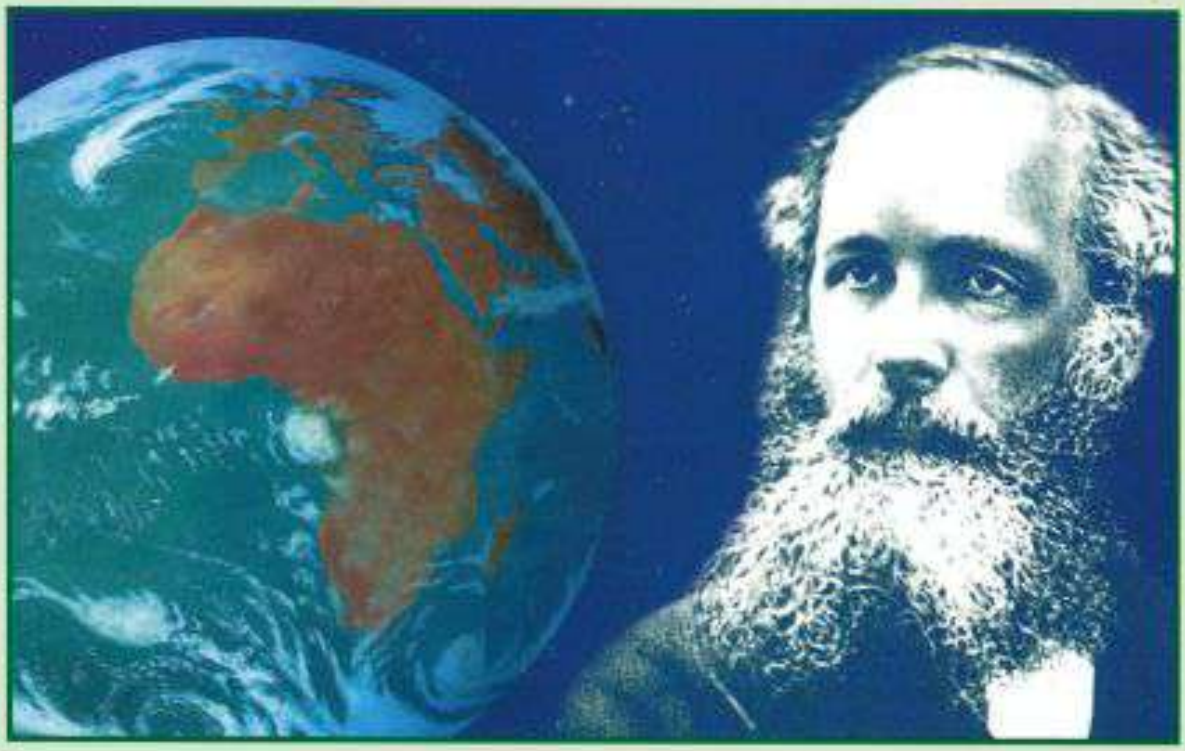
híradástechnika

VOLUME LIX.

2004/4

Április



A hullámterjedés speciális kérdései

Címzési eljárások egységesítése

A szélessávú hozzáférés és méretezési módszerei

Biztonság és elérhetőség

A Hírközlési és Informatikai Tudományos Egyesület folyóirata

Tartalom

Közeljövőnk távközlése 1

A HULLÁMTERJEDÉS SPECIÁLIS KÉRDÉSEI

Dr. Csernoch János
Információátvitel nagy relatív sebességű pontok között 2

Bakki Péter
A troposzférikus szcintilláció hatása a műholdas távközlésre 7

CÍMZÉSI ELJÁRÁSOK EGYSÉGESÍTÉSE

Erdélyi Tibor
Egységes távközlés a különböző infrastruktúrájú hálózatokon 13

Gódor Balázs
Térjünk át az ENUM-ra! 17

A SZÉLESSÁVÚ HOZZÁFÉRÉS ÉS MÉRETEZÉSI MÓDSZEREI

Dr. Dárdai Árpád
Ortogonális frekvenciaosztású többszörös hozzáférés 22

Kuruc Gábor, Lója Krisztina
Routing protokollok hatékonysága 29

Wein Tibor
A hozzáférés-korlátozott DVB CATV műsorterjesztés alapjai 35

BIZTONSÁG ÉS ELÉRHETŐSÉG

Lajtha György
Xyscom rendszer üzembe helyezése Bárdudvarnokon 46

Godányi Géza
Katasztrófavédelem és üzletmenet-folytonosság az információtechnológiában 47

Borovitz Tamás
Elektronikus szavazás – messze még az út vége 53

Könyvet ajánlunk: Információ, társadalom, történelem 58

Sipos László
A múlt tanulságait ismerve építsük a jövőt 59

Nagy Beatrix Havaska
Interjú Dr. Prószéky Gáborral, a MorphoLogic Kft. alapítójával 60

Címlap: Maxwell elmélete segítségével minden információ elérhető a világ minden pontján

Főszerkesztő
ZOMBORY LÁSZLÓ

Szerkesztőbizottság
Elnök: LAJTHA GYÖRGY

BARTOLITS ISTVÁN
BOTTKA SÁNDOR
CSAPODI CSABA
DIBUZ SAROLTA
DROZDY GYŐZŐ
GORDOS GÉZA
GÖDÖR ÉVA
HUSZTY GÁBOR
JAMBRIK MIHÁLY
KAZI KÁROLY
MARADI ISTVÁN
MEGYESI CSABA
PAP LÁSZLÓ
SALLAI GYULA
TARNAY KATALIN
TORMÁSI GYÖRGY

Közeljövőnk távközlése

DR. LAJTHA GYÖRGY

lajtha.gyorgy@ln.matav.hu

A szakembereket és a felhasználókat egyaránt érdekli, hogy szakmánk milyen irányba fog továbbhaladni, és mely újdonságok fogják a következő évtized távközlési és informatikai szolgáltatásait meghatározni. Két-három évvel ezelőtt megjelent a konferenciákon és a sajtóban is a Next Generation Network kifejezés. Ezt akkor annyira elterjesztették, hogy már csak NGN-ről írtak. Ez azonban nem határozta meg az irányvonalat. A megfogalmazás, hogy következő generáció, teljesen szabadon hagyta a fejlődés irányát és lehetővé tette, hogy a gyártók – meglévő koncepcióik alapján – a jelen eszközeit NGN címkével ellátva propagálják. A jelszó azért is előnyös volt, mert időtől függetlenül lehetett bármikor használni, és mindenkor perspektivikusnak, jövőbe mutatónak nevezni az éppen eladni kívánt eszközt, vagy rendszert.

Az elmúlt hónapokban azonban valóban kezd kialakulni a következő évtized meghatározó technikája. Ennek egyik középponti eleme a fotonika. Februári számunkban bemutattuk nemcsak a hullámhosszosztású átvitelt, hanem a fotonikai elven működő hullámhosszváltás lehetőségeit, a fénykapcsolókat és a különböző szűrő eljárásokat a hullámhosszak szétválasztására és átirányítására. Ezzel együtt a fizikusok eddig soha nem látott mértékben le tudják lassítani a fényt, és ezzel reálissá válik, hogy a fénysebességgel haladó jelzések beállítsák a kapcsolókat, amire a fény odaér, majd a fényt ismét felgyorsítva továbbítják a következő kapcsolópontig. Egyértelműnek látszik, hogy a felhasználók megnövekedett internetezési és szórakoztatási igényeit a közeljövőben a fotonika fogja kielégíteni.

A másik meghatározó technika a mobil szolgáltatással egyidejűleg alakult ki. A mobil hálózatban a hívószám már egyértelműen egy személyt jellemez, aki bárhol tartózkodik, elérhető. Ez olyan kényelmet jelent, melyet a jövő hálózatának feltétlenül teljesítenie kell. Itt egy meglévő technikát kell kiterjeszteni, és ahogy a mobil automatikusan közli a hálózattal a felhasználó jelenlétét, ugyanúgy fogja a számítógép az Internet számára tudtul adni a bejelentkező nevét, e-mail címét, amellyel az megtalálható lesz.

Ezzel kapcsolatban kialakul a harmadik megoldandó terület is, miszerint minden személyt egy szám kell, hogy jellemezzen, függetlenül attól, hogy fix állomást, mobil állomást, számítógépet, vagy más egyéni eszközt akar a hálózathoz kapcsolni. Ezt az igényt a Bell Laboratórium elnöke már 1957-ben megfogalmazta: olyan rendszert kell készíteni, melyben a csecsemő talpába tetoválják megszületése után a távközlési számát, amely egészen haláláig érvényes, és bárhonnan, bármikor hívható. Az elképzelés realizálására több mint negyven évet kellett várni, amikor is az ITU-T megkezdte az ENUM kidolgozását, amely ezt az igényt megvalósítja. Napjainkra olyan szintet ért el a fejlesztés, hogy e számunkban két cikk is beszámol erről a témáról.

A bárhol elérhető szélessávú hozzáférés lehetőségéről a villamoshálózati távközlés és az ezt alátámasztó OFDM technika bemutatásával igyekszünk képet adni. Természetesen ez csak egy szűk kiegészítő terület, mert ehhez kapcsolódik a kábeltelevíziós hálózat korszerűsítése, mely szintén segíteni fog a szélessávú elérhetőség terjesztésében. Ezek mellett elméleti jellegű hálózattervezési és hullámterjedési eredményekről is beszámolunk.

Mindezek együttvéve az Ubiquitous hálózat képét vetítik elénk. Erről több mint egy évvel ezelőtt jelent meg cikk lapunkban, – a Telecom 2003 távol-keleti pavilonjainak ez volt a fő koncepciója –, azóta pedig különböző kapcsolódó cikkekben számoltunk be róla. A nehezen kiejthető kifejezés helyett most már csak egy jó magyar szót kell keresnünk, hogy erről a hálózati koncepcióról és ennek problémáiról tudjunk vitatkozni. Talán korlátok nélküli hálózatnak is nevezhetnénk...

Információátvitel nagy relatív sebességű pontok között

DR. CSERNOCH JÁNOS

Budapesti Műszaki Főiskola, Kandó Kálmán Villamosipari Kar, Híradástechnikai Intézet
csernoch.janos@kvk.bmf.hu

Kulcsszavak: relativítás-elmélet, dopplerhatás, reflexió

Az űrkutatásban, az űrhajózásban stb. felmerülhet az információátvitel nagy sebességű közegek között. A problémák közül érdemes kettőt tárgyalni, melyek a következők: a vett frekvencia megváltozása a Doppler-elv következtében, illetve a síktükör visszaverődési törvényének a megváltozása a mozgás irányának és sebességének a függvényében. Mindkettőt a modern fizikakönyvek kimerítően tárgyalják, itt csak ezen jelenségek következményeit vizsgáljuk a távközlés szemszögéből. A következőkben az előbb említett két problémakört tárgyaljuk. A nagy távolságok esetén a duplex terjedési időt is figyelembe kell venni, így ezt a továbbiakban már nem említjük.

1. Doppler-elv

A Doppler-elvet [1,4,7] a klasszikus fizika tágyalja. A speciális relativítás ezt a tárgyalást kiegészítette. A két tárgyalásmód közötti különbség csak viszonylag nagy sebességeknél jelentkezik. A továbbiakban természetesen a relativisztikus tárgyalásmódot használjuk.

Mozogjon a K' koordinátarendszer O' origója a „nyugvó" K koordinátarendszer X tengelye mentén *v* egyenletes sebességgel oly módon, hogy a megfelelő koordinátatengelyek egymással párhuzamosak legyenek (X II X' , Y II Y', Z II Z'). Ha a K koordinátarendszer X tengelye mentén valahol egy X irányú síkhullámot bocsátunk ki, úgy ennek frekvenciáját egy, a K' rendszerben lévő M' megfigyelő „másként látja". A K' rendszerben mért f' frekvencia a K rendszerben mért f frekvencia függvényében

$$f' = \kappa f (1 \pm \beta) \qquad (1)$$

Itt a pozitív jel az egymáshoz közeledő, a negatív jel az egymástól távolodó adó és vevő esetén érvényes. A betűk jelentése:

$$\beta = v/c \quad \text{és} \quad \kappa = \frac{1}{\sqrt{1-\beta^2}}$$

A frekvencia szélső értékei

$$f'_{max} = \kappa f (1 + \beta) \quad \text{és} \quad f'_{min} = \kappa f (1 - \beta) .$$

A frekvenciaeltérés az egymáshoz közeledő adó és vevő esetén

$$\Delta f_K = f'_{max} - f = f [\kappa (1 + \beta) - 1] . \qquad (2)$$

Az említett eredményeknek csekély következményei vannak a távközlésben, ugyanis

v=3000km/sec =1,08.10^7 km/óra ~10^7 km/óra esetén Δf_K ~ 1%.

Nézzük meg milyen eltérést okoz az egymáshoz viszonyított sebesség kvarter-jelfolyam esetén ahol a névleges jelfolyam-sebesség

f = 139264 kbit/sec .

β	f_{min} [kbit/sec]	f_{max} [kbit/sec]	Δf_K [kbit/sec]
10^{-5}	139262,61	139265,39	1,393
10^{-4}	139250,07	139277,93	13,928
10^{-3}	139124,67	139403,19	139,194
10^{-2}	137864,47	140649,61	1385,607

A sugárforráshoz képest a K' koordinátarendszerrel együtt mozgó M' megfigyelő nem ugyanazt az irányt állapítja meg, mint a „nyugvó" K koordinátarendszerben levő M megfigyelő. A K' koordinátarendszerben az M megfigyelő révén megfigyelt irány

$$\cos\alpha'_x = \frac{\cos\alpha_x - \beta}{1-\beta\cos\alpha_x} \qquad (3/a)$$

$$\cos\alpha'_y = \frac{\cos\alpha_y}{\kappa\left[1-\beta\cos\alpha_x\right]} \qquad (3/b)$$

$$\cos\alpha'_z = \frac{\cos\alpha_z}{\kappa\left[1-\beta\cos\alpha_x\right]} \qquad (3/c)$$

Itt $\cos\alpha_x$, $\cos\alpha_y$, $\cos\alpha_z$ a hullámfront terjedési irányainak iránykoszinuszai a K koordinátarendszerben. Hasonlóan $\cos\alpha_x$, $\cos\alpha_y$, $\cos\alpha_z$ a hullámfront terjedési irányainak iránykoszinuszai a K' koordinátarendszerben.

Abban az esetben, ha a hullámfront a K koordinátarendszerben a Z tengely irányából érkezik és a K ' koordinátarendszer az előbbi koodinátarendszer pozitív X tengelye irányába halad, akkor

$\alpha_x = \pi/2$ $\quad$ $\alpha_y = \pi/2$ $\quad$ $\alpha_z = \pi$
$\cos\alpha'_x = -\beta = -v/c$ $\quad$ $\cos\alpha'_y = 0$ $\quad$ $\cos\alpha'_z = -1/\kappa$

A jelenséget aberációnak nevezik.

Ennek lényege, hogy a hullámfront iránya a mozgás következtében látszólag megváltozik.

Tanulság:

1.) $\beta=10^{-3}$ esetén általában
C → VC SDH átalakításnál
zavarok léphetnek fel.

2.) $\beta=10^{-2}$ esetén általában az előbbieken kívül
a PDH multiplexálásnál is zavarok léphetnek fel.

3.) $\beta=10^{-4}$ esetén
a mikrohullámú vevők utánhangolása
szükséges lehet.

2. Térerősségek megváltozása

Fontos ismerni az elektromos és a mágneses térerősség amplitudóját a K' koordinátarendszerben a K koordinátarendszerbeli térerősségeket alapul véve. A koordinátarendszerek felállása azonos az előző fejezetben rögzítettel. A K' rendszerbeli elektromos térerősségek amplitudóit a transzformációs formulákból nyerjük. Ezek mint ismeretes:

$$E'_{X0} = E_{X0}$$

$$E'_{Y0} = \kappa\,[\,E_{Y0} - v\,\mu_0\,H_{Z0}\,]$$

$$E'_{Z0} = \kappa\,[\,E_{Z0} + v\,\mu_0\,H_{Y0}\,]$$

ahol E_{X0}, E_{Y0} és E_{Z0} az elektromos térerősségek amplitúdói a K koordinátarendszerben, továbbá H_{X0}, H_{Y0} és H_{Z0} a mágneses térerősség-komponensek amplitúdói ugyanitt.

A mágneses térerősség a K koordinátarendszerben minden nehézség nélkül meghatározható:

$$\overline{H} = \sqrt{\frac{\varepsilon_0}{\mu_0}}\left[\overline{n}^0 \times \overline{E}_0\right] = \frac{1}{c\mu_0}\left[\overline{n}^0 \times \overline{E}_0\right] = H_{x0}\overline{i} + H_{y0}\overline{j} + H_{z0}\overline{k}$$

Itt

$$E_0 = E_{x0}\overline{i} + E_{y0}\overline{j} + E_{z0}\overline{k}$$

az elektromos térerősség a K koordinátarendszerben

$$Z_0 = \frac{1}{Y_0}$$

a vákuum sugárzási impedanciája és

$$\overline{n}^0 = \overline{n}^0\,(\cos\alpha_x, \cos\alpha_y, \cos\alpha_z)$$

a hullámfront normálisának az irányába mutató egységvektor.

Az elektromos térerősségek amplitúdói a „mozgó" K' koordinátarendszerben mindezek figyelembevételével

$$E'_{X0} = E_{X0}$$

$$E'_{Y0} = \kappa\,[\,E_{Y0}\,(1 - \beta\cos\alpha_x) + E_{X0}\,\beta\cos\alpha_y]$$

$$E'_{Z0} = \kappa\,[\,E_{Z0}\,(1 - \beta\cos\alpha_x) + E_{X0}\,\beta\cos\alpha_z]$$

Az előbbiek segítségével kifejezhetjük az elektromos térerősség amplitúdójának a négyzetét a K' koordinátarendszerben:

$$E'^2_0 = E'^2_{X0} + E'^2_{Y0} + E'^2_{Z0}\,.$$

A végeredmény

$$E'^2_0 = E_0^2\,(1 - \beta\cos\alpha_x)^2 \qquad . \qquad (4)$$

A K' koordinátarendszerbeli M' megfigyelő által észlelt csillapítás (ha tudja, hogy mozog) dB-ben a K koordinátarendszerhez viszonyítva

$$A_{FCS} = 20\log\left(\frac{E_0^{/}}{E_0}\right)^2 = 10\log\left[\kappa^2\left(1-\beta\cos\alpha_x\right)^2\right] \qquad (5)$$

Ha a K' koordinátarendszer *v* sebességgel távolodik a K koordinátarendszer origójától, azaz „fut a hullám elől", akkor

$$\alpha_x = 0\,.$$

A csillapítás értéke ekkor

$$S_{FCS} = 20\log\left(\frac{E'_0}{E_0}\right) = 20\log\sqrt{\frac{1-\beta}{1+\beta}}$$

Tanulság:

A fenti sebességtartományban számottevő szintcsökkenés nincs. Ellentétes irányú mozgás, illetve közeledés esetén szintnövekedés várható az információ torzulása mellett.

3. Kisugárzott spektrum megváltozása

Az előző fejezetben rögzített változások befolyásolják a kisugárzott spektrumsűrűséget.

A K koordinátarendszerben egy meghatározott helyen levő T adó által kisugárzott ω körfrekvenciát és E(t) térerősséget a K' koordináterendszerben bárhol elhelyezett R vevő általában

$$\omega' = \kappa\,\omega\,(1 - \beta\cos\alpha_x)$$

körfrekvenciájú

$$E'(t') = E'(t')\,(1 - \beta\cos\alpha_x)$$

térerősségként észleli.

