltal elértük, hogy bárki hozzájárulhat a grid teljesítményének növeléséhez saját erőforrásának felajánlásával. Ahhoz azonban, hogy sok felajánlott erőforrásra tegyünk szert, szükség van a desktopgrid és elsősorban az azon futatott alkalmazás reklámozására, népszerűsítésére. Emiatt a clustergridekkel ellentétben a desktopgridek nem sok felhasználósak, jellemzően egyetlen programmal egy adott problémára keresik a megoldást. Így általában a desktopgrid rendszert felállító intézmény egyben egyetlen felhasználója is a desktopgridnek.

1. ábra
Közösségi erőforrás-felajánláson alapuló számítási modell



A desktopgrides környezet jellemzően 'mester-szolga' mintán alapuló problémamegoldást jelent. A megoldandó feladatot kis részfeladatokra osztják (például a program bemenetét képező adathalmaz feldarabolásával), melyek egymástól függetlenül, konkurensen végrehajthatóak. A részfeladatokat ezután a desktopgridhez csatlakozó szuverén erőforrások dolgozzák fel. A desktopgrid központi szerverén futó 'mester' program gondoskodik a feladatok szétosztásáról és a 'szolgák' által szolgáltatott részeredmények feldolgozásáról.

A rendszer legnagyobb előnye az egyszerűsége, míg hátránya, hogy csak a 'mester-szolga' paradigmán alapuló programokat tud kiszolgálni. Az architektúra már világszerte bizonyított olyan nagyszabású projektekben, mint a földönkívüli intelligencia nyomait kutató SET@Home, a Föld klímaváltozását kutató Climateprediction@Home, vagy az emberi kórokozókat kutató World Community Grid.

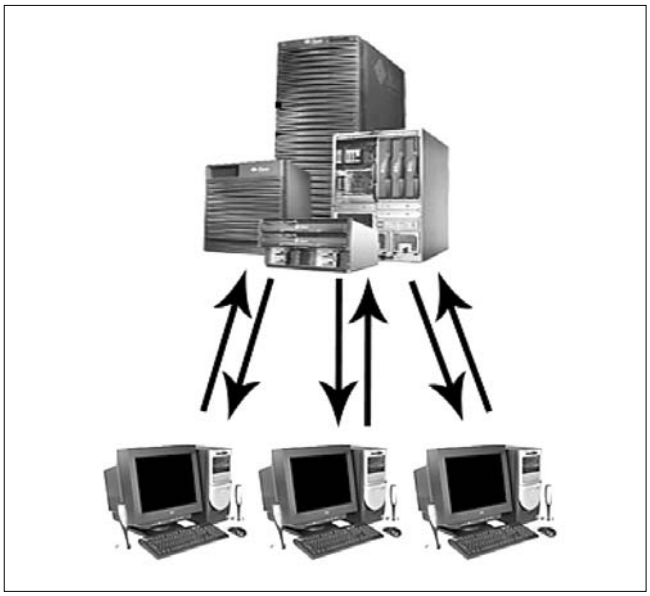
Természetesen a desktopgrid architektúrát eredményesen alkalmazhatjuk kisebb méretekben is. Hasonlóan ahhoz, mint ahogy a személyi számítógép építőeleme a desktopgridnek, egy szinttel feljebb kisebb méretű desktopgridek építőelemei lehetnek egy nagyobb gridnek. Ez egy új koncepció, mellyel közelebb hozhatjuk egymáshoz a grid technológiák két fő irányvonalát, konvergálva ez által a grid technológia eredeti elképzeléséhez. Önálló intézmények könnyűszerrel összekapcsolhatják már meglévő erőforrásparkjukat egy úgynevezett lokális desktopgridbe. A technológia könnyű, felhasználóbarát telepíthetősége miatt a desktopgrid architektúra könnyebben és gyorsabban terjedhet el, mint a robosztusabb architektúrák. Mindemellett, ha lehetővé válik, hogy a lokális desktopgridek megoszthatják egymás között erőforrásaikat a sokkfelhasználós modell előnyei is kihasználhatóak.

Ahhoz, hogy a desktopgridek együttműködhessenek a támogatott architektúrák közé kell emelni a clustereket, meg kell valósítani a desktopgridek többszintű hierarchiáját egy nagy szervezeten belül, valamint az erőforrás-megosztást a különböző desktopgridek között.