Ha az elektromos térerősség nem periodikus jel, felírhatjuk azt a K koordinátarendszerben érvényes Fourier-integrál alakra:

$$E(t) = \int_{-\infty}^{\infty} c\,(\omega)\,d\omega$$

A jel spektrumsűrűsége a K koordinátarendszer:

$$c(\omega) = \int_{-\infty}^{\infty} E(t)\,e^{-jwt}\,dt$$

A spektrumsűrűség abszolút értéke, melyet a K' koordinátarendszerben bárhol jelen levő M' megfigyelő észlel a transzformáció értelemszerű alkalmazásával:

$$\left|c'(\omega')\right| = \frac{1-\beta\cos\alpha_x}{\sqrt{1-\beta^2}}\left|c\left[\left(\frac{\sqrt{1-\beta^2}}{1-\beta\cos\alpha_x}\right)\omega'\right]\right| \qquad (6)$$

Ha a K koordináterendszerben mért körfrekvenciasáv $\Delta\omega$ akkor a K' koordinátarendszerben bárhol jelen levő M' megfigyelő ugyanezt a körfrekvenciasávot

$$\omega' = \kappa\,[\,1 - \beta\cos\alpha_x\,]\,\Delta\omega \text{ -nak méri.}$$

Ha a K' koordinátarendszerben levő R vevő közeledik a K koordinátarendszerben levő T adó felé, akkor

$$\alpha_x = \pi \qquad \cos\alpha_x = -1$$

$$\left|c'(\omega')\right|\Delta\omega' = \frac{(1+\beta)}{\sqrt{1-\beta^2}}\left|c\left[\left(\frac{\sqrt{1-\beta^2}}{1+\beta}\right)\omega'\right]\right|\Delta\omega'$$

$$\left|c'(\omega')\right|\Delta\omega' = \left(\sqrt{\frac{1+\beta}{1-\beta}}\right)c\left(\omega'\sqrt{\frac{1-\beta}{1+\beta}}\right)\Delta\omega'$$

Mivel

$$\sqrt{\frac{1+\beta}{1-\beta}} > 1$$

a spektrumvonal nagysága a K rendszerhez viszonyítva növekszik. Továbbá a független változó transzformációjában

$$\sqrt{\frac{1-\beta}{1+\beta}} < 1$$

A spekrtumfüggvény a „körfrekvencia" koordinátarendszerben a „0 frekvenciához" viszonyítva szétterül. A szétterülés mértéke $\beta = 10^{-2}$ esetén kb. 1%. Ez a Doppler-elvvel megegyezik.

Tanulság:

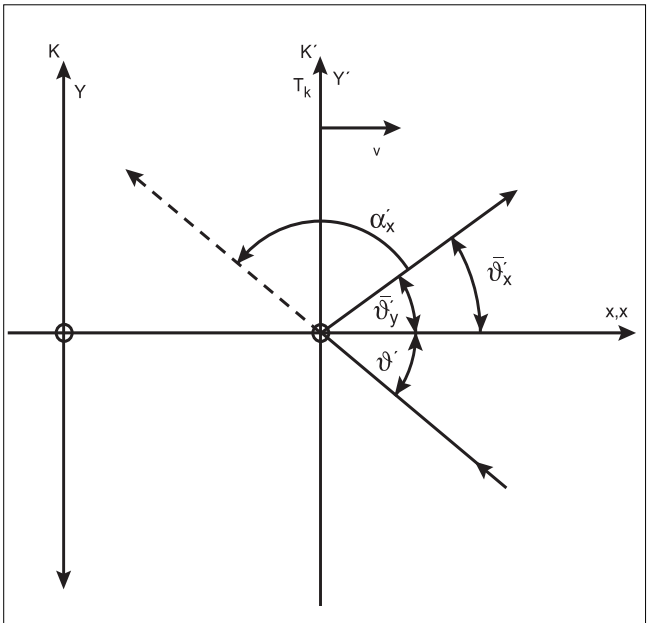
1.) Ha az elektromos jel információt hordoz valamilyen moduláció formájában (AM, FM, 2^N QAM, PSK, FSK,COFDM stb.) akkor a Doppler-effektuson kívül a modulációs oldalsávok torzulása is fellép.

2.) A T adó és az R vevő relatív mozgásának hatására a modulációs spektrum változik. Ennek mértéke $\beta = 10^{-2}$ esetén 1%.

4. A fényvisszaverődés megváltozása a relatív mozgás függvényében

A K' koordinátarendszer O' origója mozogjon a K rendszer X tengelye mentén pozitív irányban egyenesvonalú egyenletes *v* sebességgel oly módon, hogy a megfelelő koordinátatengelyek egymással párhuzamosak legyenek (X II X', Y II Y', Z II Z').

Helyezzük a totális reflexiót keltő T_K tükröt a K' koordinátarendszer origójába oly módon, hogy síkja az Y'Z' síkkal essék egybe *(1. ábra)*.



Az ábrán található szögek jelölései a következők:
ϑ' = a beesési szög a K' rendszerben
ϑ_V' = a visszaverődési szög a K' rendszerben
ϑ = a beesési szög a K rendszerben
ϑ_V = a visszaverődési szög a K rendszerben

1. ábra Visszaverődés mozgó tükrön

A hullámforrást a K koordinátarendszerben az XY tengelyek pozitív felében levő térrészben valahol egy végtelen távoli pontban képzeljük el. A fény az X'Y' síkban verődik vissza, ami most a papír síkjával azonos. A K' koordinátarendszerben érvényes a síktükörre vonatkozó a geometriai optika által rögzített visszaverődés szabálya:

$$\vartheta' = \text{beesési szög} = \text{visszaverődési szög} = \vartheta'_V$$

(Ellenkező esetben a K' koordinátarendszerbeli megfigyelő megtudná, hogy mozog.)

Ezzel szemben a K „nyugalmi" koordinátarendszerben az irodalomban megtalálható számítás szerint a geometriai optika törvényeitől a Doppler-effektus miatt eltérés tapasztalható.

Ha a tükör a hullámmal szembehalad,
akkor ϑ_V visszaverődés szöge kisebb,
mint a ϑ beesési szög.

Ha a tükör a hullám irányába halad,
akkor ϑ_V visszaverődés szöge nagyobb,
mint a ϑ beesési szög.

A helyzet elméletileg nem változik, ha a T_K tükröt a K koordinátarendszer X tengelyére nézve ferdén helyezzük el és az elektromágneses hullám az X tengely mentén negatív irányban terjed *(2. ábra)*.

A visszaverődési törvénytől való eltérés, illetve a szögkülönbség abszolút értéke a következő képlettel fejezhető ki:

$$y_V = \left|\mathrm{tg}\left(\frac{\vartheta-\vartheta_V}{2}\right)\right| = \left|1 - B_V\right|\left[\frac{\mathrm{tg}\,\vartheta}{1+\mathrm{tg}^2\vartheta}\right] = \left|\mathrm{tg}\,\Delta\theta\right|$$

Ahol

$$B_V = \sqrt{\frac{1-\beta}{1+\beta}}$$

(A szögletes zárójelben levő kifejezés az első síknegyedben pozitív, így az abszolút érték jelölést el lehet hagyni.)

Szélsőértékszámítással igazolható, hogy a geometriai optika törvényétől való maximális eltérés jó közelítéssel ϑ = 45°-os beesési szög esetén lép fel. A viszonyok áttekintésére táblázatot állítottunk össze.

$\beta = 10^{-2}$	ϑ [fok]	ϑ_V [fok]	$\Delta\vartheta=\vartheta-\vartheta_V$ [fok]
(v=3000 km/s)	20	19,6331	0,3600
	30	29,5050	0,4950
	45	44,4270	0,5730x
	60	59,5026	0,4974
	70	69,6303	0,3697

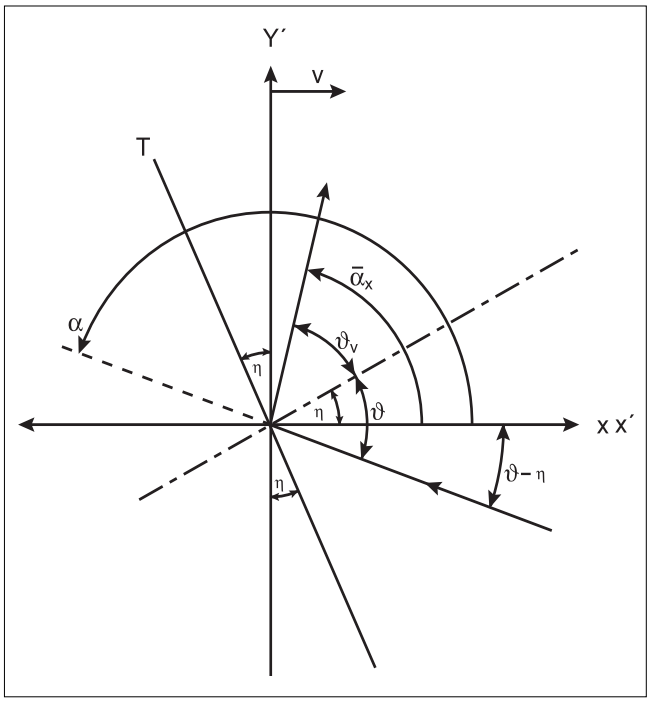
A számadatok 45°-ra vonatkoztatva bizonyos mértékben szimmetrikus elrendezésűek.

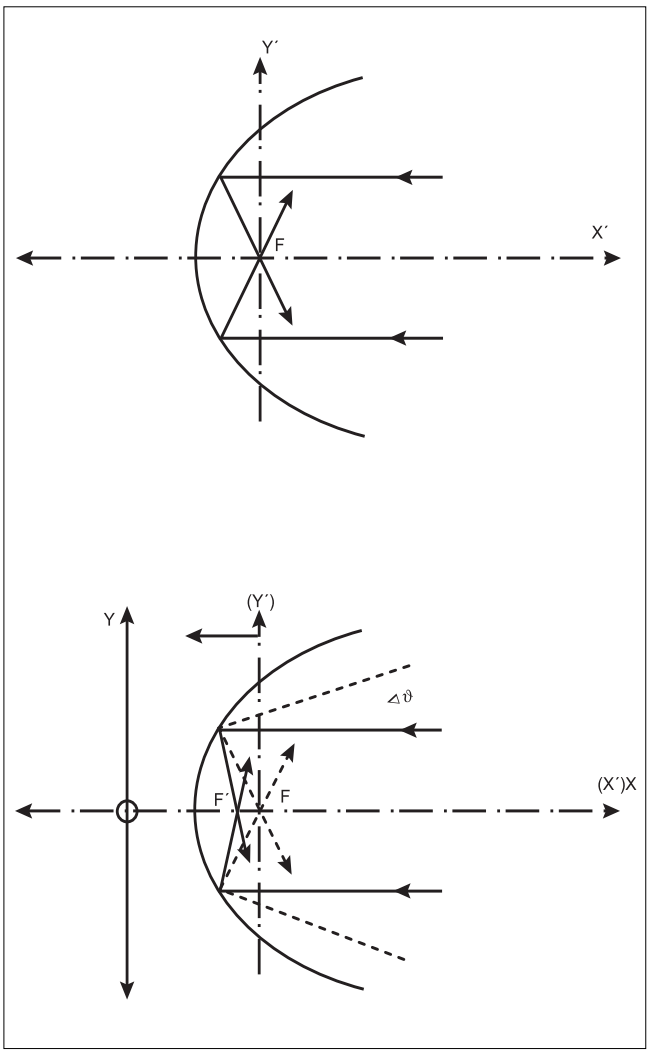
5. Elektromágneses hullámok visszaverődése forgásparaboloid tükör felületéről

Helyezzük a forgásparaboloid tükör fókuszpontját a „mozgó” K’ rendszer origójába és a tükör tengelyét a K’ koordinátarendszer X’ tengelyének az irányába oly módon, hogy a forgásparaboloid tükör tükröző felülete a pozitív X’ tengely irányába essék *(3. ábra)*.

Mozogjon a K’ rendszer O’ origója a K koordinátarendszer X tengelyének pozitív irányába oly módon, hogy

2. ábra Visszaverődés ferdén elhelyezett tükrön





3. ábra Defókuszálódás

a megfelelő koordinátatengelyek egymással párhuzamosak legyenek (X II X’, Y II Y’ és Z II Z’).

Ebben a helyzetben a forgásparaboloid antenna olyan alakzatnak fogható fel, ahol a tükör felületének a normálisa és az X’ illetve X tengely által bezárt szög

$$\eta = \vartheta$$

(ami most a mindenkori beesés szögével egyenlő) a forgásparaboloid tengelyétől eltávolodva minden pontban más és más.

Ha most a tükörre az X tengely pozitív irányából egy végtelenben elhelyezett sugárforrásból elektromágneses síkhullám érkezik, akkor a K’ koordinátarendszerben levő M’ megfigyelő a hullám fókuszálódását a tükör fókuszpontjában minden tekintetben teljesen rendben levőnek találja. (Különben megtudná, hogy mozog.)

A K koordinátarendszerben levő M megfigyelő ugyanakkor bizonyos defókuszálódást észlel, ami a szembenálló antennák nyereségének csökkenésében nyílvánul meg (jel/zaj viszony romlása, bittévesztés mértékének növekedése).

A defókuszálódás mértékét pontosan számítani igen bonyolult, már csak azért is, mert a defókuszálódás mértéke a forgásparaboloid tengelyétől eltávolodva válto-

zik. Szerencsére a defókuszálódás igen pontos számítására nincsen szükség. Elegendő a tükör főnyalábjának az alakjából kiindulni. Példaképpen vegyünk egy ∅4m átmérőjű forgásparaboloid antennát. Ennek lényeges paraméterei:

Antennanyereség	GI = 48 dB
Főnyalábszélesség (3dB-es pontok távolsága)	2x 0,5°

Az előző fejezetben rögzített táblázat alapján az átlagos defókuszálódást ϑ = 45° átlagbeesési szög esetén úgy foghatjuk fel, mintha a bejövő hullámfront az X illetve X' tengely helyett attól a forgásparaboloid antenna „nyugalmi" helyzetében a táblázatban feltüntetett szögben eltérő irányban érkezne a forgásparaboloid antenna felületére. Ez úgy adás, mint vételi irányban érvényes.

A konkrét példánk esetében

ß = 10-3 esetén a romlás már észlelhető

ß = 10-2 esetén a nyereség csökkenése már 3 dB-nél nagyobb értékű

ß = 10-1 esetén a nyereség csökkenése 10 dB-nél jóval nagyobb lehet.

A példából jól látható, hogy a többi antenna esetében a viszonyokat a főnyaláb alakjának az ismeretében jól meg lehet becsülni.

Tanulság:

Az űrhajók és az űrrepülőgépek sebességét nagyságrendekkel meghaladó érték esetén számítások szerint már észrevehető a mozgó koordinátarendszer hatása. Így a jövőben számítanunk kell a relativisztikus elvből következő hatásokkal.

Irodalom

[1] Novobácky Károly:
Relativítás elmélete.
Tankönyvkiadó 1950. Budapest

[2] Albert Einstein:
Über die spezielle und algemeine Relativitaetstheorie.
Vieweg und Dohn Brauschweig 1921.

[3] Albert Einstein:
Les fondements de la théorie de la rélativité générale.
Librerie scientifique Hermann 1933.

[4] Novobácky Károly:
Elektrodinamika.
Tankönyvkiadó 1950. Budapest

[5] Dr. Simonyi Károly:
Theoretische Elektrotechnik.
VEB Deutscher Verlag der Wissenschaften.
Berlin 1979.

[6] Csepeli Miklós–Dr. Selmeczi Kálmán–
Tóthné Szemes Marianne:
Műszaki Fizika I. (Főisk. jegyzet)
Műszaki Könyvkiadó, Budapest 1983.

[7] Richard P. Feynmann–Robert B. Leighton–
Matthew Sands: Mai fizika.
Massachusetts, USA
Műszaki Könyvkiadó. Budapest. 1970

[8] Joachim Frisius:
Vom Aether zum Raum-Zeit Kontinuum.
Eine Einführung in die spezielle Relativitats-theorie
für Physiker und Elektrotechniker.
Kézirat. Berlin 1994.

[9] Joachim Frisius:
Von Coulomb bis Einstein.
Die entwicklung der Maxwellschen Gleichungen.
Verlag Harri Deutsch 1998.

Hírek

A **Budapesti Műszaki és Gazdaságtudományi Egyetem Távközlési és Média Informatikai Tanszéke** március 22-23-án nemzetközi konferenciát rendezett. A kétnapos konferencia központi témája a domainek közötti internetkapcsolat minősége és szimulációja volt. A konferenciát Halász Edit és Vidács Attila rendezték. A világ minden részéről jöttek előadók, akik színvonalas előadásaikban igyekeztek meghatározni a követelményeket és a minőségjavítás módszereit.

A felkészült előadók vizsgálták az irányítás és hálózattervezés kérdéseit, a forgalomméretezést, a minőségi előírásokat és azok ellenőrzését, mérését. A két éve indult konferenciasorozat ezen második alkalma igazolta, hogy érdemes speciális területek megvitatására összejövetelt szervezni. Számos fiatal jelent meg új gondolatokkal, de nem féltek attól sem, hogy régen bevált módszereket korszerűsítve felhasználjanak.

Ez a szakmai műhely mindenki számára tanulságos volt és a résztvevők egymástól tanulva és egymást kiegészítve alakítottak ki a helyszínen is új eljárásokat. A sikerre jellemző, hogy jövőre ismét megrendezik Európában ezt a konferenciát.

A troposzférikus szcintilláció hatása a műholdas távközlésre

BAKKI PÉTER

BME Villamosmérnöki és Informatika Kar, Szélessávú Hírközlő rendszerek és Villamosságtan tanszék
bakki@mht.bme.hu

Reviewed

Kulcsszavak: csillapítás, fading, rövididejű változások, turbulanciák

A közeljövő tervezett műholdas adatátviteli szolgáltatásai megkövetelik a nagy sávszélességet és a kíváló használhatóságot. Az átviteli paraméterek javításának elsősorban a műholdas rádiócsatorna jellemzői szabnak korlátot, ezenbelül is főként a térben és időben is erős csillapítás ingadozás. Ennek az ingadozásnak a leggyorsabban változó összetevője a troposzférikus szcintilláció, amelynek előrejelzési módszereit, hatásait és a lehetséges védekezési eljárásokat ismerteti a cikk.

Műholdas kapcsolatok tervezésénél alapvető szempont az átviteli út csillapításának meghatározása. Ez a csillapítás több tényezőből tevődik össze, amelyek különböző módon függnek a felhasznált frekvenciasávtól, a földrajzi elhelyezkedéstől, időjárási paraméterektől és az emelkedési szögtől (eleváció), melyen a műhold látható a földi végpontról. A műholdas csatorna csillapításának számításánál felmerülő paraméterek: a szabadtéri csillapítás, az antennák jellemzői, az atmoszférikus gázok csillapítása, a csapadék hatása, a troposzférikus és az ionoszférikus szcintilláció, polarizáció elfordulás és a földi végpont környezetéből adódó hatások [1].

A nagyobb sávszélesség iránti igény maga után vonja az alkalmazott vivőfrekvenciák növekedését mind a földi, mind a műholdas rendszerekben, ezzel együtt a csillapítás összetevőinek arányai is átrendeződnek, a kisebb frekvenciákon elhanyagolható hatások válnak jelentőssé. Ilyen, 10 GHz fölött számottevővé váló jelenség többek között a troposzférikus szcintilláció [2].

A kutatások kimutatták, hogy bizonyos csillapítás összetevők (csapadékcsillapítás, atmoszférikus csillapítás, troposzférikus szcintilláció) előfordulási valószínűségei nem függetlenek egymástól, és a korrelációjuk pozitív, tehát az egyik csillapítás összetevő növekedésekor megnő a valószínűsége a többi növekedésének is [3].

Mivel az összetevők keletkezési mechanizmusa és így időbeli viselkedése jelentősen eltér, ezért érdemes külön is vizsgálni azokat, hogy megfelelő védekezési módszert találhassunk ellenük. A cikkben elsősorban a troposzférikus szcintillációval foglalkozom, mivel ennek a jelenségnek a vizsgálata a közeljövő műholdas rendszereinek kialakításával kapcsolatban újra előtérbe került. A tervek szerint ezek a rendszerek a milliméteres hullámhosszon működnek majd, ezért a kutatások is erre a hullámhossz tartományra koncentrálnak.

1. A troposzférikus szcintilláció

A troposzférikus szcintilláció már régen foglalkoztatja a tudományt, bár sokáig csupán a csillagászok vizsgálták, mivel a jelenség legegyszerűbben az optikai frekvenciasávban volt érzékelhető, és a csillagászati megfigyeléseket jelentősen befolyásolta. Ha valaki felnéz az éjszakai égboltra, akár szabad szemmel is láthatja, hogy a csillagok fénye viszonylag gyorsan változik. Más hullámhossz-tartományokban is megfigyelhető a troposzférán áthaladó elektromágneses hullám amplitúdójának ingadozása, a szcintilláció. Ennek oka, hogy a troposzférában terjedő elektromágneses hullámok időben változó, inhomogén törésmutatójú közegen haladnak át.

A szcintilláció elméleti megközelítéséhez a Kolmogorov által javasolt, folyadékok és gázok dinamikus viselkedését leíró modell szolgálhat alapul, amely a turbulens közegben fellépő sebesség-ingadozásokat is figyelembe veszi. Eszerint a turbulens jelenséget két méret jellemzi: az örvény külső (l_1) és a belső (l_2) mérete. A turbulens áramlás kialakulásakor a külső méreten felvett mozgási energia megoszlik a kialakuló kisebb örvényekben, melyekben ismét kisebb örvények jönnek létre tovább osztva az energiát. Az így felépülő turbulens áramlásban az örvények mérete l_1 és l_2 közé esik. A kisebb méretű örvényekben a disszipáció aránya egyre nagyobb a mozgási energiájukhoz képest, míg a méret el nem éri l_2-t, ahol a két érték egy nagyságrendbe esik, és további, kisebb örvények már nem tudnak kialakulni. A troposzférában kialakuló turbulencia belső mérete (l_2) néhány milliméter lehet, míg a külső méret 10 m és 1 km között alakul. A turbulencia belső szerkezete fraktálszerű [4], azaz több méretbeli nagyságrenden keresztül térbeli önhasonlóságot mutat.

A troposzférikus turbulencián belül a hőmérséklet, a nyomás és a páratartalom változik, ami a törésmutató időbeli és térbeli ingadozását eredményezi. Az alkalmazott hullámterjedési modell szempontjából alapvető kérdés a vizsgált hullámhossz és az inhomogén törésmutatójú közegben található struktúráknak a méretbeli aránya. Ha a legkisebb, már homogénnek tekinthető területek mérete (belső méret) jóval nagyobb, mint a hullámhossz, akkor a geometriai optikai megközelítés a célravezető. Ha viszont a turbulencia külső mérete kisebb, mint a hullámhossz, akkor a hullámok elhajlásával célszerű számolni. Mivel a milliméteres hullámhossz

l_1 és l_2 közé esik általában, ezért a már említett megközelítések egyike sem használható ebben az esetben.

Az alkalmazott szcintilláció-modellek csak statisztikai jellemzőket szolgáltatnak, és a számítási módszerek paramétereit mérési eredményekből származtatták. A mérési eredmények feldolgozása során felmerült, hogy a csapadékmentes (száraz) és a csapadékos (nedves) körülmények között fellépő szcintilláció statisztikai jellemzői jelentősen eltérnek. Az egyszerűbb szcintilláció előrejelzési módszerek nem tesznek különbséget a kétféle szcintillációtípus között, így csak átlagos értékeket szolgáltatnak, ezért eltérő klimatikus viszonyok (eltérő száraz és nedves szcintilláció arányok) mellett a pontosságuk is eltér. A felhőképződés és a nedves szcintilláció korrelációját felhasználva a továbbfejlesztett előrejelzési modellek pontosabbak, viszont bemeneti paraméterként szükséges a felhősödést jellemző mutató.

2. A troposzférikus szcintillációval kapcsolatos mérések

Az eddig publikált mérések általában a milliméteres hullámú, fixen telepített műholdas rendszerek használhatóságával kapcsolatos, statisztikai paraméterek meghatározására koncentráltak. A mérések során geostacionárius műholdak több frekvencián (INTELSAT: 11.45 GHz, Olympus: 12.5, 19.77, 29.66 GHz, Italsat: 18.7, 39.6, 49.5 GHz) működő jeladóinak jelszint-ingadozását és a meteorológiai adatokat regisztrálták, ezeket a méréseket különböző földrajzi területen elhelyezett állomásokon végezték el.

Általában a fading amplitúdó mintavételezésének frekvenciája 2-20 Hz között volt, de több helyen csak a néhány percre átlagolt adatokat tárolták. A szcintilláció szórását ugyancsak néhány (1-10) perces intervallumokra kiszámítva adták meg. A hosszú idejű statisztikák előállításához több éven keresztül mértek, viszont az így keletkezett adathalmazok méretük miatt nehezen kezelhetők. Ezért a közrebocsátás előtt minden mérőhely előfeldolgozást, válogatást és korrekciókat alkalmazott.

Az állomások eltérő tudományos céljai feldolgozási és kimeneti adatformátumbeli különbségeket okoztak. Azok a mérőhelyek, melyek csak a szcintilláció vizsgálatára koncentráltak, az elméleti munkák alapján, már a mérések során kiemelték a szcintilláció-fadinghez tartozó frekvenciatartományt, és a lassabb és a gyorsabb változásokat eltávolították a mért eredményekből. Több állomás csak az általuk szcintilláció-eseménynek azonosított mérési sorozatokat tette közzé.

Minthogy a jelenség igen sok tényező függvénye, melyek között a földrajzi és a klimatikus jellemzők is fontos szerepet kapnak, ezért az eddigi, viszonylag kevés földrajzi területen elvégzett mérés távolról sem adhat pontos képet. A problémákat még súlyosbítja, hogy a műhold-föld kapcsolatot sok egyéb hatás is befolyásolja, melyek nehezen különíthetők el a troposzférikus szcintillációtól.

Az eddig elvégzett mérések nehezen vethetők össze, mivel a más környezetben, eltérő berendezésekkel és különböző mintavételi és utófeldolgozási módszerekkel nyert adatok értelmezésükben, és formátumukban is eltérnek.

3. Troposzférikus szcintilláció-modellek

A légköri törésmutató ingadozásának nagysága és térbeli eloszlása meghatározza a szcintilláció mértékét, amely a frekvenciával, a hullám turbulens közegben megtett útjának hosszával együtt nő, és az apertúra átlagolás következtében, az antenna effektív átmérőjének növekedésével csökken. A turbulens rétegbeli terjedési út hossza az antenna elevációjának (emelkedési szögének) függvénye, de mivel a szcintillációt okozó troposzférikus réteg igen vékony, ennek hatása csak alacsony elevációnál jelentős. A szcintilláció erősen függ a klimatikus zónától, a hőmérséklettől, a törésmutató páratartalomtól függő komponensétől, az atmoszférikus csillapítástól illetve a cumulus és cumulonimbus típusú felhők megjelenésétől.

3.1. Hosszúidejű statisztikus modell

A legtöbb statisztikus előrejelzési modell az amplitúdó ingadozást (χ [dB]), annak szórását (σ_χ [dB]) vagy szórásnégyzetét (σ^2_χ [dB^2]) földfelszíni meteorológiai mérések segítségével határozza meg. Általánosan használják a ITU-R P. 618-as ajánlásában szereplő, hónapra átlagolt és ennél hosszabb időre számított statisztikus szcintilláció modellt, amely a többi hosszúidejű modelleknek is hivatkozási alapja. Ez az ajánlás a műhold-Föld összeköttetések tervezéséhez szükséges előrejelzések készítéséhez ad támpontokat, legnagyobb segítséget a műholdas rendszerek rendelkezésre-állásának számításához nyújt.

Az ajánlásban ismertetett, szcintillációra vonatkozó fading-statisztikai számítási eljárás figyelembe veszi az átlagos felszíni hőmérsékletet (t), az átlagos felszíni páratartalmat (H), a vivőfrekvenciát (f), az összeköttetés eleváció szögét (Θ), a földi antenna átmérőjét (D) és az antennahatásfokot (η). [1]

Ez a módszer kombinálja az elméleti megfontolások alapján megalkotott összefüggéseket, a mérési eredmények segítségével meghatározott paraméterekkel. Az eljárás a következő bekezdésekben leírt lépéseken keresztül vezet el a szcintilláció okozta fading időszázalékra vonatkoztatott amplitúdó eloszlásának kiszámításáig.

Először a hőmérséklet és a páratartalom segítségével az ITU-R P. 453 [5] ajánlás szerint meghatározzuk a törésmutató index „nedves” tagját (N_{wet}), amely a hőmérséklet és a páratartalom növekedtével nő. Majd képezzük a referencia amplitúdó szórást (σ_{ref} [dB]):

$$\sigma_{ref} = 3.6 \cdot 10^{-3} + 10^{-4} \cdot N_{wet} \qquad (1)$$

A következő lépés az effektív útvonalhossz (L [m]) kiszámítása, melynek paramétere a turbulens réteg magassága (e modellben $h_L \approx 1000$ m használandó):

$$L = \frac{2 \cdot h_L}{\sqrt{\sin^2(\Theta) + 2.35 \cdot 10^{-4}} + \sin(\Theta)} \qquad (2)$$

Az antennába érkező jel térbeli eloszlása nem egyenletes és időben változó. Az antenna különböző pontjain megfigyelhető jelek korrelációja a növekvő átmérő esetén csökken. Ha az antenna elég nagy, akkor a térbeli átlagolás révén a szcintilláció fading csökkenését érhetjük el.

Az antenna átlagolási tényező vagy más néven apertúra átlagolás a (3) képlet szerint alakul, mely az effektív antennaátmérő, a frekvencia és az effektív útvonalhossz segítségével számítható. A modellt 3-30 méteres antenna átmérőkre hitelesítették. Ez az a paraméter, melynek számítását a továbbfejlesztett modellekben, a legtöbb esetben módosították.

$$g(x) = \sqrt{3.86 \cdot \left(x^2 + 1\right)^{11/12} \cdot \sin\left[\tfrac{11}{6} \cdot arctg\left(\tfrac{1}{x}\right)\right] - 7.08 \cdot x^{5/6}} \qquad (3)$$

ahol

$$x = 1.22 \cdot D_{eff}^2 \cdot f / L; \qquad D_{eff} = \sqrt{\eta} \cdot D \qquad (4)$$

Az (5) egyenlet alapján számolhatjuk ki a szcintilláció-szórást (σ [dB]), amelyben figyelembe vesszük a terjedési útvonalat, a frekvenciát, az antennát és a már említett, helyi légköri adatokat.

$$\sigma = \sigma_{ref} \cdot f^{7/12} \cdot \frac{g(x)}{(\sin(\Theta))^{1.2}} \qquad (5)$$

A fenti módszerrel kiszámított szórásból a (6) időszázalékokra vetített súlyozó tényezővel kapjuk a szcintilláció-fading amplitúdójának időszázalékokra vetített eloszlását, $A_s(p)$-t a (7) egyenlet alapján.

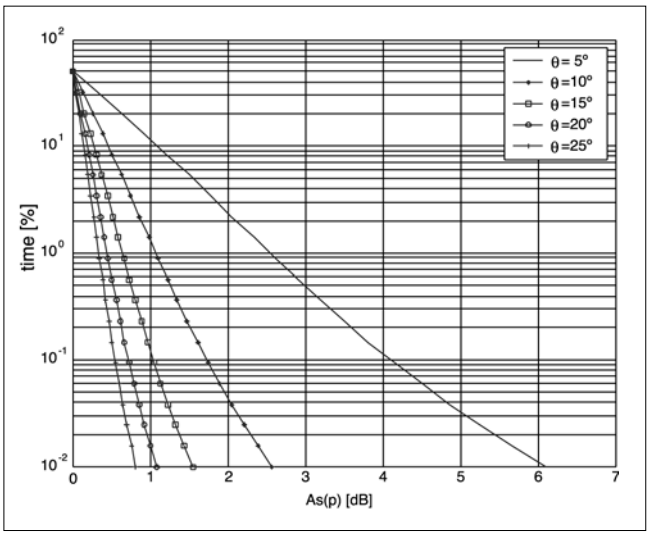
$$a(p) = -0.061 \cdot (\log_{10} p)^3 + 0.072 \cdot (\log_{10} p)^2 - 1.71 \cdot (\log_{10} p) + 3.0 \qquad (6)$$

$$A_s(p) = a(p) \cdot \sigma \qquad (7)$$

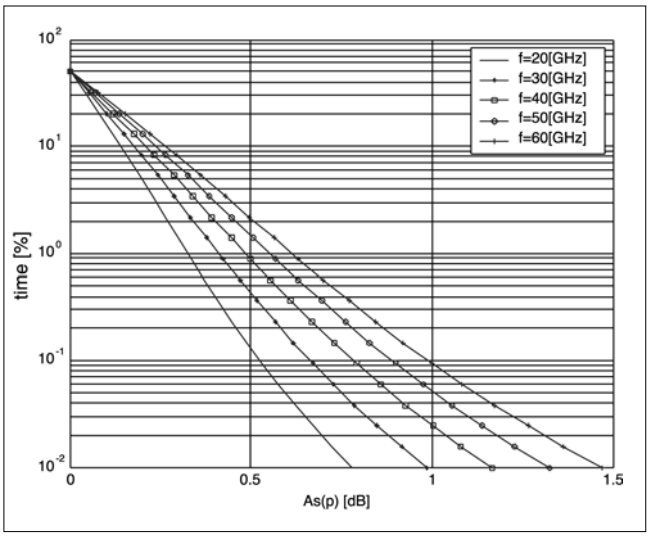
A számítási módszer megismerése után láthatjuk, hogy a szcintilláció igen összetett jelenség, sok tényezőtől függ, és ezek komplex összefüggéseken keresztül hatnak a végeredményre. Látható továbbá az is, hogy a különböző paraméterekre erősen eltérő érzékenységgel reagál a szcintilláció-modell. Az értékek gyakorlatban felmerülő tartományában kisebb hatása van az antenna paramétereinek, a turbulens réteg magasságának és a meteorológiai tényezőknek, közepes a frekvenciának, míg az elevációs szög dominál.

Nézzük, hogyan alakul a szcintilláció a domináns paraméterek különböző értékeinél. Az *1. és 2. ábrán* figyelhetjük meg a szcintilláció függését az elevációs szögtől és a frekvenciától 3 m-es átmérőjű 75%-os hatásfokú antenna esetén, 25°C hőmérséklet, 50% páratartalom, 1000 km turbulens réteg magasság mellett.

Az *1. ábra* mutatja a szcintilláció függését az elevációs szögtől 30 GHz-en, és a *2. ábra* a frekvenciafüggést 25°-os elevációnál. Megfigyelhető, hogy a szcintillációt erősen befolyásolja az eleváció szöge, különösen jelentős a változás az alacsony emelkedési szögek esetén. A szcintilláció mértéke a kisebb antenna átmérővel számolva nagyobb. A modell érvényességét a 3-30 m-es antenna átmérő tartományra ellenőrizték, de napjainkban általában kisebb antennákat (max. D=2 m) alkalmaznak.



1. ábra A szcintilláció okozta fading időszázalékra vetített eloszlása az eleváció függvényében 30 GHz-en



2. ábra A szcintilláció okozta fading időszázalékra vetített eloszlása a frekvencia függvényében 25°-os elevációnál

3.2. Kis időléptékű sztochasztikus modellek

Első közelítésben a szcintilláció által okozott jelingadozások decibelben, néhány percnél kisebb mintavételi periódus esetén, Gauss eloszlást mutatnak, melyet várhatóértékével és szórásnégyzetével jellemezhetünk. Banjo és Vilar megfigyelései alapján a mért eloszlás nem teljesen szimmetrikus a várható értéke körül, hanem a negatív oldalon (csillapítás) kihasasodik a pozi-

tív oldalhoz (erősödés) hasonlítva. Ez a jelenség a nagy szórású szcintillációs esetekben különösen jól megfigyelhető.

Az eredeti modellt pontosította Van de Kamp [6], szerinte a szcintilláció-folyamat (χ), amelyet a csillapítás várható értékétől decibelben kifejezett eltéréssel definiált, inkább Rice-Nakagami eloszlást követ a (8) egyenlet szerint.

$$p_\chi(\chi)=\frac{\ln 10}{20}\cdot\frac{10^{2\cdot\chi/20}}{\xi^2}\cdot\exp\left(-10^{2\cdot\chi/20}-1\right)\cdot I_0\left(\frac{10^{\chi/20}}{\xi^2}\right) \quad (8)$$

Az egyenletben szereplő ξ paraméter a szcintilláció intenzitását jellemzi, és a folyamat szórásával arányos.

Távközlési rendszerek viselkedésének szimulációjához szükségünk van a szcintilláció fading időbeli lefolyásának modellezésére. Ezt az amplitúdó ingadozási folyamatot – Kassanides és Otung munkája alapján [2] – egyszerű dinamikus modellel állíthatjuk elő, a spektrális tulajdonságok és a valószínűség sűrűség-függvény ismeretében. Ez a módszer fehér Gauss zajból megfelelő határfrekvenciájú aluláteresztő szűrővel kialakítja a kívánt spektrumot, majd memóriamentes, nemlineáris eszközzel képezi a szcintilláció fading mintáit, melyek így az elvárt statisztikai jellemzőkkel rendelkeznek. Az aluláteresztő szűrő 0.3 Hz határfrekvencia felett $f^{-8/3}$-os meredekséggel vág le, az alkalmazott nemlinearitás hetedfokú, melynek együtthatóit mérési eredmények segítségével állapították meg.

A szcintilláció-folyamat időbeli lefolyása fraktál (önhasonló) jellemzőket mutat, tehát a kis időléptékű fading becslésnek eszköze lehet a fraktál folyamattal történő modellezés is. Celandroni és Potorti bemutatta [4], hogyan alkalmazható a szakaszos Brown-mozgás fraktál-jellegű folyamat a szcintilláció modellezésére.

4. A szcintilláció a csatornaparaméterek és időjárási jellemzők függvényében

A műholdas rendszer tervezésénél felhasználhatók a meglévő szcintilláció modellek, de használatukhoz a tervezett összeköttetésre vonatkozó összes paraméter pontos ismerete szükséges, és még ekkor sem garantált, hogy az adott földrajzi teületen a választott modell megfelelő pontossággal becsli a szcintilláció fading-et. Pontosabb képet kaphatunk, ha már vannak mérési eredményeink és a tervezett rendszer csak egy paraméterben tér el attól, amelyen a mérést végezték. A tervezés során a paraméter változtatás hatásának becslésére egyszerűsített modelleket használnak, amelyekkel átskálázható a már meglévő, más értékeken alapuló előrejelzés.

4.1. Frekvencia és polarizációfüggés

Mind az ITU-R [1] mind a továbbfejlesztett Karasawa, Yamada és Allnutt [7] modellből meghatározható a frekvenciafüggés, amely minden esetben hatvány függvény szerint alakul.

$$\frac{\sigma_1^2}{\sigma_2^2}=\frac{g^2(D_e,f_1)}{g^2(D_e,f_2)}\cdot\left(\frac{f_1}{f_2}\right)^a \quad (9)$$

A frekvenciaaránytól függő tényező kitevője (*a*) az ITU-R modell szerint 7/6, más modellek ennél alacsonyabb értéket is javasolhatnak (pl.: 0.9).

Az antenna átlagolási tényezők hányadosa is frekvenciafüggő, bár a mérések szerint általános antenna méreteknél a változás elhanyagolható (<1%), viszont nagyobb antenna méretek és magasabb eleváció esetén a függés erősebb lehet.

A különböző helyeken regisztrált mérési eredmények a frekvenciafüggés számításakor mutatnak jelentősebb eltéréseket a predikciós modellekhez képest. Ennek a jelenségnek az értelmezésére több elmélet is körvonalazódik. A lehetséges okok között szerepel, hogy a más-más helyen elvégzett mérések során nem tettek különbséget a szcintilláció-események kialakulási körülményei szerint.

A mérési tapasztalatok szerint a száraz és a csapadékos időben jelentkező szcintilláció statisztikus jellemzői erősen eltérhetnek. Száraz esetben a szcintilláció eredete a légkörben jelenlévő pára és gázok turbulencián belüli egyenetlen és időben változó eloszlására vezethető vissza. A csapadékos, illetve felhős esetben viszont a felhőkben keletkező turbulens áramlások okozzák a vett jel ingadozását. Bár ez az elmélet igazolást nyert, mégsem képes a mérési és a számítási eredmények közötti eltérések maradéktalan magyarázatára. Egy másik érdekes elmélet szerint a szcintilláció-jelenség során az antennába érkező hullám beesési iránya is ingadozik, ami a nagy átmérőjű, kis nyalábszélességű antennák esetén a vett jelben járulékos ingadozást okozhat. Ez az érték összemérhető lehet a szcintilláció okozta amplitúdó ingadozással.

A rádióösszeköttetést a frekvenciáján kívül a polarizációja jellemzi. Felmerülhet a kérdés, hogy a szcintilláció milyen mértékben függ a jel polarizációjától. A fizikai modell szerint a turbulenciában keletkező örvények izotróp elektromágneses tulajdonságokat mutatnak, tehát polarizációfüggés nem várható. Ezt az elméletet a mérések többsége is igazolta, bár a száraz szcintilláció esetén, egyes mérések ettől eltérő eredményeket szolgáltattak, de az eltérés elméleti igazolása még várat magára.

4.2. Függés az időjárási paraméterektől

Az egyszerű modellek csak a törésmutató index nedvességfüggő tényezőjét veszik figyelembe az időjárási tényezők közül, amelyet a felszíni hőmérséklet és páratartalom mérésekből becsülnek. Az előrejelzési modellek általában elég jól illeszkednek a mért értékekre, bár egyes esetekben az eltérés jelentős is lehet, és nem csökkenthető tovább újabb időjárási paraméter modellbe történő beépítése nélkül.