4. SZTAKI Desktop Grid

Laborunkban felállított SZTAKI Desktop Grid, önálló desktopgridként, az első építőköve a grid technológiák két nagy trendjének összeházasításában végzett munkánknak. A grid alapját a nyílt forráskódú BOINC (Berkeley Open Infrastructure for Network Computing [3]) platform szolgáltatja. A BOINC platform kifejlesztésével a Berkeley-egyetem kutatói egy olyan nyílt infrastruktúra létrehozását tűzték ki célul, mely alapjául szolgálhat számos olyan nagyszabású tudományos projektnek, melyben személyi számítógépek millióit használják információfeldolgozásra.

A platform két fő részből áll: egy központi szerverből és a hozzá kapcsolódó kliensekből *(2. ábra* – lásd a következő oldalon).



2. ábra A BOINC platform

A szerver komponensekből épül fel, ami lehetővé teszi, hogy az adott komponensek különálló hardveren futtassuk, megfelelő robusztussággal ruházva fel ez által a szervert. Feladata, hogy az adott projekt által szolgáltatott feldolgozandó információt szétdarabolva és adatbázisba rendezve elérhetővé tegye azt a csatlakozó kliensek számára, továbbá a kliensek által feldolgozott és visszaküldött eredményeket hitelesítse és rendszerezze. A számítási kapacitásukat felajánlóknak nincs más dolguk, mint letölteni és telepíteni egy kliens programot számítógépükre.

Attól a ponttól kezdve, hogy az erőforrás felajánlója megadta, hogy milyen beállítások mellett engedélyezi a projekt számára a processzor üres idejének kihasználását, a kliens program teljes mértékben automatizáltan csatlakozva a szerverhez, letölti a projekt által feldolgozandó bemenet egy kis részletét, valamint annak feldolgozásához szükséges programot egy munkacsomag formájában. A program segítségével a kliens megkezdi a kapott bemenet feldolgozását. Amennyiben végzett a feldolgozással, a kapott eredményt visszatölti a szerverre, és újabb munkát kér attól.

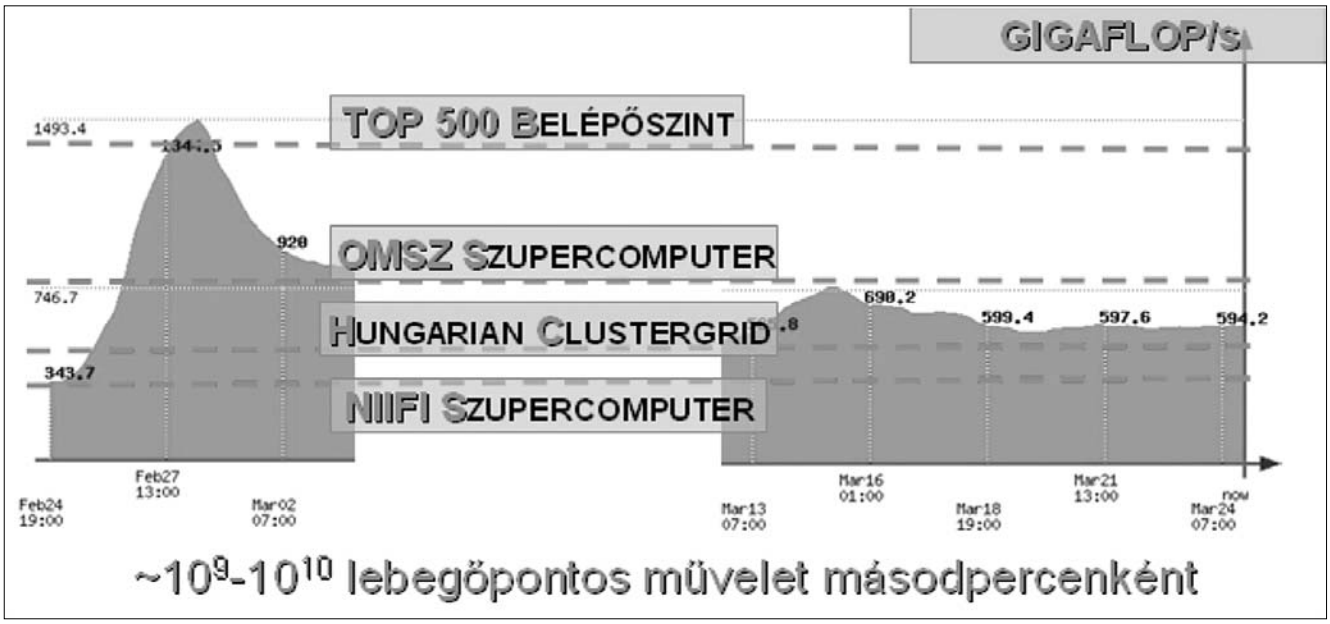
A platformot használó projektek összes teljesítménye 2006. áprilisában mintegy 419 TeraFLOPs [4], mely messze meghaladja a Föld jelenlegi legnagyobb teljesítményű IBM BlueGene/L (280 TeraFLOPs [5]) szuperszámítógép teljesítményét.