A nedves és a száraz szcintilláció-jelenségek, mint már említettük eltérő tulajdonságokat mutatnak, ezért ké-

zenfekvő, hogy olyan időjárási paramétert válasszunk, amely jellemzi a szcintilláció típusát. A nedves szcintilláció összefügg a megfigyelt felhőképződési adatokkal, különösen a cumulus és a cumulonimbus típusú felhők megjelenésével. Az említett felhőtípusok megjelenési valószínűségének beépítése a modellbe jelentős pontosság-növekedést jelenthet azokban a klimatikus zónákban, ahol a nedves szcintilláció típus nagyobb arányban vesz részt a szcintilláció statisztika összetételében.

A légköri páratartalommal és a felhőképződéssel kapcsolatos adatoknak több forrása lehet. A légköri páratartalom becsülhető atmoszférikus csillapítás méréssel, melyet az égbolt háttérfénylés megfigyelésével végeznek. A felhőadatok, pedig vizuális megfigyelésből, vagy rádiószondás mérésből nyerhetők.

5. A szcintilláció hatása és a védekezési lehetőségek

A műholdas távközlési rendszer a szcintillációt, mint időben véletlenszerűen előforduló fading-et, jelingadozást érzékeli. Ennek hatása a digitális átviteli rendszerekben csomós (börszt) bithibaként jelentkezik, ami a kapcsolat magasabb rétegeiben csomagvesztéssel, sebesség visszaszabályozással, felesleges csomagismétléssel és kapcsolat szakadással járhat még akkor is, ha az átlagos csillapítás megengedné a folyamatos üzemet.

A napjainkban használt digitális átviteli rendszerek időzítései olyanok, hogy a csatorna jellemzőinek másodperc időléptékű ingadozásait nem tudják kompenzálni, mert ez az idő a magasabb rétegű protokollok adaptációjához túl rövid, viszont ahhoz túl hosszú, hogy a fizikai rétegben rendelkezésre álló kompenzációs módszerek hatékonyak lehessenek.

A csomós hibák ellen általában hibajavító kódolással és bit átszövéssel (interleaving) lehet védekezni. A bit átszövés viszont csak akkor lehet hatásos, ha az alatt az idő alatt, amire az átszövés kiterjed, átlagosan kevés bit hibásodik meg; a szcintillációból eredő hibacsomók viszonylag hosszú ideig tartanak (kb. 1 másodperc), ezért ennek többszörösére kellene az átszövést tervezni, hogy az átlagolási hatás érvényesüljön. Az átszövés megvalósításához a készülékekben plusz memóriára van szükség, és az eljárás járulékos késleltetést is okoz. Mivel nem engedhető meg a néhány másodperces plusz késleltetés, így az átszövés és kódolás nem alkalmazható a szcintilláció okozta csomós bithibák ellen.

Tervezési szempontból a szcintillációt sok esetben az esőcsillapításhoz hasonlóan kezelik, és elsősorban a fading-tartalék növelésével védekeznek a hatása ellen. Problémát jelent, hogy a felhőképződéssel és így az esőcsillapítás növekedésével számottevő korrelációt mutat a szcintilláció, ezért a fading tartalék számításánál összegződik a hatása az esőcsillapításával. Az eső és a szcintilláció okozta fading ellen, használhatók az adaptív rendszerek, melyek a teljesítmény, a moduláció vagy a hibajavító kódolás változtatásával próbálják az összeköttetés minőségét (bithibaarány, sebesség) optimalizálni az időben változó csatornajellemzők mellett. Az adaptív rendszerek megvalósításának egyik legkomolyabb korlátja az összeköttetés késleltetése, ami az adaptáció sebességét vagy pontosságát meghatározza.

A terjedési késleltetés geostacionárius műholdas rendszerek esetén összemérhető a szcintilláció csillapítás változási időállandójával, ezért a szcintillációt is figyelembe vevő adaptív rendszerek megvalósítása ebben az esetben nagy körültekintéssel megoldandó technikai feladatot jelent.

Megoldást szolgáltat erre a problémára a fading előrejelzés (predikció) alapján történő adaptáció, melynek hatékonyságát a késleltetés helyett az előrejelzési módszer pontossága korlátozza. További lehetőségként a légkör állapotának, rádiószondás megfigyelésén alapuló megoldás jöhet szóba, amely a troposzféra pillanatnyi páratartalmának jellemzésére alkalmas, és igen jól indikálja a szcintilláció kialakulásának lehetőségét, viszont a földi állomás költségeit számottevően növeli.

Az alacsonypályás rendszerek késleltetése jóval kisebb, így az adaptív módszerek alkalmazása sokkal hatékonyabb lehet, bár a műholdak mozgásából adódó változások is szerepet játszanak a csatorna jellemzőinek alakulásában, így sokkal erőteljesebb változásokhoz kell az adaptív megoldást illeszteni.

Lehetőséget jelentenek még a szcintilláció hatása elleni védekezésben a különböző diverziti eljárások. Ezek közül használható az antenna (tér) diverziti. Az egymástól több mint 10 m-re elhelyezett antennákon már függetlennek tekinthető a szcintilláció-fading pillanatnyi értéke, ami a diverziti hatásosságának a feltétele. Ez a módszer nem alkalmazható az olcsóbb vagy kis méretű földi állomásoknál.

Drágább eljárás a műhold diverziti, melyben a földi állomás több műholddal kommunikálhat. Ez a lehetőség a geostacionárius (GEO) rendszereknél közel megkétszerezi a költséget, viszont az alacsonypályás (LEO) rendszerekben már a műholdpályák és a műholdszám tervezésénél figyelembe vehető ez a lehetőség.

Az egyes alacsonypályás műholdak a keringési pályájukon mozogva csak az idő egy részében láthatók, tehát ha folyamatos kapcsolattartásra kívánjuk tervezni a rendszert, a műholdváltást (handover) mindenképpen meg kell oldani, és ez már egyszerű műhold diverziti eljárásnak tekinthető. Ha a rendszer átkapcsoláskor a láthatóság mellett a várható szcintillációt is figyelembe veszi, akkor kisebb költségnövekedéssel is hatékony megoldást alkalmazhatunk a szcintilláció-fading ellen.

Az alacsony csillapítás tartalékkal, illetve kíváló használhatóságra tervezett műholdas rendszerek átviteli minősége érzékenyen reagál a szcintilláció-fadingre, ezért az ilyen rendszerek tervezésekor a szcintilláció hatása semmiképpen sem hagyható figyelmen kívül.

6. Következtetések

A műholdas távközlésben a kisugárzott teljesítmény növelése a műhold energiaellátásának, termikus és szerkezeti terveinek átdolgozását is eredményezheti, ezért a fading tartalék tervezésekor sokkal kevésbé lehet a decibelekkel szabadon gazdálkodni, mint a földi rendszereknél. A műhold-Föld összeköttetések esetén nagyon fontos a csatorna jellemzőinek lehető legpontosabb előrejelzése és statisztikai paramétereinek ismerete, mert enélkül nem teljesíthetők egyszerre a pénzügyi és a technikai specifikációban adott minőségi elvárások.

Bár a szcintilláció okozta csillapítás ingadozás általában nem túl nagy (néhány dB), de ez is kapcsolatkiesést és éves szinten 0.1-1% körüli használhatóságcsökkenést eredményezhet, ha a csillapítástartalék túl alacsony. Ezt a felhasználó több, néhány óráig tartó kapcsolat szakadásként érzékeli, ami a rendszer használhatóságának megítélését rontja.

Digitális átviteli rendszerek esetén további problémát jelent a szcintilláció 1 másodperc körüli időléptéke, mert az ilyen változási sebességű átviteli minőség ingadozást jelenleg egyik protokoll rétegben sem lehet hatékonyan kompenzálni. Jelentős előrelépést jelenthet a protokoll rétegek közötti kommunikáció új modelljének kifejlesztése, melynek segítségével a rétegek összehangolt, optimális kompenzációs stratégiát követhetnek ilyen esetekben.

Irodalom

[1] ITU-RP. 618 ajánlás:
„Propagation Data and Prediction Methods Required for the Design of Earth-Space Telecommunication Systems”

[2] Kassianides C. and Otung I. E.:
„A Dynamic Model Of Tropospheric Scintillation”,
COST 255 Final Report on Radiowave Propagation Modeling for SatCom Services at Ku-band, 1998.

[3] Jouni K. Tervonen, Max M. J. L. van de Kamp and Erkki T. Salonen:
„Prediction Model for the Diurnal Behavior of the Tropospheric Scintillation Variance”,
IEEE Transactions on Antennas and Propagation, Vol. 46, No.9, September 1998.

[4] Nedo Celandroni and Francesco Potorti:
„Modeling Ka-Band Scintillation as a Fractal Process”,
IEEE Journal on Selected Areas in Communications, Vol. 17, No.2, February 1999.

[5] ITU-R P.453-6 ajánlás:
„The Radio Refractive Index: Its Formula and Refractivity Data”

[6] Maximilianus Maria Josephus Leonardus van de Kamp:
„Climatic Radiowave Propagation Models for the design of Satellite Communication Systems”,
PhD Thesis 1999, Technische Universiteit Eindhoven

[7] Y. Karasawa, M. Yamada and J.E. Allnutt:
„A new prediction method for tropospheric scintillation on earth-space paths”,
IEEE Transactions on Antennas and Propagation, Vol. 36, November 1988, pp.1608-1614.

Hírek

Optimal Business Routing rendszer az Ericssontól

A távközlési piac szabályozása óta megvalósult összekapcsolások száma és az összekapcsolási szerződések komplexitása most érett meg arra, hogy a bemutatott megoldás vezetés-, illetve mobilszolgáltatók részére egyaránt érdekessé válhat. A szabad összekapcsolás és hívástovábbítás lehetősége egy új ágazat kialakulását eredményezte: a közvetítő (broker) szerepre szakosodott szolgáltatók a forgalmat optimális úton továbbítják a különböző hálózatokba.

Az Ericsson új megoldást kínál az összekapcsolási szolgáltatások gazdaságosabb kezelésére: az Optimal Business Routing (OBR) hatékonyan hidalja át az összekapcsolás kereskedelmi (számlázás, elszámolás) és hálózatvezérlési területei közötti rést.

Az OBR funkciói:

– Különböző bemeneti adatok, például a hívás percdíja, a minőség, a kapacitás, a vállalt forgalommennyiség vagy egyéb preferenciák alapján optimális irányítási tervet készít.
– Az irányítási tervet letölti a hálózatelemekbe (telefonközpontokba).
– Monitorozza az irányítási terv hatékonyságát, minőségét.
– Menedzseli, szükség esetén módosítja az irányítási tervet.
– Támogatja a perckereskedelemhez kapcsolódó pénzügyi döntéseket: az ajánlati árszintek kialakítását és az ehhez tartozó költségek meghatározását.

Egységes távközlés a különböző infrastruktúrájú hálózatokon

ERDÉLYI TIBOR

BME, Automatizálási és Alkalmazott Informatikai Tanszék
erdelyi.tibor@aut.bme.hu

Kulcsszavak: SIP, ENUM, hálózat-irányítás, mobil hálózat

A távközlés fejlődésének egyik irányvonala az, hogy az Interneten elterjedt, és népszerű szolgáltatások jelennek meg a mobil és vezetékes távközlés világában is. Az egyik ilyen szolgáltatás a SIP, mely lehetővé teszi a felhasználók számára, hogy attól függetlenül, hogy a hívott fél hol tartózkodik, és milyen eszközön érhető el, annak azonosítóját megadva tetszőleges jellegű kommunikációs kapcsolatot létesíthessenek vele. Ez a szolgáltatás azonban akkor válhat igazán erőteljessé, ha az egyes hálózatokon nem külön-külön, hanem egységesen érhető el.

A napjainkban elérhető kommunikációs igényeket alapvetően három, egymástól teljesen különböző infrastruktúrájú hálózat szolgálja ki. A legnagyobb múlttal rendelkező PSTN előnyeként a széles elterjedtsége emelhető ki, míg hátrányaként a régi technológia okozta rugalmatlanság említhető. A közelmúltban megjelent mobil távközlés infrastruktúrája már lényegesen modernebb, ami lehetővé teszi annak folyamatos fejlődését, így évről évre tanúi lehetünk az új szolgáltatások megjelenésének. Itt azonban a szűk sávszélesség korlátozza a lehetőségeket. A legdinamikusabban fejlődő terület mindenképp az Internet, hiszen itt pusztán szoftverek készítésével minden szolgáltatás megvalósítható. Ebben az esetben azonban a kommunikáció minősége (QOS) nem garantálható.

A cikkben egy, a SIP [1] mintáján alapuló egységes kommunikáció jövőképének felvázolását követően annak megvalósításának lehetőségei kerülnek megvizsgálásra az egyes hálózatokban. Végül pedig az egyik legalapvetőbb feladat, az egységes azonosítás megvalósításáról esik részletesebben szó.

1. Jövőkép

Az egységes távközlés jövőképének felvázolása előtt, a jelenlegi problémák hangsúlyozása érdekében tekintsünk egy mindennapos telefonbeszélgetést:

– *Küldtem SMS-t, de nem válaszoltál!*
– *Igen, elfelejtettem. Legközelebb email-t küldj, akkor biztosan válaszolok!*
– *Arra a címre küldjem, ami a névjegykártyádon van?*
– *Nem! Azóta már megváltozott. Mondom…*

A példa három különböző problémára próbálja felhívni a figyelmet:

- Mindenkinek ismernünk kell a preferenciáit, akikkel kapcsolatban állunk, hogy valóban oda, és olyan módon jutassuk el hozzá az információt, ahogyan ő elvárja.
- Nem tudhatjuk, hogy a másik fél éppen hol tartózkodik, ezért különböző módokon kell próbálkoznunk ahhoz, hogy elérjük.
- A különböző jellegű kapcsolatok felépítéséhez különböző azonosítókat kell megjegyeznünk, melyek gyakran meg is változhatnak.

Egy ideális távközlési hálózatban tehát a kapcsolat felépítéséhez csak arra volna szükség, hogy a hívott fél egyetlen és egységes azonosítását követően megadjuk, hogy milyen jellegű kapcsolatba kívánunk lépni vele (beszélgetés, üzenetküldés stb.), ezt követően a rendszer automatikusan ismerné a hívott fél állapotát. (Be van-e kapcsolva a mobiltelefonja, külföldön tartózkodik-e, be van-e jelentkezve a csevegő programjába stb.) Majd az általa beállított preferenciák szerint döntene, hogy milyen címen található és milyen eszközzel építi fel a kapcsolatot. Természetesen ezt a felhasználó egyaránt megtehetné, ha egy számítógép előtt ül, ha egy hagyományos telefonkészüléket használ, vagy ha egy mobil telefont tart a kezében.

Rövidítések

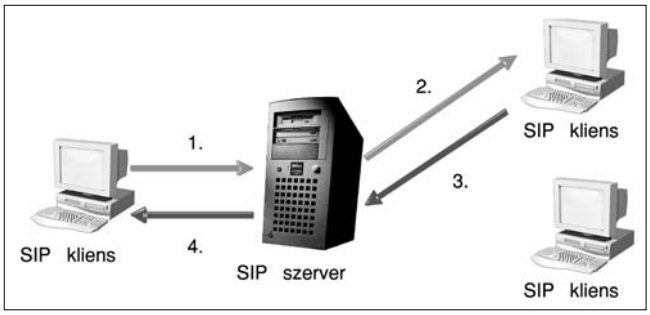
DNS	Domain Name Server
ENUM	Electronic Number
FCC	Federal Communications Commission
HLR	Home Location Register
IMS	IP Multimedia Subsystem
LNDB	Local Number Portability Database
LSMS	Local Service Management System
NAPTR	Naming Authority Pointer
NPAC	Number Portability Administration Center
PSTN	Public Switched Telephone Network
QOS	Quality of Service
SCP	Service Control Point
SIP	Session Instantiation Protocol
URI	Universal Resource Identifier
SOA	Service Order Administration
VLR	Visitor Location Register

2. A jelenlegi infrastruktúra

Természetesen a fent leírtak inkább csak víziónak tekinthetőek, mintsem a közeljövő egy reális céljának. A megvalósítás lehetősége azonban mindhárom hálózaton adott.

Internet

Az Internet bárki által hozzáférhető, és használatának lehetőségeit szinte semmi sem korlátozza. Nem véletlen tehát, hogy a SIP protokoll elsőként itt jelent meg. Ennek működési elve igen egyszerű: A kliensek adott időközönként üzeneteket küldenek egy jól meghatározott szerver felé, mely így nyilvántarthatja, hogy egy adott pillanatban mely felhasználó érhető el, és hol. A kapcsolat felépítéséhez a kliens egy üzenetet küld a szerverhez, mely ha jelenleg elérhető a hívott fél, akkor a megfelelő eszközhöz juttatja el az üzenetet, ellenkező esetben pedig a felhasználó beállításainak megfelelően vagy visszautasítja a kérést, vagy más irányba továbbítja azt (PSTN átjáró felé, egy adott telefonszámra, üzenetrögzítő klienshez, hanglevelet küldő klienshez...).



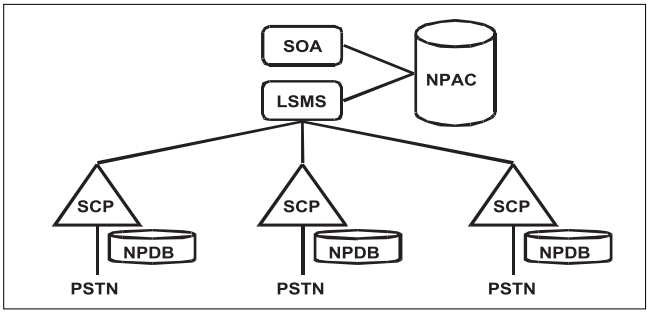
Az Internet világában felvázolt jövőkép tehát már maga a jelen. A SIP vállalaton belül, és világméretekben egyaránt elterjedt. Azonban utóbbi is egy teljesen központosított megoldás, mert noha a SIP lehetővé teszi, hogy a szerverek az üzeneteket egymás felé továbbítsák, az Internet infrastruktúrája lehetővé teszi, hogy egyetlen szerver (vagy egyetlen címen elérhető szerver farm) szolgálja ki a világméretű igényeket. Természetesen a Interneten bármely más topológia is egyszerűen megvalósítható volna, így a központosított megoldás elterjedése a SIP működésében keresendő: Az üzenetek irányításához a felhasználók aktuális állapotának ismerete szükséges, melynek legegyszerűbb magvalósítása az adatokat tároló egyetlen szerver.

PSTN

A SIP működési elvéhez a központosított topológiák lényegesen jobban illeszkednek, mint az elosztottak, hiszen működéséhez az szükséges, hogy a csomópontok egy gyakran változó tartalmú adatbázishoz (állapotinformációkhoz) férjenek hozzá. Egy elosztott környezetben pedig komolyabb időt emésztene fel annak felderítése, hogy az adott információ melyik csomóponton férhető hozzá. A hagyományos telefonhálózat azonban teljesen elosztottan működik, így annak érdekében, hogy minden hívás felépítésében részt vegyen egy olyan csomópont, mely támogatja a SIP-nek megfelelő működést, minden egyes helyi központot le kellene cserélni (a helyi hívások csak ezeket érintik), ami mérhetetlen költségeket róna a szolgáltatókra.

Egy szerencsés véletlennek köszönhetően azonban a közelmúltban az Egyesült Államokban, és Európa sok országában a távközlési szolgáltatóknak külső kényszer hatására kellett valamelyest centralizálttá átalakítaniuk hálózatukat. A távközlési piac liberalizációjának elősegítése érdekében ugyanis állami kezdeményezésre indult meg a számhordozhatóság megvalósítása, mely a SIP-hez hasonlóan egyfajta centralizált működést követelt meg. Az Egyesült Államokban például a FCC 1996-ban rendelte el a számhordozhatóság megvalósítását, mely 1997-re készült el. Az átállás nagyságrendjét jelzi, hogy a költségek több mint 3 milliárd dollárt emésztettek fel. Minden bizonnyal ez volt tehát a legnagyobb átalakítás a PSTN-en fennállása óta.