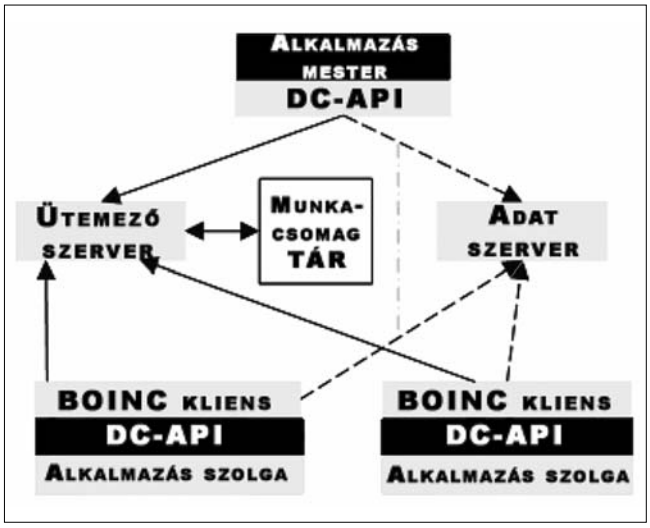
A SZTAKI Desktop Grid [6] globális verziójának felállítása óta eltelt háromnegyed éve az ELTE Komputeralgebra tanszékén futó BinSYS [7,8] projekthez szolgáltat infrastruktúrát. A projekt keretében matematikus kollégáink az összes általánosított bináris számrendszer felkutatását tűzték ki célul. 2005 nyarán, a projekt indulásakor a számrendszereket a 11. dimenzióval bezárólag tűnt reálisnak meghatározni. A 11. dimenzió becsült fél éves feldolgozási ideje a SZTAKI Desktop Grid segítségével 1 hónapra rövidült, továbbá azóta már a 12. dimenzió feldolgozása is megkezdődött. A projektnek jelenleg több mint 7500 résztvevője van, mintegy 18000 számítógéppel. A rendszer által biztosított teljesítmény 700-800 GigaFLOPs *(3. ábra)*, ami majdnem eléri az OMSZ által üzemeltetett leggyorsabb magyar szuperszámítógép teljesítményét, és jelentősen meghaladja az NIIF szuperszámítógépének, valamint cluster gridjének teljesítményét.

A BinSYS projekt szembesített minket azzal, hogy bár a BOINC platform rendelkezik egy programozói API-val, melynek segítségével az alkalmazások felkészíthetőek az elosztott környezetben való futásra, annak használatához elengedhetetlen a BOINC platform átfogó ismerete.

Ez nagymértékben megnehezíti a desktopgrid architektúrára való alkalmazásfejlesztést. Az alkalmazás-

3. ábra SZTAKI Desktop Grid teljesítmény-összehasonlítás





4. ábra Desktop grid infrastruktúra

fejlesztés megkönnyítése érdekében laborunkban kifejlesztettük a DC-API [9] programozói interfészt, melynek feladata elrejteni az alkalmazásfejlesztő elől a BOINC platform sajátosságait. A *4. ábra* a BOINC platformot és a DC-API beépülését szemlélteti.

Az API használata lehetővé teszi, hogy a kutatók saját tudományos kihívásukra koncentráljanak, anélkül hogy a számítási igényeiket kiszolgáló grid infrastruktúrának bármilyen részletével is törődniük kellene.

5. Klaszterek támogatása a SZTAKI Desktop Gridben

A BOINC platform önmagában nem nyújt semmilyen támogatást klaszterek csatlakozására. Mivel a klaszterek 'job management' koncepciója sokkal általánosabb, mint a desktopgridekben alkalmazott részfeladat szétosztás, ezért ez utóbbit át lehet ruházni az előbbire. A BOINC infrastruktúra klaszterekkel való kiterjesztésének öt lehetséges módja van.

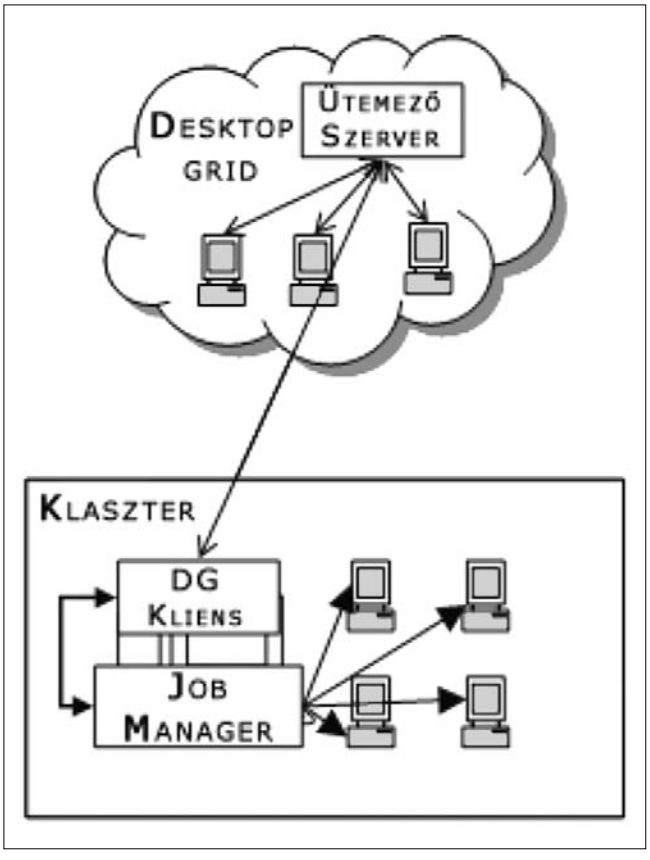
1) A klaszter valamennyi számítógépére telepítjük a BOINC kliens programot, így a klaszter összes erőforrása önállóan csatlakozik a desktopgridhez.
2) Egy teljes desktopgrid telepítésre kerül a klaszterre. A desktopgrid szerver feladatát a klaszter frontend gép látja el. Ez lehetővé teszi a klaszter hierarchikus desktopgridhez való csatlakozását. Erről bővebben a 6. fejezetben szólunk.
3) Egy független magas szintű borker segítségével osztjuk szét a munkát klaszerek és desktopgridek között.
4) A desktopgrid szerver klaszter jelenléte esetén munkacsomagok helyett 'job'-okat küld a klaszternek.
5) A desktopgrid kliens módosított változata kerül telepítésre a klaszter frontend számítógépére, mely a hagyományos desktopgrid munkacsomagokat 'job'-okká alakítja, majd beküldi őket feldolgozásra a klaszterba.

Az első két megoldás hátránya, hogy megkerülik a klaszter 'job manager'-ét, ezért alkalmazásuk nem javasolt. Ennek ellenére, amennyiben a desktopgridek hierarchiába szervezésének lehetősége életre kel, a második megoldás szóba jöhet, mint egy ingyenes lehetőségként klaszterek hierarchikus desktopgridhez való csatolásakor.

A harmadik megoldás hátránya, hogy egy teljesen új brókert kell kifejleszteni hozzá, bár megjegyzendő, hogy egy ilyen bróker segítségével tetszőleges grid architektúra összekapcsolható, amennyiben a különböző koncepciók, reprezentációk és szintaxisok közötti átalakítások megoldhatóak. A negyedik megoldás rendkívül nagy módosítást igényel a desktopgrid szerver oldalán. A szervernek tudnia kell a csatlakozó klaszterről, annak statikus és dinamikus állapot információiról, mely elkerülhetetlenné teszi egy monitorozó rendszer alkalmazását.

Az *5. ábrán* látható ötödik megoldás tűnik a legelegánsabb módszernek klaszterek desktopgridekbe integrálásához. Desktopgrid környezetben a kliensek rácsatlakoznak a szerverre, és munkát kérnek attól. Szakszóval ezt a fajta működést 'pull' üzemmódnak nevezzük. Ezzel szemben a már bemutatott másik architektúrán 'job-manager'-ek küldik be a munkákat a kiválasztott erőforrásoknak, úgynevezett 'push' üzemmódban. Ezzel a megoldással a klaszterek is részt tudnak venni a 'pull' üzemmódú desktopgridek működésében. A desktopgrid klienst módosítva az egyetlen munkacsomag helyett többet is elkérhet egyszerre a szerver-

5. ábra Desktopgridhez csatlakozó klaszter



től, klaszter kompatibilis 'job'-okká alakíthatja azokat, majd beküldheti feldolgozásra a klaszterbe. A desktopgrid szerver egy átlagon felüli teljesítménnyel rendelkező klienst lát csatlakozni. Ehhez a megoldáshoz csak a kliens programot kell módosítani, továbbá mivel az a klaszter 'frontend' gépen fut, ezért az információgyűjtés és a munkabeküldés a klaszterba könnyen megoldható.