A számhordozhatóság megvalósításában a központi szerepet egy szolgáltató független, központi adatbázis játssza, a NPAC. Ez minden ügyfél megtalálásához tartalmazza a szükséges információkat. Karbantartása a SOA segítségével végezhető el. Az egyes szolgáltatók az LSMS segítségével kapcsolódhatnak ehhez az adatbázishoz, és kérdezhetik le az abban található információkat. A szolgáltatók azonban egy saját adatbázissal is rendelkeznek, LNDB-vel, melynek tartalmát az SCP frissíti az LSMS segítségével. Az egyes szolgáltatók PSTN hálózata és a szolgáltatóktól független adathálózat között az SCP-k teremtik meg a kapcsolatot.



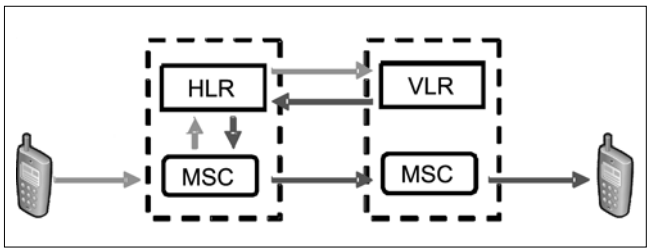
Végeredményben tehát a PSTN olyan változáson ment át, melynek köszönhetően mégis alkalmassá vált arra, hogy a felvázolt jövőképhez hasonlóan működjön. A felhasználók aktuális állapotának nyilvántartása, és a számhordozhatóság igen hasonló problémák, hiszen az, hogy az adott ügyfél mely szolgáltatónál, és milyen számon érhető el, szintén egyfajta állapot. Ennek köszönhetően a SIP szerű működés egy kisebb változtatással, az SCP-k cseréjével megoldható.

Mobil hálózatok

A Mobil hálózatokat a vizsgálat szempontjából mindenképp ketté kell választanunk, mert noha napjainkban a második generációs (2G) hálózatok terjedtek el, technológiailag már a két és feledik (2.5G), illetve harmadik generációs (3G) változatok is kiforrottak.

A GSM hálózatok esetében külön problémát okoz az, hogy a hívott fél helye megváltozhat, ezért egy adott telefonszámra kezdeményezett hívást ennek megfelelően esetleg teljesen más irányba kell továbbítani. Ez a probléma eleve elveti annak a lehetőségét, hogy a hálózat a PSTN-hez hasonlóan működjön. Mindenképpen szükséges tehát, hogy a hívás felépítésében részt vegyen egy olyan egység is, mely a felhasználók adataihoz (mely tartalmazza azok aktuális állapotát is) hozzáfér. A GSM hálózatok esetében ez a HLR.

Az Internet esetével ellentétben azonban itt nem oldható meg, hogy a Föld minden előfizetője egyetlen központhoz kapcsolódjon, az egyes földrajzi területek infrastruktúráját ugyanis más-más szolgáltató alakította ki. Ahhoz tehát, hogy egy ügyfél akkor is elérhető legyen, ha egy másik szolgáltató hálózatára jelentkezett be (például mert külföldön tartózkodik), az egyes szolgáltatók együttműködése szükséges. Ezért ebben az esetben az előfizető helyzetét az idegen hálózat központja, a VLR tartja nyilván, mely bejelentkezéskor értesíti a HLR-t. Az ügyfél megkeresését a HLR úgy végzi el, hogy kapcsolatba lép az illetékes VLR-el.



A SIP működésébe illeszkedő központosított architektúra tehát a mobil hálózatok esetében technológiai adottság. Az előfizetőket nyilvántartó HLR pedig alapvetően ugyanazt a szerepet tölti be, mint a SIP szerver. A felhasználók aktuális helyzete igen sűrűn változhat, ezért az itt kialakult infrastruktúra lehetővé teszi, hogy a HLR adatai percről percre változzanak.

Az következő generációs (2.5G és 3G) mobil hálózatok újítása, hogy a hang mellett adat kommunikációt is lehetővé tesznek. Ennek egyik lehetséges felhasználási területe az, hogy különböző típusú híranyagokat (beszéd, szöveg küldés, kép küldés, csevegés stb.) vihetünk át egyazon felépült kapcsolaton. A rohamosan fejlődő mobil készülékek pedig már most képesek ezen információk jelentős részének átvitelére. Természetesen a szolgáltatások értékesebbel, ha a multimédia kapcsolatok nem pusztán mobil telefonokkal, hanem más kliensekkel – például Interneten elérhető számítógépekkel – is felépíthetőek.

Egy a 3GPP keretein belül indított projekt, az IMS [3] éppen ezt tűzte ki célul. Az IMS működése egyaránt beilleszkedik az Internet és a mobil hálózatok világába is. A HLR és a VLR szerepében itt is megtalálható egy-egy komponens. Ezek azonban már SIP szerverek, és mind a végberendezéssel, mind egymással a SIP protokollon kommunikálnak. A következő generációs mobil hálózatok tehát már be tudnak illeszkedni a SIP világába, annak minden előnyével együtt.

3. A hívott fél egységes azonosítása – az ENUM

A továbbiakban egy olyan kezdeményezéssel foglalkozunk, mely elengedhetetlen ahhoz, hogy az adott három hálózatot a megfelelő módon összekapcsoljuk, és egyúttal az első részben felvázolt három problémából kettőt meg is old.

Ahhoz, hogy a hívott felet úgy érhessük el, hogy nem tudjuk milyen hálózatban fog végződni a hívás, mindenképpen szükséges egy olyan azonosító, melyet minden hálózat megért. Az azonosító formátumát a PSTN végberendezések korlátozzák a leginkább. Ezek segítségével rendszerint csak számok adhatóak meg, így kézenfekvő, hogy az azonosításra egy E.164 telefonszámot használjunk. Ezt az azonosítót felhasználva már a felépítendő kapcsolat típusától függően – egy elosztott adatbázis segítségével – meghatározható az adott hálózatnak megfelelő más formátumú cím.

Ez a működési elv egyúttal lehetővé teszi azt is, hogy az elosztott adatbázis a felhasználó preferenciáit is tartalmazza (noha ezek nem függhetnek az aktuális állapottól). Így az ügyfélspecifikus irányítás is megoldható.

Az ENUM tehát az Interneten bárhonnan elérhető címtárszolgáltatás, a DNS segítségével teszi lehetővé az E.164 telefonszámok hálózatfüggő címmé alakítását [10].

A DNS mint elosztott adatbázis

Az azonosítók átalakítására mindenképp szükséges egy olyan adathálózat, mely a Föld minden részén hozzáférhető. Szerencsére az egyetlen ilyen hálózaton, az Interneten egyúttal meg is található egy olyan általános címtárszolgáltatás, mely kulcsok (nevek) és értékek összerendelését, és az értékek kulcs szerinti lekérdezését teszi lehetővé ebben az elosztott környezetben. A DNS legfontosabb feladata, hogy a felhasználók által megjegyezhető tartományneveket a csomópontok azonosítására szolgáló IP címekké alakítsa át. Az ENUM azonban lehetőségeit arra használja, hogy felhasználók azonosítója alapján határozza meg azok címeit a különböző hálózatokon.

A DNS egyik speciális bejegyzés típusa az NAPTR [7]. Ennek érdekessége, hogy több sort is tartalmaz, melyekhez különböző protokollok tartozhatnak. A visszakapott sorok sorrendjéből az ENUM esetében meghatározhatóak az ügyfél preferenciái, így annak megfelelő sorrendben kezdődhet meg a próbálkozás a kapcsolat felépítésére. Az egyes sorok pedig tartalmazzák a protokollt, melyből meghatározható, hogy mely hálózatba illetve milyen címre kell továbbítani a hívást.

Az NAPTR rekordok a fentieken túl tartalmaznak egy-egy reguláris kifejezést is. Mivel DNS lekérdezések teljes tartományokra is végezhetőek, így megoldható az is, hogy egy-egy teljes telefonszám tartományhoz tartozzon egy bejegyzés. Ebben az esetben a reguláris kifejezés segítségével határozható meg, hogy az adott számra melyik sor érvényes.

Telefonszám – URI átalakítás

Az előző részben leírt működés feltételezi, hogy a hívott fél adatait egy a DNS adatbázis által elvárt tartománynév alapján kérdezzük le, a valóságban azonban egy telefonszám áll a rendelkezésünkre. Ezért az ENUM egyértelműen definiálja az átalakítás algoritmusát [8] :

1.) Minden karakter eltávolítása, mely nem számjegy.
2.) Pontok elhelyezése a szomszédos számjegyek között.
3.) A számjegyek sorrendjének megfordítása.
4.) Az „e164.arpa" végződés elhelyezése a kapott azonosító végén.

Az algoritmus tehát a +36-1-1234567 telefonszámhoz a „7.6.5.4.3.2.1.1.6.3.e164.arpa.net" DNS nevet rendeli.

A fent leírt lépések alapvetően formai átalakításokat definiálnak, a harmadik pont azonban az E.164 számok hierarchikus jelentését tartja meg a DNS hasonló felépítésében is. Ennek köszönhető, hogy logikus tartományokhoz – például adott országokhoz – is tartozhatnak DNS bejegyzések.

4. Összegzés

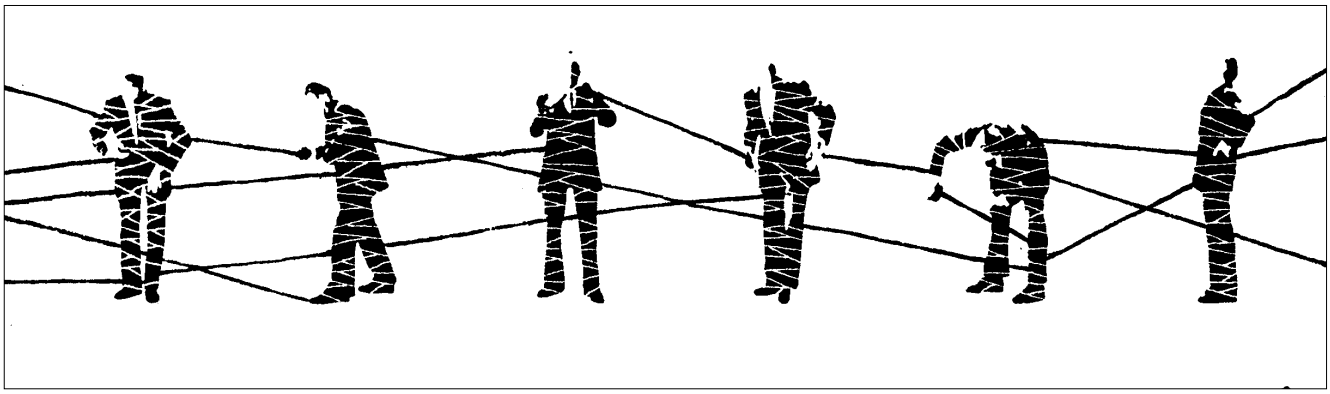
Az ismertetett három távközlési hálózat struktúrája és működési elve tehát egyaránt lehetővé teszi az egységes azonosítók használatát, mivel mindegyik esetben központi szerepben található az a komponens, mely meghatározza, hogy ténylegesen mely végponttal épül fel a kapcsolat. Az Internet, a PSTN és a mobil hálózatok esetében ez a komponens rendre a SIP szerver, az SCP illetve a HLR. Az egységes azonosítás megvalósításához tehát elégséges az, hogy ezek a komponensek az ENUM előírásainak megfelelően működjenek.

Az ENUM egyúttal lehetővé teszi azt is, hogy egy adott ügyfél hívásakor a kapcsolat felépítésére az általa megadott szabályok szerint kerüljön sor. Az ügyfél aktuális állapotának vizsgálata ezekben a szabályokban még nem megoldott. (A DNS rekordok csak nagy átfutási idővel frissíthetőek.) Amennyiben azonban ez az állapot információ egyetlen szerveren van, akkor a probléma egy újabb lépés segítségével, a mobil hálózatok mintájára megoldható: A DNS lekérdezésből meghatározható az állapotot tároló szerver, melytől egy újabb lépésben megtudható az aktuális állapot. Mivel a PSTN hálózat nem tárol ilyen információkat, ezért IMS-t feltételezve, ez elérhető azáltal, ha a felhasználók az Internetről is a mobil szolgáltatójuk SIP szerveréhez csatlakoznak.

Természetesen az ENUM csak a felmerülő problémák egy részét oldja meg. A hívott fél megfelelő címének meghatározását követően a kapcsolat felépítése újabb problémákat rejt magában. (Például Internetről kezdeményezett hívás esetén mely átjárón kerüljön át a hívás a PSTN vagy mobil hálózatba?) További kérdés emellett az is, hogy a DNS a hatékonyság és adminisztráció szempontjából ténylegesen alkalmas lesz-e ezen feladat ellátására. Végezetül pedig a hívás számlázása is gondot okoz, hiszen a hívó fél nem tudhatja, hogy mely hálózattal lépül fel a kapcsolat, így nem lehet tisztában annak költségével sem.

Irodalom

[1] RFC 3261: Session Initiation Protocol
[2] Nicklas Beijar: TRIP, ENUM and Number Portability
[3] Michael Tadault, Laurent Thiébaut, Sajid Soormally: Network Evolution towards IP Multimedia Subsystem
[4] Rebecca A. Stillings, Robert M. Wienski: Number Portability in Next Generation Networks
[5] Jonathan Lennox, Kazutaka Murakami, Mehmet Karaul, Thomas F. La Porta: Interworking Internet Telephony and Wireless Telecommunications Networks
[6] Qi Wang, Mosa Ali Abu-Rgheff: Towards a Complete Solution to Mobility Management for Next-Generation Wireless System
[7] RFC 2915: The Naming Authority Pointer (NAPTR) DNS Resource Record
[8] RFC 2916: E.164 number and DNS
[9] 3GPP R5 Requirements on SIP (Internet draft)
[10] Gódor Balázs: Térjünk át az ENUM-ra! Híradástechnika, 2004/4.



Térjünk át az ENUM-ra!

GÓDOR BALÁZS

MATÁV PKI, Fejlesztési Intézet
godor.balazs@ln.matav.hu

Kulcsszavak: címzés, szolgáltatások együttműködése, személyiségi jogok

A számítástechnika és a távközlés fejlődésével egyre több olyan elektronikus szolgáltatás létezik, melyek könnyebbé teszik az emberek közötti kommunikációt. Ilyenek például a beszédszolgáltatás fix, mobil-, vagy IP hálózaton, az elektronikus postafiók, az SMS, MMS, fax, vagy az a chatelést lehetővé tevő szolgáltatás. A felsorolt szolgáltatások felfoghatók a felhasználónak egy-egy elérési pontjaként. A különböző elérési pontokra azonban gyakran különféleképpen lehet hivatkozni. Ez azt jelenti, hogy egy elektronikus levelet például másképp kell címezni, mint egy SMS-t. Ez sok esetben kivitelezhetetlen, mert így akár 5-10 címet is fel kellene tünteni, melyek bármelyikének változását közzé kell tenni. Az ENUM felhasználásával ez a probléma egyszerűen megoldható és még sok más új lehetőséget is kínál. Felmerül azonban a kérdés, hogy ha az ENUM a fenti problémát egyszerűen orvosolja, miért nem terjedt még el. Erre a kérdésre keresi a cikk a választ.

Az ENUM [2] elnevezés, felsorolásra, enumerációra utal és egyúttal egy betűszó is: tElephone NUmber Mapping (telefonszám leképezés). Az ENUM célja, hogy telefonszámokból DNS neveket képezzünk, a DNS nevek pedig eligazítást adjanak arra nézve, hogy a hívott milyen módokon érhető el. A lehetséges elérési módok egyike a SIP protokollal történő címzés, de megadható egy mobil telefonszám, vagy akár egy elektronikus levélcím is. Az ENUM nem egy klasszikus értelemben vett protokoll, ami definíció szerint a kommunikáció üzenetformátumait rögzíti. Az ENUM meglévő protokollok és adatstruktúrák egy lehetséges felhasználási módját határozza meg [3].

Ezek a következők:

- E.164-es számok és az “e164.arpa” domain (IAB: RFC3172) [4];
- a DNS protokoll (RFC1034/35) [5] [6];
- NAPTR Resource Rekordok (RFC2915) [7];
- NAPTR kérésekre adott URI válaszok értelmezése (RFC2396) [8]

ENUM-mal tehát egy olyan IP alapú szolgáltatás valósítható meg, ahol az előfizetőnek csupán egy azonosítót (praktikusan egy E.164-es számot) kell nyilvánossá tennie, s ez mutatóként szolgál az összes elérési címére. Az ENUM által használt E.164-es szám tehát nem egy univerzális cím, hanem egy olyan azonosító, mely által címekhez lehet hozzáférni.

Kijelenthető, hogy az ENUM kulcsfontosságú az IP hálózatok és a távközlő hálózatok (PSTN, GSM) közötti konvergenciában. Előmozdíthatja az IP telefónia fejlődését, mert a felhasználók jelezni tudják, hogy milyen hálózati csatornákon érhetők el, és a hívó kiválaszthatja a számára legmegfelelőbb (legolcsóbb, legjobb minőségű, leggyorsabb stb.) elérési módot. [3] A platformfüggetlen címzési rendszer az egységes távközlés jövőképét vetíti előre [21].

Az ENUM feladata röviden a következő két pontban foglalható össze [9]:

1) Egyes hálózati elemek (IP-PSTN átjárók, SIP szerverek) miként találnak meg bizonyos szolgáltatásokat az Interneten, ha csupán egy telefonszám (E.164-es cím) áll rendelkezésükre
2) Az előfizetők hogyan határozhatják meg, hogy bizonyos, feléjük irányuló forgalmi, kapcsolati kérések mely szolgáltatások és szerverek igénybevételével szolgálhatók ki.

Megjegyzendő, hogy az ENUM bevezetése önmagában nem indokol semmiféle változtatást a nemzeti számozási tervben és nem igényel semmilyen extra számozási erőforrást. Az ENUM-ban rejlő új lehetőségek kiaknázása során azonban felmerülhet igény további E.164-es számok iránt [1].

Az ENUM szó önmagában nem elég kifejező a cikk tartalmát illetően. Az ENUM ugyanis három különböző modellben is értelmezhető. Ezeket felhasználói, operátor és infrastrukturális ENUM-ként nevezik. *Felhasználói (user vagy subscriber) ENUM* esetében a hierarchikus szervezésű elosztott (DNS) adatbázisban felhasználói adatokat tárolnak. A hierarchia tetején a .e164.arpa tartomány található. *Operator ENUM* esetén a hierarchikus szervezésű elosztott adatbázis (továbbiakban egyszerűen adatbázis) például egy nagyobb cég belső hálózatában kerülhet megvalósításra, így a nyilvánosan nem hozzáférhető, és gyökerét nem a nyilvános .e164.arpa tartomány alkotja. *Infrastrukturális (infrastructure) ENUM* esetében az adatbázisban nem felhasználói adatokat tárolnak, hanem olyan adatokat, melyek forgalomirányításoz, a számhordozhatóság megvalósításához, zöld szám és más IN jellegű, szám vagy cím feldolgozást igénylő feladatok elvégzéséhez szükségesek. A cikk ezek közül egyedül a felhasználói ENUM-mal foglalkozik.

SIP vagy ENUM?

Cikkekben vagy szakmai vitákon gyakran hangzik el a fenti kérdés implicit vagy explicit módon. Melyik a jobb? A kérdést azonban nem lehet megválaszolni, mert a SIP és ENUM nem alternatívái egymásnak. Míg a SIP egy protokoll, az ENUM nem az, mint azt korábban már tisztáztuk. A konfúzióra az adhat okot, hogy adott esetben SIP alapú VoIP rendszerekben ENUM nélkül is lehet E.164-es számokat használni. Lehet E.164-es számokkal IP-ből hívást kezdeményezni IP-be, PSTN-be és lehet a PSTN-ből is IP-be. Ekkor a SIP szerver (proxy) képezi le az E.164-es számokat, IP címekre. A dolog szépséghibája csupán annyi, hogy ez a megoldás nem skálázható, és csak specifikus esetekben működik. Az IP telefonok közötti (tisztán IP-s) E.164-es számokkal való hívásra például csak akkor van lehetőség, ha a két végpont ugyanannál az IP-beli intelligens eszköznél (H.323 gatekeeper, SIP proxy, SoftSwitch stb. – a továbbiakban kiszolgáló) regisztrálta magát. Jelenleg ugyanis nem létezik olyan protokoll, mely az egyes kiszolgálók között az IP cím és E.164-es számok közötti leképezések terjesztésére alkalmas volna.[10]

ENUM használata esetén továbbá nem csupán SIP alapú szolgáltatások érhetők el, hanem más protokollokon alapuló szolgáltatások is. Erről bővebben egy Internet-Draft [11] ad felvilágosítást, mely részletesen taglalja, hogy egy E.164-es számhoz milyen szolgáltatások regisztrálhatók az ENUM által használt DNS adatbázisban található NAPTR rekordokban [7] [12].