Laborunkban ezt a megoldást választottuk, mert ezáltal a klaszterek elegánsan integrálhatóak a desktopgrid architektúrába, megmarad a klaszterek 'job-manager' funkciója, továbbá kevés módosítást igényel a megvalósítása. A SZTAKI Desktop Grid klaszteres verzióját használja a Miskolci Egyetem Általános Informatika Tanszéke a desktopgrid technológia oktatására.

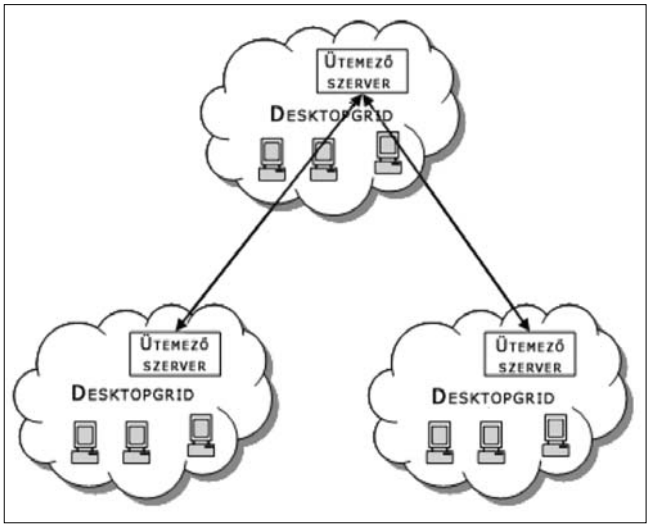
6. Hierarchikus Desktopgrid

Klaszterek támogatásával jelentősen megkönnyítjük a desktopgrid architektúra intézményi elterjedését. Miután sok kisebb intézmény (pl. egyetemi tanszék) önállóan kiépítette saját használatú desktopgridjét, természetes igényként merülhet fel az intézmény egy magasabb szintjén (pl. egyetemi kar) egy nagyobb lélegzetvételű feladat megoldásához a kisebb destkopgrideket összekapcsolva használatba venni. A kiépített desktopgrideket építőelemekként használva lehetőség nyílik azok hierarchiába szervezésére *(6. ábra)*.

Ilyen hierarchiában az alacsonyabb szinten elhelyezkedő desktopgridek munkát igényelhetnek a hierarchiában felettük állótól (pull üzemmód) és fordítva, a magasabb szinten elhelyezkedő desktopgridek munkát adhatnak az alájuk beosztottaknak (push üzemmód).

A SZTAKI Desktop Grid a pull üzemmódot támogatja, mivel ez áll közelebb a desktopgridek működési elvéhez. A magasabb szintről érkező fontos munkáknak prioritáskezeléssel elsőbbség biztosítható, amennyiben a hierarchia ezt megkívánja. A SZTAKI Desktop Grid egy lokális példánya beállítható hierarchikus működésre, vagyis, hogy csatlakozzon rá egy a hierarchiában felette álló SZTAKI Desktop Gridre (a fa struktúrában a szülő elemre). Abban az esetben, ha a hierarchiában a gyermek elemnek kevesebb végrehajtandó munkája akad, mint amennyi szabad erőforrása van, a szülő elemtől további munkát kérhet. A szülő elem egyetlen, nagyteljesítményű kliensként látja a gyermek elemet, analóg módon a klaszterillesztés résznél tárgyaltakhoz. Ehhez természetesen a BOINC szervert olyan funkcionalitással kell kiegészíteni, mely lehetővé teszi annak a kliensként való működést. Ezáltal lehetővé válik az újabb munka kérése, abban az esetben, ha lokálisan nem áll elegendő rendelkezésre.

6. ábra Desktopgridek hierarchiája



A BOINC platform esetében ez könnyűszerrel kivitelezhető. A munkacsomagokat a mester alkalmazás generálja, melyek a BOINC platform saját adatbázisában kerülnek tárolásra. Hogy egy adott munkacsomag egy lokálisan futó alkalmazástól, vagy egy távoli gépről érkezett a BOINC platform számára érdektelen. Elegendő tehát egy új, a szerveren futó démont kifejleszteni, mely figyelemmel kíséri a szerver állapotát. Amennyiben a kliensek munkacsomag kérelme elutasításra kerül, vagyis a szerveren nincs több feldolgozásra váró munkacsomag, a démon BOINC klienst szimulálva további munkacsomagokat kér a hierarchiában felette álló szülő elemtől. Miután megkapta az új munkacsomagokat, nem áll neki a feldolgozásuknak, hanem továbbítja azokat saját szerverének adatbázisába. A démon feladata továbbá az is, hogy figyelje, a hierarchiából kapott munkacsomagok feldolgozásának elkészültét és az eredményeket visszaszolgáltassa a szülő elemnek.

A SZTAKI Desktop Grid hierarchikus verziójának első prototípusa már elkészült, mely egyszintű hierarchiát képes támogatni. Egy most folyó Jedlik Ányos projekt keretében (DTGRID05: Új generációs grid technológiák kifejlesztése és meteorológiai alkalmazása a környezetvédelemben és az épületenergetikában) dolgozunk az általános hierarchikus architektúra megvalósításán.

7. SZTAKI Desktop Grid alkalmazások

Cikkünk végén röviden bemutatjuk azokat a tudományterületeket és alkalmazásokat, melyekhez a SZTAKI Desktop Grid architektúraként szolgál.

A már említett BinSYS projekt mellett nagy számításigény jelentkezik a gyógyszerkutatásban is. Nagymértékű költségcsökkentés érhető el azáltal, ha már a kutatási fázis legelején sikerül kiszűrni a kémiailag instabil, biológiailag inaktív és toxikus molekulákat.

Az ADMEToxGrid [10] projekt keretében a Comgenex cég egy vállalati SZTAKI Desktop Grid felállítását végzi, amit molekulák millióinak ilyen irányú szűrésére fog alkalmazni.

Adatbányászat és mesterséges intelligencia [11] témakörben a Szegedi Egyetemmel karöltve folynak kutatások, egy a SZTAKI Desktop Grid architektúra lehetőségeit kihasználó adatbányász algoritmus kifejleszté-

sében. A projekt innovatív eleme az adatbányász algoritmusok ütemezésének optimalizálása meta-szintű tanulás segítségével. A projekt különös figyelmet szentel az adatvédelemnek. A Szegedi Egyetemen felállított lokális SZTAKI Desktop Griden futó prototípus támogatja az adatbányász projektek helyesség-ellenőrzését, az architektúrának köszönhetően pedig mindemellett bővíthető marad.

A cikk bevezetőjében már említett időjárás-előrejelzés területen a lokális SZTAKI Desktop Grid architektúrát szolgáltat a Magyar Meteorológiai Szolgálatnak numerikus időjárás-előrejelzési és klímamodellezési alkalmazásokhoz [12].

A SZTAKI Desktop Grid projekt nemzetközi sikerét követően, második nemzetközi eredményünk az Egyesült Királyság két egyetemével – a Westminsteri Egyetemmel és a Brunneli Egyetemmel – való együttműködés [13]. Az együttműködés keretében digitális jelfeldolgozás témakörben folyik kutatás periodikus, nem egyenletes eloszlású mintavételi szekvenciák tervezésének területén a digitális jelfeldolgozás zavarmentessé tételéért. A két egyetemen felállításra került egy 100 személyi számítógépből álló desktopgrid, mellyel az addig egyetlen számítógépen futó algoritmus 1 hónapos feldolgozási idejét sikerült 2 napra csökkenteni.

A kutatások mellett a SZTAKI Desktop Grid architektúra a miskolci egyetemen oktatás tárgyát is képezi a Párhuzamos és Elosztott Rendszerek tárgy keretein belül, melynek során a tárgy hallgatói megismerkednek a desktopgrid architektúrára való alkalmazásfejlesztés rejtelmeivel. Az egyetemen felállításra került egy lokális SZTAKI Desktop Grid rendszer, mely a diákok tanulmányi munkáján kívül az egyetemen folyó kutatómunkát is támogatja.

8. Összefoglalás

A cikkben bemutatásra került a BOINC platformra épülő SZTAKI Desktop Grid. A grid személyi számítógépeket építőelemként felhasználva lehetővé teszi számításigényes feladatok megoldását. Külön került bemutatásra a klaszterek támogatásának lehetősége, egy módosított kliens program segítségével, mely a BOINC platform által generált munkacsomagokat hagyományos ‘job’-bá konvertálva átadja azokat a klaszter ‘job manager’-énak. Az építkezést tovább folytatva tárgyaltuk továbbá a desktopgridek hierarchiába szervezésének lehetőségét.

A lehetőség, hogy desktopgridek egymás között átadjanak munkacsomagokat egymásnak egy újabb lépés egy olyan grid infrastruktúra kialakításában, mely könnyen telepíthető és melyhez bárki felajánlhatja erőforrását; két olyan tulajdonság mely napjaink grid rendszereiben egyszerre nem lelhető fel. A SZTAKI Desktop Grid technológiát mind az oktatási, mind a kutatási intézmények használhatják saját gridük felállítására, de mint a Comgenex példája is mutatja, cégek számara is hasznos vállalati gridek létrehozására.