DNS – az egyetlen megoldás?

A DNS [5] [6] egy hierarchikus szervezésű elosztott adatbázis. Ezt elsősorban az Interneten használják, tartomány (domain) nevek és IP címek közötti leképezésre. Az információ alapeleme a DNS-ben az erőforrás rekord (RR = Resource Record).

Ennek több fajtája is létezik, de az ENUM működése szempontjából egyik kiemelendő típus a NAPTR (Naming Authority Pointer) RR [7]. Ez egy reguláris kifejezésen alapuló feldolgozó szabályt fogalmaz meg, mely által egy bemenő karaktersorozatból (pl. tartománynévből) új tartománynév vagy URI [8] képezhető. Itt tárolják az egyes telefonszámokhoz tartozó szolgáltatások

DNS	Domain Name System	Tartománynév rendszer
DNSSEC	DNS Security Extensions	DNS biztonsági kiterjesztés
DoS	Denial of Service	Szolgáltatás megtagadás
E2U	ENUM to URI	ENUM leképezése URI-vá
ENUM	tElephone NUmber Mapping	Telefonszám leképezés
ETSI	European Telecommunications Standards Institute	Európai Távközlési Szabványosítási Intézet
GSM	Global System for Mobile Communication	Mobilkommunikációs globális rendszer
IN	Inelligent Network	Intelligens hálózat
IP	Internet Protocol	Internet protokoll
ITU	International Telecommunication Union	Nemzetközi Távközlési Egyesület
MMS	Multimedia Messaging Service	Multimédiás Üzenetküld_ Szolgáltatás
NAPTR	Naming Authority Pointer	Névfeloldás mutató
PINT	PSTN/Internet Interworking Service	PSTN/Internet együttm_ködési szolgáltatás
PKI	Public Key Infrastructure	Nyilvános kulcsú titkosítás infrastruktúrája
PLMN	Public Land Mobile Network	Nyilvános Mobil hálózat
PSTN	Public Switched Telephone Network	Nyilvános kapcsolt telefonhálózat
RR	Resource Record	Er_forrás rekord
SCN	Switched Circuit Network	Vonalkapcsolt hálózat
SIGTRAN	Signaling Transport	Jelzés átvitel
SIP	Session Initiation Protocol	Viszony kezdeményez_ protokoll
SMS	Short Message Service	Rövid szöveges üzenet
SPAN	Services and Protocols for Advanced Networks	Szolgáltatások és Protokollok Speciális Hálózatokhoz
SPIRITS	Service in the PSTN/IN Requesting Internet Service	Internet szolgáltatást igénybe vev_ PSTN/IN szolgáltatás
SS7	Signaling System 7	7-es jelzésrendszer
TIPHON	Telecommunications and Internet Protocol Harmonization over Networks	Telekommunikációs és Internet Protokoll harmonizáció
TISPAN	SPAN+TIPHON	SPAN+TIPHON
TRIP	Telephony routing over IP	Telefonos jelzések forgalomirányítása IP felett
TSIG	Secret Key Transaction Authentication for DNS	Titkos kulcsú azonosítás a DNS-ben
URI	Universal Resource Identifier	Általános er_forrás Azonosító

listáját is. (Az ENUM új szolgáltatást definiál „E.164 to URI” néven, amely egy E.164-es számhoz egy URI listát rendel. Ennek rövidítése E2U.)

Adott telefonszámhoz regisztrált szolgáltatások listájához az ENUM RFC-ben [2] definiált algoritmus alkalmazása után lehet hozzáférni. Eszerint az E.164-es telefonszámokból tartománynevet képeznek az alábbi módon. Megfordítják a telefonszám számjegyeit, közéjük pontok kerülnek, az így képzett tartománynév végére pedig az ’.e164.arpa’ sztring írandó. Példaképpen tehát a +36-1-234-5678 telefonszámból a következő tartománynév képződik:

8.7.6.5.4.3.2.1.6.3.e164.arpa.

Ehhez a tartománynévhez tartozó szolgáltatások a DNS adatbázisból kérdezhetők le. A lekérdezés eredménye a NAPTR rekordokban megfogalmazott sztring transzformációs szabályok alkalmazása során keletkező egy vagy több URI, mely egy vagy több szolgáltatást jelöl meg. A kimenetként előálló URI lista feldolgozási sorrendje a NAPTR rekordban található.

A DNS névszervereinek használata telefonszámok tárolására kézenfekvő megoldás, hisz a DNS egy olyan elosztott adatbázis, mely nyilvánosan elérhető bárhol a világon, ahol az Internet hozzáférés biztosított. Kérdéses azonban, hogy mennyire közelíti az optimálist a DNS ilyen célú felhasználása. DNS-sel kapcsolatban az alábbi problémák merülnek fel [16]:

– Nem biztonságos.
  TSIG [13], DNSSEC [14], PKI [15], biztonságosabbá teheti a DNS-t – kérdés, hogy mennyire. Kérdés továbbá, hogy milyen többletráfordítást (overhead) jelent alkalmazásuk és mennyire kiforrottak ezek a technikák.
– Nincs jól karbantartva, sem jól szinkronizálva.
– „Nem mond nemet” – holtidőn (timeout) túli válasz elmaradás jelenti a ’nemet’.
– Konvergenciája lassú.

Megjegyzés: ENUM-nak csak azt a rendszert nevezik, ahol a hierarchikus DNS adatbázis gyökere az .e164.arpa. Egyéb megvalósításokra ENUM-szerű rendszerként (ENUM-like system) hivatkoznak.

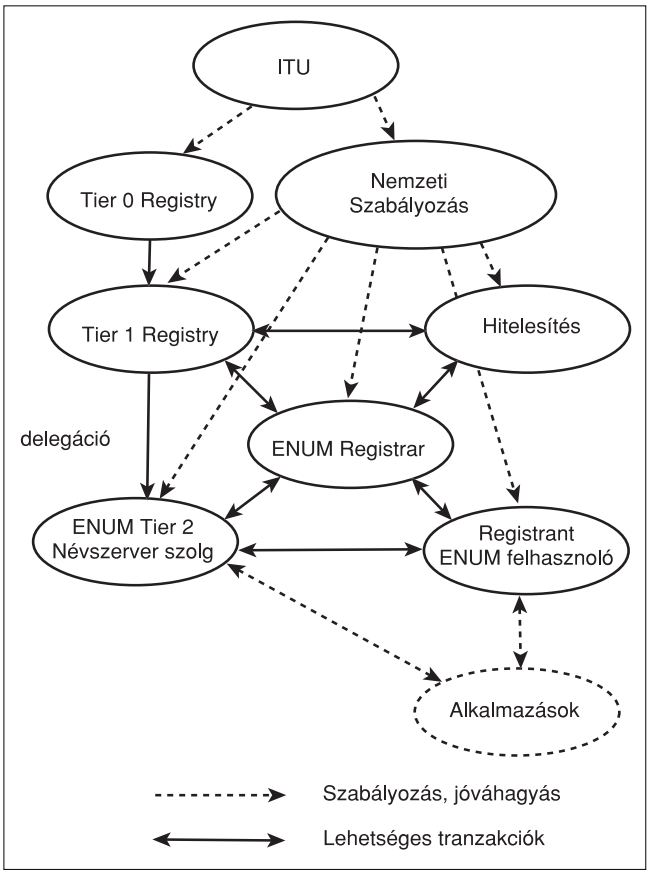
ENUM adminisztráció

Az *ábrán* látható az ENUM referencia modellje [1]. Az ábra megértéséhez szükséges egyes elemek definiálása.

Tier: Nyilvántartási szint

Registry (nyilvántartó): Az a logikai egység, amely birtokolja a regisztert (register). A regiszterben fel van sorolva az összes tartománynév, melyeket adott tartományon belül regisztráltak. A tartomány (domain) műszaki felelőse (technical contact) betöltheti a nyilvántartó szerepét. Ő felelős a tartomány névszervereinek működtetéséért is. [1]

Registrar: Az a logikai egység, amely egy tartományon belül a tartománynév kérelmeket kezeli. A nyilvántartó és a tartománynév birtokosa (Registrant) közötti ügynökként is felfogható. [1]



A modell alapja a háromszintű funkcionális tagolás. A szinteket a Tier0, Tier1 és Tier2-nek nevezik. Fő feladat a legfelső (Tier0) szinten az ENUM tartomány adminisztrációja és üzemeltetése. Ezt a feladatot a Tier0 nyilvántartó látja el. Ez egy egyedi nemzetközi nyilvántartó, mely Tier1 szintű nyilvántartókra mutat. A második (Tier1) szinten az E.164-es országkódokhoz tartozó tartomány adminisztrációja a feladat. Hazánk esetében ez a tartomány a .6.3.e164.arpa. Ezt a feladatot a Tier1 nyilvántartó látja el, ami egy nemzeti nyilvántartó és Tier2 szintű névszerver szolgáltatókra mutat. Tier2 szinten a fő feladat az ENUM üzleti funkcióinak megvalósítása. Ez a névszerver szolgáltató felelőssége. Ezen a szinten kell bejegyezni a telefonszámokhoz tartozó szolgáltatásokat. Az ENUM rétegelt modelljének köszönhetően adott telefonszámhoz regisztrált szolgáltatás szolgáltatójának változása nincs hatással a felsőbb rétegek adminisztrációjára [1].

A ’Hitelesítés’ (Validation) címkével ellátott logikai egység felelős azért, hogy az ENUM adatbázisba adatai felvételét kérő személy valóban az, akinek mondja magát. Hitelesítésre nem csak regisztráció esetén van szükség, hanem minden alkalommal, amikor a felhasználó módosítani szeretné a hozzá tartozó NAPTR bejegyzéseket. Fontos, hogy csak az illetékesnek legyen hozzáférése ezekhez az adatokhoz.

Telefonszámot az ENUM adatbázisban kizárólag az előfizető kérésére lehet regisztrálni [1]. Ezt a külföldi szakirodalom ’opt-in principle’ terminológiával illeti. Erre különféle biztonsági és adatvédelmi megfontolásokból van szükség.

Az ENUM bevezetésének veszélyforrásai és kockázati tényezői

Eddig az ENUM-ban rejlő lehetőségről volt szó, azonban ennek a megoldásnak is vannak árnyoldalai.

Minden olyan E.164 számra történő híváskezdeményezés, melyhez tartozik ENUM rekord lehetővé teszi az (hívó) ENUM kliens számára, hogy hozzáférjen a hívott személy összes címéhez és számához (e-mail cím, mobil szám, fax szám stb.) mely az adott személy NAPTR rekordjában rögzítve van. Ennek az a veszélye, hogy egy véletlenszerűen begépelt E.164 szám alapján egy előfizető összes elérhetősége rendelkezésre álljon, s azokat rosszindulatúan használják (például nem kért reklámok nagy mennyiségben való terjesztése). Ez alapján kideríthető, hogy egy ENUM előfizető mely szolgáltatók milyen jellegű szolgáltatásait veszi igénybe, s így konkurens szolgáltatók közvetlenül tehetnek jobb ajánlatot az előfizető által használt szolgáltatásokra. A konkurens szolgáltató ez esetben persze illetéktelenül jut az információhoz [1].

Az ENUM rendszer különösen érzékeny a DoS (Denial of Service) jellegű támadásokra. Egy támadó ugyanis képes annyira leterhelni a DNS névszervereket, hogy a NAPTR rekordokból semmilyen címinformáció nem kérdezhető le (korlátos időn belül). Ennek eredményeképpen az ENUM azonosítók használhatatlanná válnak – senkit nem lehet elérni ENUM azonosítóján keresztül (közvetlenül PSTN számon, mobilon stb. elérhető marad mindenki) [1].

További két probléma a megszemélyesítés (passing off) és az eltérítés (hijacking). Megszemélyesítés akkor történik, ha valaki vagy valami (entitás) másnak adja ki magát, mint aki valójában. Az ENUM-mal kapcsolatban akkor merül fel, ha valaki egy nem őhozzá tartozó (másik előfizetőnek a birtokában lévő) E.164 azonosítóhoz a saját adatait rögzíti. Ez a rendszert megbízhatatlanná teszi, hisz nem tudni, hogy a kommunikációs partner az e valójában, akinek mondja magát. Eltérítés akkor történik, ha valaki illetéktelenül, a felhasználó tudta nélkül belép a kapcsolatfelépítés útvonalába. ENUM vonatkozásában ez akkor történhet meg, ha egy szolgáltató például regisztrál egy felhasználót az ENUM adatbázisban, annak tudta nélkül, vagy hívásait átirányítja olyan hálózati részeken, alkalmazásokon melyeket a szóban forgó személy nem kért. [1]

A DNS hierarchiában egy adott tartománynévhez tartozó összes információ pontosan egy helyen található meg. Problémát okozhat, ha a .e164.arpa gyökerű ENUM mellett más ENUM-szerű rendszerek is megjelennek (pl. .e164.com). Ez veszélyezteti az E.164-es számokhoz tartozó bejegyzések egyediségét [1].

Problémák, protokollok, architektúrák

Az Internet és PSTN együttműködésével kapcsolatos problémák nyomán szükségessé válik új protokollok kifejlesztése és a meglévők továbbfejlesztése.

A megfelelő átjáró kiválasztása szorosan kapcsolódik az ENUM témaköréhez. Az IP telefónia elterjedésével ugyanis egyre több IP-PSTN átjáró lesz a hálózatban. Az IP-ből a PSTN-be irányuló hívások esetén ki kell választani egy átjárót, amely optimálisan biztosít átjárást az IP és PSTN hálózat között. Az optimumot több tényező is befolyásolhatja. Különböző esetekben más és más hívásirányítás lehet optimális. Haladhat például a hívás javarészt az IP-ben, és csak a hívott félhez eső legközelebbi átjárón lép át a PSTN-be, vagy a lehető legrövidebb szakaszt teszi meg IP-ben és amint lehet áttér a PSTN hálózatba. Ennek a problémának a megoldása nem triviális, a TRIP protokoll jelentheti a megoldást, amely kidolgozás alatt van [17]. Jelenleg az átjárókat nem dinamikusan választja ki a rendszer, hanem statikusan. Az átjáró címe statikusan be van írva az intelligens központi funkciókat ellátó kiszolgáló (gatekeeper, softswitch, SIP proxy) konfigurációjába.

A PINT [18] protokoll azt specifikálja, hogy miként lehet elérni a PSTN szolgáltatásait az IP-ből. Ehhez szorosan kapcsolódik a SPIRITS [19], mely a PSTN-ben berendezett, de az IP és PSTN szoros együttműködését igénylő szolgáltatások architektúráját rögzíti. Ilyen például az 'Internetes hívásra várás' (Internet call waiting). Gyakorlatban ez azt jelenti, hogy ha az előfizető analóg modemes kapcsolattal internetezik és ugyanazon a vonalon valaki éppen hívja őt, értesítést kap a beérkező hívás tényről az Interneten keresztül és választhat a hívás kezelését illetően. Bontja az internetes kapcsolatot és fogadja a hívást, elutasítja a hívást stb. Az IP-PSTN együttműködéssel kapcsolatban megemlítendő még a SIGTRAN keretrendszer [20]. Ennek célja az SCN hálózatok (PSTN, PLMN) jelző protokolljainak (pl.: SS7, Q.931) átvitele IP-n.

Összefoglalás

Az ENUM sok lehetőséget és veszélyt rejt magában. Kérdés, hogy melyikből van több és hogy miként lehet az ENUM-ban rejlő lehetőségeket úgy alkalmazni, hogy a használatával járó kockázat minimális legyen. Ehhez minél több szabványra és konkrét iránymutatásra van szükség. Az ENUM-mal kapcsolatos szabványalkotással mind az ITU-ban mind pedig az ETSI-ben foglalkoznak. Az ETSI-n belül a 2003 nyarán, TIPHON és SPAN szakbizottságok összevonásával alakult TISPAN szakbizottság 4-es munkacsoportja foglalkozik e feladattal.

A szabványalkotás mellett szükséges kísérleti hálózatok kialakítása, és azon veszélyforrások feltárása, melyek a problémamentes bevezetést és üzemeltetést akadályoznák. A bevezetőben feltett kérdésre (hogy az ENUM miért nem terjedt még el) most már könnyen megadható a válasz. Sok olyan eleme van az ENUM-nak, melyek jelen pillanatban adatvédelmi szempontból több problémát okozhatnak, mint hasznot. Az ENUM bevezetése széles társadalmi rétegeket érintő változást eredményezne a távközlő hálózatban és ezen belül az egyes kapcsolatokban. Ennek megfelelően nagy körül-

tekintéssel kell eljárni, hiszen nem mindegy, hogy egy balul meghozott döntés nyomán csupán néhány ember, vagy egy ország jár pórul.

Bár az ENUM RFC-je terjedelmét tekintve csak kilenc oldal, a téma mégis annyira szerteágazó, hogy egy megközelítően tökéletes modell kidolgozása is a kapcsolódó szakterületek alapos ismeretét kívánja.

Irodalom

[1] ENUM Admin. in Europe Technical Specification ETSI TS 102 051 V1.1.1 (2002-07)

[2] RFC 2916 E.164 number and DNS, P. Faltstrom. September 2000.

[3] Introduction to ENUM, Document version 0.1 Austrian ENUM trial platform

[4] RFC 3172 Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain („arpa“), G. Huston, Ed. September 2001.

[5] RFC 1034 Domain names – concepts and facilities, P.V. Mockapetris. November 1987.

[6] RFC 1035 Domain names – implementation and specification, P.V. Mockapetris. November 1987.

[7] RFC 2915 The Naming Authority Pointer (NAPTR) DNS Resource Record, M. Mealling, R. Daniel. September 2000.

[8] RFC 2396 Uniform Resource Identifiers (URI): Generic Syntax, T. Berners-Lee, R. Fielding, L. Masinter. August 1998.

[9] Implications of ENUM, Geoff Huston September 2002. www.potaroo.net/papers/2002/enum.ppt

[10] TRIP, ENUM and Number Portability, Nicklas Beijar Networking Lab., Helsinki University of Technology http://keskus.hut.fi/opetus/s38130/k01/Papers/Beijar-TripEnumNp.pdf

[11] ENUM Services http://www.potaroo.net/ietf/ids/draft-brandner-enum-services-compendium-00.txt

[12] RFC 3403 Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database, M. Mealling. October 2002.

[13] RFC 2845 Secret Key Transaction Authentication for DNS (TSIG), P. Vixie, O. Gudmundsson, D. Eastlake 3rd, B. Wellington. May 2000.

[14] RFC 3008 Domain Name System Security (DNSSEC) Signing Authority, B. Wellington. November 2000.

[15] Public-Key Infrastructure (X.509) (pkix) Internet draft és RFC gyűjtemény http://www.ietf.org/html.charters/pkix-charter.html

[16] An IETF view of ENUM, Geoff Huston, Executive Director, IAB http://enum.nic.at/documents/AETP/Presentations/Austria/0011-2003-03-Australia/huston.ppt

[17] RFC 2871 A Framework for Telephony Routing over IP, J. Rosenberg, H. Schulzrinne. June 2000.

[18] RFC 2848 The PINT Service Protocol: Extensions to SIP and SDP for IP Access to Telephone Call Services, S. Petrack, L. Conroy. June 2000.

[19] RFC 3136 The SPIRITS Architecture, L. Slutsman, Ed., I. Faynberg, H. Lu, M. Weissman. June 2001.

[20] RFC 2719 Framework Architecture for Signaling Transport. L. Ong, I. Rytina, M. Garcia, H. Schwarzbauer, L. Coene, H. Lin, I. Juhasz, M. Holdrege, C. Sharp. October 1999.

[21] Egységes távközlés a különböző infrastruktúrájú hálózatokon, Erdélyi Tibor, BME-AUT Híradástechnika, 2004. március

Hírek

Március 24-én Kovács Kálmán informatikai és hírközlési miniszter bejelentette az **Európai Teleház Szövetségek Uniója** megalakulását.

A jelenleg egyedülálló regionális teleház szervezet a jövőben segíti a nemzeti teleház mozgalmak kialakulását és emeli működésük színvonalát. Célja, hogy nemzetközi segítséggel a leghátrányosabb települések is közösségi és otthoni hozzáférési lehetőséghez jussanak. Az Unió fontosnak tartja a teleházak és felhasználóik közti közvetlen kapcsolatok erősítését, ezért megkezdi a virtuális – határoktól független – kisközösségek erősítését a „Virtuális Teleházország” szervezésével. A szervezet nyitott, s mivel az Alapszabály nem zárja ki Európán kívüli szövetségek csatlakozását sem, így az sem kizárt, hogy a kezdeményezés világszervezet kibontakozásához vezethet.

Ortogonális frekvenciaosztású többszörös hozzáférés

DR. DÁRDAI ÁRPÁD, okleveles híradástechnikai szakmérnök

dardai.arpad@axelero.hu

Kulcsszavak: sokvivős moduláció, OFMD, fading- és interferenciaállóság, WLAN

A cikk a vezetékes, a vezetéknélküli és a mobil távközlés hozzáférési szakaszainak és a digitális műsorszórásnak fontos átviteli és modulációs eljárásával, a sokvivős modulációs eljárásokhoz tartozó ortogonális frekvenciaosztásos többszörös hozzáféréssel (OFDM) foglalkozik. Ismerteti az OFMD átviteli és modulációs eljárások alapjait, a műszaki, rendszertechnikai, alkalmazási és értéknövelő megoldásokat. Számos alkalmazásban – különösen, ahol kiemelt szempont a zavarvédelem és az egyszerű, gyors, gazdaságos létesíthetőség – segíthet az OFDM.

A gyors fejlődése sok hasonló távközlési és informatikai alkalmazási területet nyitott meg. Ennek fontos eredményei: a többszörös hozzáférési- és a modulációs technika újszerű, hatékony módjainak kialakulása, a fénytávközlés elterjedése, minőségének lényeges javulása, árának csökkenése, az Internet Protokoll egyre növekvő alkalmazása.

Az utóbbi években dinamikusan fejlődő ágazat a különféle kód, vagy frekvenciaosztású többszörös hozzáférési eljárásokon alapuló technológiák. Ilyen az OFDM is, ez a 3G, 4G generációjú vezetéknélküli távközlőrendszerek hozzáférési szakaszaiban, a WLAN rendszerekben, a vezetékes távközlésben (például xDSL), és a villamos hálózati távközlésben (PLC), valamint a digitális műsorszórásban is egyre nagyobb szerepet kap.

Az OFDM (Orthogonal Frequency Division Multiplexing) az ortogonális frekvenciaosztásos hozzáférés egyike a digitális modulációs átviteli technikáknak. A távközlési csatornát nagyszámú, egyenlő osztású frekvenciasávokra osztja. Minden egyes részsávban egy alvivőfrekvencia továbbítja a teljes információ egy részét. Az alvivők egymással kölcsönösen ortogonálisak (kölcsönösen függetlenek).

1. Az OFDM kialakulása, alkalmazások, nemzetközi tevékenység

Az OFDM többszörös hozzáférési eljárást kezdeti kutatás és kísérletek után az 1950-es évektől alkalmazták. Az 1960-as évekre kidolgozták az OFDM elméletét. 1970-es években az OFDM készülékek a diszkrét transzformációt (DFT – Discrete Fourier Transform) már gyors Fourier-transzformációval (FFT – Fast Fourier Transform) végezték. Az OFDM átvitelt az 1980-as években nagy sebességű modemekhez és digitális mobil összeköttetésekhez, és 1987-ben digitális hang műsorszóráshoz (DAB) is használták. Az 1990-es évektől szélessávú összeköttetésekhez, xDSL digitális előfizetői vonalakhoz, és DVB, HDTV célokra vezették be. Ma az OFDM eljárás a távközlés számos más területén is fontos: ETSI BRAN, ETSI HIPERLAN/2, IEEE 802.11a, b (WiFi) és g szerinti WLAN eszközök, PLC, DMB, 3G, 4G mobil rendszerek.

Az OFDM technika, a szabványosítását és a bevezetését nemzetközi távközlési szervezetek (ITU-T,-R, ETSI) és programok (3GPP) segítik. Cél a távközlési infrastruktúra és a szolgáltatások összehangolt fejlesztése. Lényeges az ETSI, az IEEE és a COST kutatási és szabványosítási szerepe. E szervezetek és programok keretében dolgozták ki az UMTS, a BRAN, a WLAN, és a WiFi megoldásokat, a Bluetooth, és az ad hoc hálózati rendszereket.

2. Az OFDM eljárás

2.1. A zajos csatorna leírása

A mobil rendszerek tervezését alapvetően befolyásolják a rádiócsatorna fizikai és hullámterjedési viszonyai. A szokásos rádiócsatornában többutas hullámterjedés lép fel, így az adótól a vételi helyre érkező jel reflexiós összetevőkből áll. A mobil állomások mozgása miatt a hullámterjedési utak eltérő késleltetéssel és a megfelelő Dopplerfrekvenciákkal jellemezhetők, ezekből meghatározhatók a rádiócsatorna frekvencia-szelektív tulajdonságai és időbeli szórása (idő diszperzió). A mobil állomás vételi viszonyait és a rádiócsatorna impulzusválaszát (CIR – Channel Impulse Response) a *1. ábra* szemlélteti.

Az épületekről, járművekről, tereptárgyakról visszavert hullámok érkeznek a vevőantennához. A vételi helyre közvetlen hullám is érkezhet, de lehet olyan vételi pont is, amelyre csak reflektált hullám verődik. Legyen a hullámok közötti legnagyobb időkülönbség τ_{max}, a továbbított adatok szimbólum ideje T.

A reflexiók következtében egy vett szimbólumot

$$I = \tau_{max} / T \qquad (1)$$

számú előző szimbólum befolyásolhat, ahol I a szimbólumközi interferencia (ISI – Inter-Symbol Interference)

mértéke. Ennek a hatásnak a kiküszöbölése, illetve minimalizálása a vevőkészülék feladata.

A többutas rádiócsatorna erős szimbólum közötti interferenciát okoz főleg a nagy adatátviteli sebességű és a szélessávú alkalmazásoknál. Ezt figyelembe kell venni a zajos átviteli-rendszerek megvalósítása során.

2.2. Az OFDM eljárás kialakulása és alapelvei

Az OFDM eljárás alapgondolata

Az OFDM frekvenciaosztású átvitel és többszörös hozzáférés alapgondolata az, hogy egy nagy adatátviteli sebességű adatfolyam sok kisebb sebességű adatfolyamra osztható, amelyek alvivőinek modulációja egyedi, a többitől független, de azokkal egy időben történik. Az alvivők adatátviteléhez tartozó szimbólum idő az eredeti többszöröse lesz, így a részcsatornák átvitele ellenállóbb a csatorna többutas hullámterjedés okozta időszórásával és a zajokkal szemben. A vivőfrekvencia összetevők kölcsönösen ortogonálisak, innen az eljárás neve is: ortogonális frekvenciaosztásos többszörös hozzáférés (OFDM).

A szimbólumok közötti interferencia csökkentése az OFDM eljárásnál

Az *I* interszimbólum interferencia (ISI) értéke a (4.1) összefüggés szerint

$$I = \tau_{max} / T . \qquad (2)$$

Egy N részcsatornás sokvivős rendszernél egy részcsatorna adatátviteli sebessége

$$D_r = D / N , \qquad (3)$$

a részcsatorna szimbólumideje pedig

$$T_r = 1 / D_r . \qquad (4)$$

Helyettesítéssel adódik, hogy

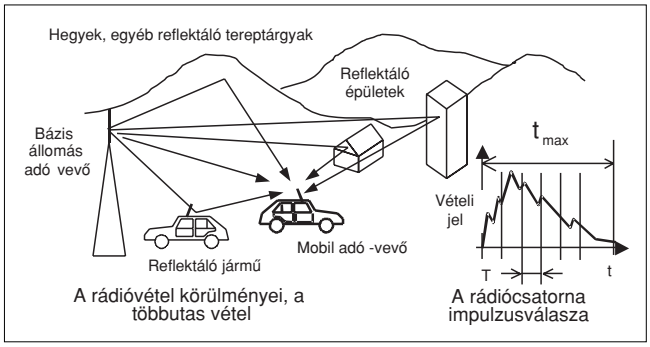
$$T_r = N \bullet T , \qquad (5)$$

vagyis a részcsatorna szimbólumideje az eredeti szimbólumidő *N*-szerese, amiből a szimbólumközi interferencia (ISI) idő részcsatornára adódó értéke

$$I_r = \frac{\tau_{max}}{T_r} = \frac{\tau_{max}}{T \bullet N} \quad . \qquad (6)$$

A hányados szerint a szimbólumközi interferencia az eredeti érték N-ed részére csökkent. Látható, hogy az OFDM átvitel a részcsatornák számának alkalmas megválasztásával a zavarok és a többutas terjedés káros hatásait jelentősen csökkentheti. Az alvivők N száma LAN hálózatoknál szokásosan 64-256, DVB rendszernél 2000-8000.

1. ábra Többutas átvitel és a csatorna impulzusválasza



Az OFDM jel sávszélessége és spektruma

Az OFDM átviteli és multiplex eljárásnál az adatszimbólumok továbbítása, a szélessávú jelet sok, ortogonális, keskenysávú jelösszetevőre bontva, a frekvencia-összetevők segítségével párhuzamosan viszi át. Az átvitel után az összetevők adatfolyamát egyesítik és visszanyerik az eredeti nagy adatátviteli sebességű, szélessávú adatfolyamot.

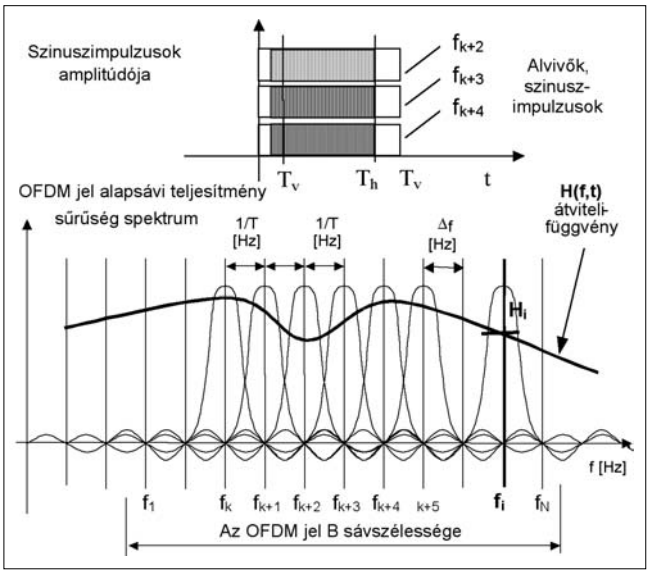
Az OFDM jel összetevőit, vagyis a szinuszimpulzosokat, az OFDM jel spektrumát, és a *H* átviteli függvényt a *2. ábra* szemlélteti. Az ábra szerint a *H* függvény a csatorna frekvencia és időfüggése következtében frekvencia és időfüggő; *H = H(f,t)*.

Az OFDM színusz csomagokban jelentkezik. Ennek időtartama a T_r szimbólumidő (részcsatorna szimbólumideje), a színusz hullámok frekvenciái pedig $f_1, f_2, \ldots, f_i, \ldots, f_k, \ldots, f_N$, ahol az f_1, f_2, f_3 stb. frekvenciák rendre az $f_0, 2f_0, 3f_0, \ldots, Nf_0$ frekvenciáknak felelnek meg. Ha a vivők száma *N*, akkor az OFDM jel teljes *B* sávszélessége a frekvenciaösszetevők között lévő $f_0 = \Delta f = 1/T_r$ távolsággal:

$$B \approx N / T_r = N \bullet \Delta f \qquad (7)$$

Színuszcsomag impulzus Fourier-transzformáltja, vagyis frekvencia-spektruma *sinx/x* alakú. Az egyenlő Δf alvivőtávolság esetén az alvivők spektruma nem lesz teljesen elválasztva. Az OFDM jel ortogonális alvivőinek spektrumai átlapolódnak, de az összetevők spektrumainak maximumai a többi frekvencia összetevő spektrumának minimumaihoz esik. A spektrumok egyéb részei Δf távolságonként, a spektrumok zérus értékeinél kereszteződnek. A teljes OFDM spektrum kialakításánál arra törekszenek, hogy az alvivők spektrum energiájának döntő része egy adott sávszélességen belül legyen, és a szomszédos frekven-

2. ábra Az OFDM jel spektruma



cia-összetevő sávjába minél kisebb energia jusson. Az alvivőspektrumok kialakítása következtében, a teljes OFDM jel *B* sávszélességű spektruma közel négyszögletes, így az OFDM jel spektrumhatékony.

A részcsatornák átviteli függvénye

Az OFDM jelet a *H=H(f, t)* átviteli függvényű csatorna továbbítja. A *2. ábra* szerint az OFDM jel egyedileg modulált, majd összegzett részjelei párhuzamosan kerülnek továbbításra a számos keskenysávú részcsatornán. A *H* átviteli függvény a frekvencia és az idő függvénye, de a részcsatornák átvitelére nem a szélessávú jel átviteli függvénye érvényes, hanem csak a Δf sávszélességre eső, ami jó közelítéssel konstans. A keskenysávú részcsatornákra a jelátvitel összefüggése így:

$$R_i = S_i \bullet H_i + P_z \qquad (4.9)$$

ahol

R_i az i-edik csatorna vételi jele, az átvitel után nyert jel teljesítménye,
S_i a részcsatorna adási jele, az átviendő jel teljesítménye,
H_i a i-edik részcsatornára érvényes keskenysávú átvitel átviteli függvénye,
P_z az átvitel során a jelhez adódott Gaussi-fehér zaj teljesítménye.

A keskenysávú részcsatornákban az adatszimbólum ideje már lényegesen nagyobb lesz, mint a csatorna maximális késleltetése. Frekvencia-szelektív rádiócsatornánál további előny az egyfrekvenciás szélessávú rendszerhez képest az, hogy a részcsatornákra bontott szélessávú rendszer részcsatornás vevőiben jelentősen csökken a kiegyenlítők számítási igénye. Az OFDM eljárással megfelelő átvitel valósulhat meg az olyan szélessávú csatornában, amelyben a maximális hullámterjedési késleltetés sokkal nagyobb, mint a szélessávú adatfolyam szimbólum ideje.

Védőtávolságok alkalmazása az OFDM jelben

Az alvivőkkel átvitt információk az alvivők ortogonalitása következtében szétválaszthatók. Az alvivők ortogonalitását a frekvenciák értékének és egymáshoz való viszonyának 2. ábra szerinti speciális választása eredményezi. A jó működéshez azonban a szimbólumidőkben védőtávolságok alkalmazása is szükséges.

A 2. ábrán feltüntetett T_v időmennyiség a védőintervallumot, és T_h a hasznos szimbólumidőt képviseli. A T_v a védőintervallum (GI – Guard Interval), amelyben a ciklikus előtag (CP – Cyclic Prefix) is helyet foglal, redundanciát, illetve többletadatot (overhead) jelent, ami a hasznos szimbólumidőt csökkenti. Szerepe mégis fontos, mert a védőintervallummal kiküszöbölhető, vagy jelentősen csökkenthető a szimbólum közötti interferencia (ISI), amely a többutas fadinges, idő-diszperzív rádiócsatornán történő átvitel során felléphet. Az OFDM jelben a ciklikus előtag előállításának egyik módja az, hogy az adott szimbólum (blokk) időfüggvényének meghatározott részét, rendszerint a szakasz végéről, a szimbólum elejére másolják, meghosszabbítva így a szimbólum lefolyását. Az előtagot az adott blokk időfüggvénye végének egy részéből képezik, bemásolva ezt a védőintervallumba úgy, hogy ennek folytatása maga az adott adatblokk időfüggvénye lesz.

A többutas terjedéssel a vevőbe érkező összetevők közötti késleltetés különbséget az OFDM vevő kiegyenlíti. A védőintervallumnak legalább akkorának kell lenni, hogy az alatt a csatorna impulzusválasza (tranziense) az 1. ábra szerint lecsengjen, más szavakkal, a T_h és a T_v idők összege, vagyis az eredő T_e szimbólumidő, legyen lényegesen kisebb, mint a rádiócsatorna T_c koherenciaideje. A T_h hasznos szimbólumidőre a T_r választás is tehető, illetve a realizáció során más értelmezés és megoldás is lehetséges.

2.3. Az OFDM jelek előállításának matematikai alapjai

Az OFDM esetében fontos a gyors Fourier-transzformáció (FFT), amely a Fourier-módszerek családjába tartozik. A gyors Fourier-transzformáció áttekintésekor utalunk a Fourier-transzformáció (FT), illetve a diszkrét Fourier-transzformáció (DFT) és a mintavételezés alapjaira.

Diszkrét Fourier-transzformáció. Egy *f(t)* függvény *N* darab *f(k)* mintával, vagyis diszkrét idősorral is megadható, ahol *k = 0, 1, 2, 3, …, N-1*. Az *f(k)* értékek valós és képzetes részekkel rendelkező komplex számok is lehetnek. Egy ilyen sorozat Fourier-transzformáltja frekvenciaértékeket, frekvenciamintákat ad. A frekvenciatartománybeli kép, a frekvenciaspektrum is *N* mintát tartalmaz.

A diszkrét függvényértékek Fourier-transzformáltja a diszkrét Fourier-transzformációval:

$$F(n) = \sum_{k=0}^{N-1} f(k) e^{-j\frac{2\pi kn}{N}}; \quad n = 0,1,...,N-1 \qquad (9)$$

ahol F(n) általában szintén komplex sorokat képezhet.

Az inverz diszkrét Fourier-transzformált:

$$f(n) = \frac{1}{N} \sum_{k=0}^{N-1} F(k) e^{j\frac{2\pi kn}{N}}; \quad n = 0,1,...,N-1 \qquad (10)$$

Mintavételezés. A diszkrét Fourier-transzformáció alkalmazása és a jelek feldolgozása során követni kell a Shannon-féle mintavételi szabályokat és a Nyquist-kritériumokat ($f_{mv} \geq 1/T_{mv} = 2f_{max}$, $f_{mv} = 2f_{max}$, $f_N = 2f_{max}$). E szerint egy sávhatárolt jel, esetünkben egy modulált jel időfüggvénye egy szimbólumának *T* ideje alatt, elegendő $\Delta t = 1/2B = T_{mv}$ periodikus gyakorisággal *N* db *(0, 1, 2, …, N-1)* pillanatnyi mintát venni. Itt Δt a mintavételi időköz, *B* a jel sávszélessége és $f_{mv} = 1/\Delta t$ a mintavételi frekvencia. Az így nyert idősorozathoz a frekvenciatartományban szintén *N* db *(0, 1, 2, …, N-1)* frekvencia összetevő, frekvenciaminta tartozik.

Az időfüggvényből transzformált frekvencia értékek sorának *0*-adik eleme az időfüggvény átlaga (DC – Direct Current), az első eleme az első harmonikus, és a többi összetevő frekvenciája az elsőnek harmonikusa, az adott index szerint.

A fentieket alkalmazva, a *B* sávszélességben elhelyezkedő, *N* tagú frekvenciasor (a szemléletesség végett a sor

képzetes része legyen zérus) az *N/2*-edik (az f_N Nyquist-frekvencia felének megfelelő) mintára szimmetrikusnak tekinthető (a pozitív, ill. negatív frekvenciák analógiájára). Az *N*-edik minta, illetve a megfelelő frekvencia a Nyquist-frekvencia.

Ebben a szimmetrikus esetben, a Nyquist első kritériuma szerint elegendő a frekvenciatartománybeli *N* minta közül az első *N/2*-edik mintáig figyelembe venni a spektrumot. Szimmetrikus esetben ez az a frekvencia, illetve a megfelelő frekvencia minták, amelyeknek létezni kell ahhoz, hogy az inverz diszkrét Fourier-transzformáció (IDFT) segítségével az adatjeleket hibamentesen visszaállíthassuk. Ennek ismeretében, a $B = N\Delta f$ sávszélességű OFDM jelre a szükséges mintavételi idő $\Delta t = 1/B = 1/N\Delta f$.

Sávátlapolódás, Aliasing. A mintavételezés során az alapsávi spektrum mellett megjelenik a mintavételi frekvenciára (és harmonikusaira) szimmetrikusan, az alapsávnak megfelelő alsó és felső oldalsáv is. Alul mintavételezésnél ($f_{mv} < f_N$) az alapsáv és a mintavételezési frekvencia alsó sávja átlapolódik (Aliasing). Az alapsávban idegen összetevők jelennek meg, ami az adatátvitelnél átviteli hibákat okoz.