Az adott intézmény már rendelkezésre álló gépeinek bevonásával, minimális költséggel – egy kis szerver üzembeállításával – szuperszámítógép teljesítmény érhető el. A fentiek alapján javasoljuk az oktatási és kutatási intézményeknek, illetve vállalatoknak saját Grid felállítását, amiben a SZTAKI kész a szükséges segítség megadására.

Köszönetnyilvánítás

A szerző köszönetét fejezni ki Kacsuk Péternek, az MTA-SZTAKI Párhuzamos és Elosztott Rendszerek Kutatólaboratórium vezetőjének, Kovács Józsefnek a SZTAKI Desktop Grid projekt vezetőjének, továbbá munkatársainak, Gombás Gábornak, Marosi Attilának és Vida Gábornak a cikk megírásához nyújtott sok segítségért és szakmai támogatásukért.

Irodalom

[1] EGEE: Enabling Grids for E-SciencE. http://public.eu-egee.org/
[2] D.P. Anderson, J. Cobb, E. Korpela, M. Lebofsky, D. Werthimer: SETI@home: An Experiment in Public-Resource Computing, Communications of the ACM, Vol. 45 No. 11, November 2002, pp. 56–61.
[3] D. P. Anderson: BOINC: A System for Public-Resource Computing and Storage. 5th IEEE/ACM International Workshop on Grid Computing, November 8, 2004, Pittsburgh, USA. Available at: http://boinc.berkeley.edu/grid_paper_04.pdf
[4] BOINCstats.com. http://boincstats.com
[5] TOP500 Supercomputer Sites. http://www.top500.org
[6] SZTAKI Desktop Grid. http://szdg.lpds.sztaki.hu/szdg, http://www.desktopgrid.hu
[7] A. Kovács PhD, P. Burcsi, J. Kasza, N. Podhorszki PhD, G. Vida, A. Kornafeld, Generalized binary number systems. http://compalg.inf.elte.hu/projects/binsys/
[8] Kornafeld, A., Kovacs, A.: Szuperszámítógépes teljesítmény szuperszámítógép nélkül – A BinSYS projekt –, Networkshop 2006, Miskolc, NIIF, 2006. Elérhető: http://www.lpds.sztaki.hu/~kadam/BinSYS.pdf
[9] Podhorszki, N., Vida, G.: Alkalmazói programozási felület SETI-jellegű elosztott programokhoz és végrehajtó rendszer a BOINC infrastruktúrára, Networkshop 2005, Szeged. NIIF, 2005. Elérhető: http://www.lpds.sztaki.hu/~pnorbert/pub/desktopgrid-nws05.pdf
[10] ADMEToxGrid. http://www.admetoxgrid.hu
[11] További információ: http://www.sztaki.hu/search/projects/project_information/?uid=00025
[12] További információ: http://www.sztaki.hu/search/projects/project_information/?uid=00188
[13] Gridalliance. http://www.gridalliance.org.uk

Infrastructure of the National Research and Education Network – NIID Program

Keywords: research and education networks, HBONE

In all countries of Europe national research and education networks have an important role in providing information infrastructure for research and development, as well as testing, development and dissemination of the latest networking technologies. In Hungary, the development and operation of research and education network is executed within the framework of the National Information Infrastructure Development Program (NIID Program). A brief overview of recent results of the NIID Program is given, and main components of the frontline infrastructure are introduced along the four strategic fields of the development program.

10 Gigabit Ethernet

Keywords: 10 Gigabit Ethernet, Ethernet, 802.3, LAN

Standardization of 10 Gigabit Ethernet has been going on for several years now. Some recommendations have already been published, but some are being worked on by IEEE members, and are to be finalized this year or next year. In this paper I present the new features of 10 Gigabit Ethernet compared to the earlier and slower members of the Ethernet family.

Impact of WiFi technology on multimedia applications

Keywords: IPv4, IPv6, IEEE 802.11b/g, IEEE 802.11a, WiFi, L2/L3 roaming, VoIP, codec, QoS, H.323.

At WiFi hot-spot deployment an essential question is that 802.11b or 802.11g and/or 802.11a system will be installed. For this decision an efficiency analysis is needed beyond the economic and rational considerations. As IP phone system is increasingly available in university environment, the analysis of practicability of WiFi phones during movement appears as an obvious object in indoor and outdoor environment as well. In this paper we focus on the analysis of the properties of multimedia applications (video, streaming, IP phone) operated over IEEE 802.11b/g/a WiFi systems.

Identification and Authentication of Clients in the European e-Government

Keywords: e-Government, identity management, entity authentication, interoperability

Identification and authentication of the clients are crucial problems of the e-Government procedures. Solutions and models applied in the European countries – among them in Hungary – are highly different and are not interoperable. It is often true within the individual countries too. The most frequent models and practices are outlined and evaluated in the paper. The recent effort of the European Commission to ensure secure, interoperable identity management at all levels of e-Government services by 2010 is also presented.

Authentication and Authorization Infrastructures (AAI) – Protection of Personal Data and AAI Systems

Keywords: identity management, federation, security

It is one of an organization's primary interests to have users properly authenticated and authorized prior accessing services and proprietary information. In heterogenous environment it is worth to apply dedicated infrastructure, so-called middleware for AA tasks. This article shows its importancy and presents some models of identity federations, which are generally used world-wide.

Network Middleware

Keywords: network incident handling and inventory, configuration- and access list management

In the last couple of years something changed in the daily work of network managers. We've got more and more network services so we have to manage more servers and configuration files. How can we decrease this administration load? There is no way to use some undocumented short scripts. What do we mean by "middleware" application and how does it work in some parts of network management?

"Köztéka" – Application for Library and Databank Networks

Keywords: library, library automation, Internet, catalogue

Cooperation of libraries became very important nowadays. Especially the physically separated but for some other points of view (collection, financial resources, territorial closeness etc.) joined libraries have to create their own networks for coordinating their services, customer support, acquisition policy and organizational behavior. These projects should be supported by the integrated library automation systems. The by the MTA SZTAKI developed and distributed and on the "Kistéka" integrated library automation software based "Köztéka" application is one of the solutions especially constructed and produced for all kinds of library networks, and it is particularly suitable for supporting web OPAC and portal services of library networks of local regions.

Metadata Toolkit for Collections of Digital Documents

Keywords: 'eleMEK', digital document, XML, Java, GNU GPL

The 'eleMEK' – is a platform independent, Java and WWW based modular metadata handler toolkit for collections of digital documents. The initial idea for developing it born from the experience of handling digital documents at the Hungarian Electronic Library (MEK). Having seen problems of everyday use and having met with incompatible, inappropriate, incomplete, inaccessible local metadata systems, the developers decided to make a metadata data structure and a toolkit for it to propose for owners of local digital collections. For this purpose, the 'eleMEK' is free for using and modifying under GNU GPL. The article reviews some highlights of the developing story and the state of the toolkit.

Networking challenges in astronomy

Keywords: astronomy, Internet, Virtual Observatory

The paper describes the use of the Internet in the field of astronomy. The focus is on networking challenges and perspectives at Konkoly Observatory of the Hungarian Academy of Sciences.

Application of public resource computing model in practice

Keywords: desktopgrid, dc-api, boinc, SZTAKI Desktop Grid

Supercomputers lead the way in solving computational intensive tasks. However, in some cases one could use the several grid technologies available. The development of grid technologies has begun in two completely different ways. Anyone can be the user of the resources of grids utilizing the clustergrid model, but resources can only be offered with competence. On the contrary, anyone can offer resources for grids utilizing the public resource computing model, but only the institute running the grid can access the resources of it. The article presents the possibility of extending the public resource computing model through SZTAKI Desktop Grid.

Summaries • of the papers published in this issue

Contents

Cover: GEANT – The pan-European broadband research network

Szerkesztőség
HTE Budapest V., Kossuth L. tér 6-8.
Tel.: 353-1027, Fax: 353-0451, e-mail: info@hte.hu

Előfizetés
HTE Budapest V., Kossuth L. tér 6-8.
Tel.: 353-1027, Fax: 353-0451
e-mail: info@hte.hu

Hirdetési árak
1/1 (205x290 mm) 4C 120.000 Ft + áfa
Borító 3 (205x290mm) 4 C 180.000 Ft + áfa
Borító 4 (205x290mm) 4 C 240.000 Ft + áfa

2006-os előfizetési díjak
Közületi előfizetők részére: bruttó 30.450 Ft/év
Hazai egyéni előfizetők részére: bruttó 6.800 Ft/év
HTE egyén tagok részére: bruttó 3.400 Ft/év

Cikkek eljuttathatók az alábbi címre is
Szabó A. Csaba, BME Híradástechnikai Tanszék
Tel.: 463-3261, Fax: 463-3263
e-mail: szabo@hit.bme.hu

Subscription rates for foreign subscribers:
12 issues 150 USD,
single copies 15 USD

www.hte.hu
Felelős kiadó: NAGY PÉTER
Lapmenedzser: Dankó András

HU ISSN 0018-2028

Layout: MATT DTP Bt. • Printed by: Regiszter Kft.