Gyors Fourier-transzformáció. A gyors Fourier-transzformáció (FFT) olyan algoritmus, amely egy valóságos (idő)-függvényhez tartozó diszkrét adatok véges készletéből Fourier-transzformáltat ad. Az adatok periodikus mintavétellel keletkeznek. Az FFT eljárás a folyamat frekvencia összetevőit adja. Az FFT az inverz transzformációra is megoldás, így a frekvencia adatokból az eredeti függvény egyértelműen visszaállítható.

A diszkrét Fourier-transzformációval adódó idő- és frekvenciasorok komplex értékűek is lehetnek. Komplex sorokkal végzett számítógépes műveletek – különösen nagy sorokkal – időigényesek. A Fourier-transzformáció N^2 komplex szorzást és összeadást igényel. A számítási idő tetemes, mert a sorok tagjainak számával négyzetesen arányos. Kifejlesztettek lényegesen kisebb számítási idejű algoritmusokat is, ezek gyűjtő neve gyors Fourier-transzformációnak (FFT), amelyek azonos eredményre vezetnek, mint a DFT. Az FFT algoritmusok számítási időigénye közelítőleg a sorok tagjai száma és számuk kettesalapú logaritmusának szorzatával arányos.

A számítások érvényessége. A diszkrét és inverz diszkrét Fourier-transzformáció a periodikus függvényekre értelmezett Fourier-soroknak felel meg. Szigorúan nézve, a modulált jelek nem periodikusak, egy-egy *T* szimbólumidőre a diszkrét Fourier-transzformáció, illetve inverz transzformáció, a gyakorlatban mégis jól használható. Ennek oka, hogy egy T időtartamú, nem periodikus jel megadható frekvenciatartománybeli mintákkal, amelyekből az időfüggvény teljesen visszaállítható. A számításokhoz használhatók a Fourier-transzformáció, komplex sorok, komplex számok tételei.

Alkalmazások. Az FFT eljárás alkalmazásai közül: matematika és fizika, lineáris rendszerek analízise, erősen zajos, illetve zaj alatti jelek hatékony visszaállítása. Az esetekhez a gyors Fourier-transzformáció igen hatékony eszköz. Jellemzője, hogy a megoldandó problémákat könnyebben kezelhető alakra hozza.

3. Az OFDM adási és vételi jel

Az OFDM adási alapsávi jel előállításának elve

Az OFDM megoldás rész-frekvenciasávjai a T_r szimbólum időben egész számú periódusidőkkel helyezhetők el. Az alvivők frekvenciája a $\Delta f = 1/T_r = f_0$ frekvenciatávolság, illetve frekvencia egészszámú többszörösei (harmonikusai), vagyis f_0, $2f_0$, $3f_0$, …, nf_0, …, $(N-1)\,f_0$, Nf_0 . Az alvivők a T_r időben, illetve T_v védőintervallummal kiegészített részében is ortogonálisak.

Az OFDM jel ortogonális összetevőinek és az átlapolódó spektrumoknak az előállítását az adó és a vevő oldalon digitális jelfeldolgozó eljárások végzik. A digitális moduláció a szinuszos jelek három paraméterét modulálhatja: amplitúdó, frekvencia és fázis (ASK, FSK, PSK). Az OFDM átvitelnél gyakori az ASK és a PSK moduláció kombinációja (APSK) vagy a QAM moduláció. Az OFDM adási jel alapsávi időfüggvénye:

$$s_{as}(t) = (A_k + jB_k) \bullet e^{j2\pi f_v t} = M_k \bullet e^{j2\pi f_v t} \qquad (5.1)$$

ahol $e^{j2\pi f_v t}$ az f_v frekvenciájú vivőhullám, és $M_k = (A_k + jB_k)$ a komplex digitális moduláció a *k-adik* adatblokkban. A modulált alvivők átvitele az f_v vivő segítségével történik, amelyhez az alvivők frekvenciái hozzáadódnak (transzponálás, konverzió a kívánt sávba). Így a frekvenciák értékei rendre f_v+f_0, f_v+2f_0, f_v+3f_0, …, f_v+nf_0 lesznek. Az f_v vivő elvileg lehet a végleges RF vivő, de az adott készüléktől függő jel- és frekvencia-feldolgozás módja szerint lehet egy közbenső segédvivő is. A vivő az alvivők (részsávok) helyére nézve a frekvenciatengelyen additív, vagyis a vivő az OFDM jel alvivőit, illetve alapsávi spektrumát a vivő értékével eltolja a kívánt áteresztő sávba.

Az információ átvitele az alvivők amplitúdójának és fázisának modulációjával történik. A modulált alvivők összege adja az alapsávi OFDM jelet. Az alapsávi OFDM jel időfüggvényének matematikai összefüggése:

$$s_{as}(t) = \sum_{n=0}^{N-1} \{a_n \cos(2\pi n f_0 t) + b_n \sin(2\pi n f_0 t)\} \qquad (5.2)$$

Az (5.2) összefüggés szerint az s_{as} alapsávi jel előállításához N darab alvivő generátor és N darab alvivő modulátor szükséges, a teljes modulált időfüggvény a külön-külön, de egyidejűleg modulált alvivők időfüggvényeinek összege. Az időfüggvény a külön-külön modulált alvivők előállítása és összegzése helyett, a nagyszámú modulátorok készítése nélkül, a Fourier-transzformáció eljárásaival is generálható.

Az OFDM jel generálása az adóban, moduláció

Előállítandók az alapsávi OFDM jel időfüggvényéből az egyidejű párhuzamos adatok, majd az alvivők modulálásával a modulált alvivők alapsávi időfüggvényeit, illetve az időfüggvények frekvenciaspektrumait.

Ezt követi a modulált analóg adatjelek analóg-diszkrét átalakítása a mintavételi értékekkel a $\Delta t = 1/B = 1/N\Delta f$ mintavételi időpontokban. Az alapsávi adási OFDM jel diszkrét értékei így:

$$s_{as\,k,i} \cong \frac{1}{N}\sum_{n=0}^{N-1} m_{k,n} e^{j\frac{2\pi ni}{N}}; \quad i = 0,1,2,...,N-1 \quad (11)$$

ahol az $s_{as\,k,j}$ értékek a *k-adik* adatblokkhoz tartozó időfüggvény *i-edik* mintavételi értéke, és $m_{k,n}$ a *k-adik* adatblokkhoz tartozó *n-edik* rész-időfüggvény (alvivő) komplex modulációs szimbóluma, $m_{k,n} = (a_{k,n} + jb_{k,n})$ és $\Delta f = 1/T_e$, a szimbólumidő reciproka.

Az (5.3) kifejezés megfelel az inverz diszkrét Fourier-transzformációnak. Végrehajtása, az időfüggvény minták előállítása a modulációs szimbólumokkal, az inverz gyors Fourier-transzformációval (IFFT – Inverse Fast Fourier-Transformation) lehet. A mintákból a D/A konverter diszkrét-analóg átalakítással analóg jelet állít elő, amelyet a kívánt sávba konvertálva kisugároz.

Az adatok visszanyerése az OFDM jelből, demodulálás

Az $s_{as}(t)$ alapsávi jelből az a_n, b_n $(n = 0, 1, 2, ..., N)$ modulációs tartalom, vagyis a szimbólum információ a Fourier-transzformációval visszaállítható:

$$a_n = \int_0^T s_{as}(t)\cos(2\pi n f_0 t)dt,$$
$$b_n = \int_0^T s_{as}(t)(\sin(2\pi n f_0 t))dt \quad (12)$$

Az OFDM jel demodulálása a következők szerinti. Az f_v sávjában levő OFDM jelet a $2\pi f_v$ vivő körfrekvenciájú koszinuszos, illetve színuszos jellel szorozva, aluláteresztő után az alapsávi jelet kapjuk. Az I (In Phase) jelet koszinuszos (cos) függvénnyel, a Q (Quadrature) összetevőt színuszos (sin) függvénnyel szorozva nyerhetjük. A komplex alapsávi jel:

$$s(t) = s_I(t) + js_Q(t) \quad (13)$$

Az (5.1) és az (5.3) egybevetéséből

$$s(t) = \frac{1}{N}\sum_{n=0}^{N-1} m_n \bullet e^{j2\pi n f_0 t} \quad (14)$$

ahol $f_0 = 2\pi/N$. Az (5.6) megadható diszkrét értékekkel a következő alakban is (15):

$$s(n) = \frac{1}{N}\sum_{k=0}^{N-1} m(k) e^{j\frac{2\pi kn}{N}}; \quad n = 0,1,...,N-1$$

Az (5.7) összefüggés alapján, diszkrét Fourier-transzformációt alkalmazva a modulációs adatszimbólumok visszanyerhetők (16):

$$m_n(k) = \sum_{n=0}^{N-1} s(n) e^{-j\frac{2\pi nk}{N}}; \quad k = 0,1,2,...,N-1$$

Ez a rádiócsatornán történő átvitel, majd vétel és detektálás után, az OFDM vevő feladata. A valóságos esetekben az eredő szélessávú adatfolyamot visszaállító diszkrét Fourier-transzformációhoz a gyors Fourier-transzformáció használatos.

4. Az OFDM jel előállításának és demodulálásának tömbvázlata

Az OFDM átvitel tömbvázlata

Az OFDM jel előállítása a 3. pontban részletezett matematikai összefüggések alapján, a *3. ábrával* szemléltethető.

Adjunk az ábra szerinti OFDM modulátor bemenetére szélessávú, nagy adatátviteli sebességű bináris digitális adatfolyamot. A soros bináris adatok OFDM rendszeren történő átvitelének főbb lépései a matematikai összefüggések és a szükséges jelfeldolgozási feladatok alapján az alábbiak:

– kódolás (FEC), átszövés (interleaving),
– soros-párhuzamos átalakítás, majd
– modulálás, ezt követően
– inverz Fourier-transzformáció és a védőintervallum beiktatása
– párhuzamos-soros átalakítás, majd diszkrét-analóg konverzió,
– az OFDM jelek adása, átvitele, vétele, és visszaalakítása.

A modulátor működése

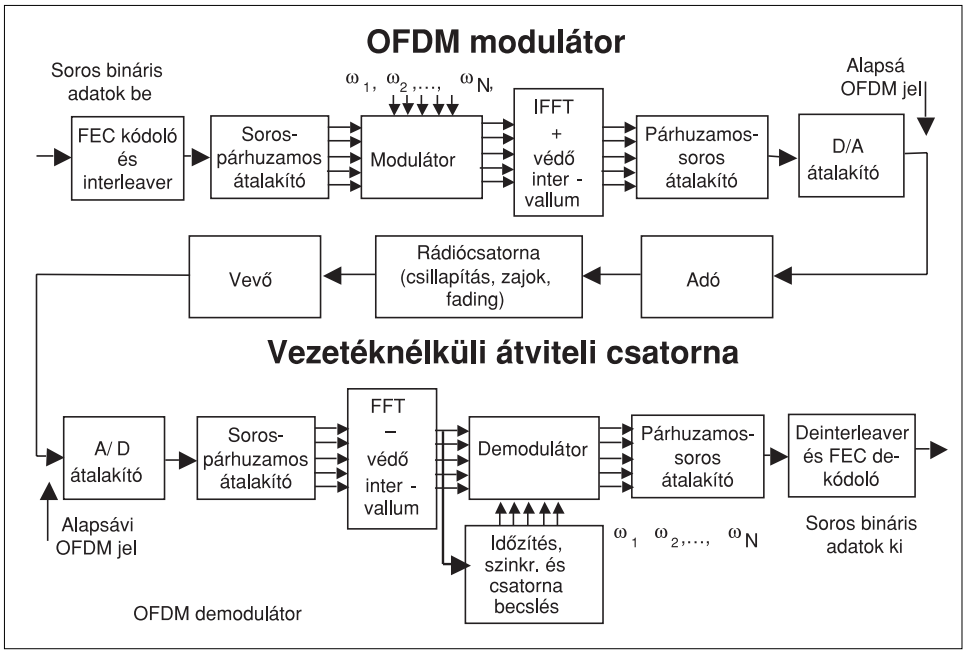
Kódolás és átszövés. Az OFDM modulátor a szélessávú adatfolyamot kódolja (FEC, konvolúciós kódolás) és átszövés (átlapolás, interleaving) eljárásnak veti alá. A kódolás (pl. Reed-Solomon) feladata az átviteli hibák elleni védelem, az átszövés pedig a csomós hibák hatását csökkenti. Az átszövés történhet mind a frekvencia-, mind az időtartományban.

Soros-párhuzamos átalakítás. A kódolás és átszövés után az OFDM eljárás a szélessávú adatfolyamot nagyszámú, kisebb sebességű bináris adatfolyamra, rész adatcsatornára bontja.

Moduláció. A részcsatornákra bontás után a részadatcsatornák modulációja következik. A megoldástól függően, PSK (Phase Shift Keying), QPSK (Quadrate Phase Shift Keying), QAM (Quadrature Amplitude Modulation), APSK (Amplidude and Phase Shift Keying), vagy más moduláció alkalmazható. A modulációs eljárások szintje lehet M (páros egész szám), és a moduláció lehet differenciális, vagy nem differenciális, a rendszertől függően.

Inverz Fourier-transzformáció és a védőintervallum beiktatása. A moduláció létrehozza azt a frekvenciaspektrumot, amelyet az inverz diszkrét Fourier-transzformáció a megfelelő időfüggvénnyé, illetve az időfüggvény mintavételi pontjaivá alakít át. A mintavétel gyakorisága a 2. ábra és a (4.8) összefüggés alapján $\Delta t = 1/B$. Az inverz Fourier-transzformáció, a modulátor kimenetén megjelenő digitális jel spektrumának megfelelően, az inverz diszkrét Fourier-transzformációval (IDFT), illetve az inverz gyors Fourier-transzformációval (IFFT) végezhető el. Az IFFT egység tehát, a részsávok spektrumaiból a részsávok időfüggvényeit állítja elő.

Az egység adatblokkonként védő intervallumot (GI – Guard Interval, CP – Cyclic Prefix, Cyclic Guard Period) is beiktat a jelbe, ami a többutas hullámterjedés okozta fading hatását csökkenti. Egy-egy adatblokk a soros adat-



3. ábra Az OFDM átvitel blokkvázlata

folyamból egy-egy lépésben párhuzamos adatokká alakított adatmennyiség. Az adatstruktúrának más kialakítása is lehetséges.

Párhuzamos-soros átalakítás, majd diszkrét-analóg konverzió. A párhuzamos-soros átalakító feladata, hogy a bemenetein jelentkező, párhuzamosan jelen levő részsávok visszaállított időfüggvényeinek diszkrét mintavételi értékeit sorosan rendezze (időfüggvények összegzése, szuperpoziciója). A diszkrét mintavételi értékeket folytonos időfüggvénnyé alakítja a D/A egység. Kimenetén az alapsávi analóg OFDM jelet nyerjük.

Az OFDM jelek adása és átvitele. Az OFDM modulátort az RF adó követi. Az adó az alapsávi OFDM jelet egy megfelelő modulációval és transzponálással a rádiófrekvenciás vivőre helyezi, és a kívánt teljesítményű RF jelet az adóantennáról kisugározza. Az RF jelek vételét a rádiócsatornán történő átvitel után az OFDM vevő és demodulátor végzi.

A demodulátor működése

Az OFDM vétel az adás fordítottja. A fontosabb működési fázisok az alábbiak.

Az OFDM jelek vétele. A vevő RF fokozatai a kívánt frekvenciájú OFDM jelet veszik és kiválasztják. A keverés és transzponálás révén a jel a KF egységbe jut. A KF egység kimenetén megjelenik a KF sávi, sávhatárolt OFDM jel, illetve spektrum.

Analóg-diszkrét átalakítás, soros-párhuzamos felbontás. A KF egység kimenetéhez csatlakozó A/D egység a KF sávi OFDM spektrum időfüggvényét mintavételezi és előállítja a diszkrét digitális adatfolyamot, illetve a megfelelő diszkrét időfüggvény értékeket. Ezt követi az adatfolyam felbontása párhuzamos részadatcsatornákra.

Gyors Fourier-transzformáció. A részadatcsatornák jeleinek időfüggvényeiből a vevő FFT egysége gyors Fourier-transzformációval a modulált jelek frekvenciaspektrumait állítja elő, amelyeket a demodulátorok demodulálnak.

Demoduláció és párhuzamos-soros átalakítás. A demodulátorok koherens vagy PSK, AQAM stb. demodulátorok, amelyek bináris adatokat adnak. A demodulált, párhuzamos részadatcsatornák adatait a párhuzamos/soros átalakító soros adatfolyammá képezi.

Inverz-átszövés, FEC dekódolás. Ezután következik az inverz-átszövés (deinterleaving) és a FEC dekódoló. A deinterleaver (lehet idő- és frekvenciatartománybeli) visszaállítja az eredeti adatsorrendet, megszüntetve, illetve csökkentve az esetleges csomós hibák hatását. Az ily módon elállított adatsorozatot a FEC kódolásnak megfelelően dekódolják. Az adótól küldött adatszimbólumok becslésére Viterbi-algoritmus használható. A Viterbi-dekóder a küldött szimbólumszekvenciához legközelebbi szimbólumsorozatot választja ki.

Időzítés, szinkronizálás, csatornabecslés. A vevőkészülék feladata a vivők időzítése, szinkronizálása, a csatorna becslése, a szükséges csatornakiegyenlítések elvégzése is.

5. Az OFDM adás előnyei és hátrányai

Fontosabb előnyök:

• a frekvenciaspektrum hatékony felhasználása a részspektrumok átlapolódásával,

• a részcsatornák átvitele a szimbólumidőkben gyakorlatilag fadingtől mentes,

• a részcsatornák ortogonalitása és a védőidő az interszimbólum interferenciát jelentősen lecsökkenti,

• az átvitel során technikai védettséget ad, detektálása speciális technikát igényel,

• megfelelő csatornakódolással és átszövéssel az átviteli biztonság tovább növelhető,

• a részcsatornákra egyszerűbbé válik a csatorna kiegyenlítése, mint a teljes sávra, mint az egyvivős esetre,

• a gyors Fourier-transzformációs eljárás csökkenti a számítási műveletek számát, ez kedvező a modulátor és a demodulátor megvalósíthatóságára,

• differenciális modulációval a csatornakiegyenlítő egyszerű, esetenként szükségtelen,

• az időszinkronizálás és a mintavételezés egyszerűbb, mint az egyvivős rendszereknél.

Hátrányos tulajdonságok:

• az OFDM jel amplitúdó eloszlása zajszerű, nagy dinamikájú, a teljesítményerősítők nagy csúcs-átlag teljesítményviszonnyal működnek, ez az erősítőkkel szemben nagy követelményeket támaszt,

• az OFDM átvitel a frekvenciapontosságra és -megváltozásra sokkal érzékenyebb, mint az egyvivős rendszer, a diszkrét Fourier-transzformáció sajátosságai miatt.

A jellemzők vizsgálata az előnyök túlsúlyát mutatja. A hátrányok hatása a korszerű jelfeldolgozási módszerekkel és a modern áramkörtechnikával kiküszöbölhető.

Az OFDM eljárás összefoglaló értékei és értéknövelő képességei

Az OFDM moduláció előnyös mert:

• *Hálózat létesíthető:* infrastruktúrális, ad hoc, vagy vegyes távközlőhálózatok.

• *IP- és multimédia-alkalmasság.* Kedvező a fejlett IP alapú kommunikációhoz, a beszédcélú és a multimédiás alkalmazásokhoz, az adaptív alkalmazási feltételekhez.

• *Csatlakoztathatóság, együttműködés, alkalmazások.* Az OFDM alapú távközlés rendszereinek, alrendszereinek kialakítása lehetővé teszi a hálózatok, alhálózatok és terminálok jó együttműködését, a korszerű távközlési szolgáltatásokat.

Irodalom

[1] Dr. Pap László:
A hírközlő csatornák fizikai védelme,
szórt spektrumú eljárások.
Híradástechnika, XLVI. évf., 1995. március

[2] Dr. Pap L.–Dr. Dárdai Á.:
SST-CDMA rendszerek tulajdonságai.
Cellás rendszerek összehasonlítása.
Híradástechnika, XLVI. évf., 1995. április

[3] Sklar, Bernard:
Digital Communications.
Fundamentals and Application.
Prentice-Hall, Englew. Cliffs, N.J. 1988.

[4] Stallings, William:
Handbook of Computer Communications Standards.
Local Area Network Standards. Vol. 1,2,3, 2nd Edition.
Howard W. Sams and Company Carmel, USA.

[5] Cooley, J. W.-Tukey, J. W.:
An algorithm for the machine calculation of
complex Fourier series.
Mathematics of Computation, 1965.

[6] Brigham, E. Oren:
The Fast Fourier Transform and its Application.
Englewood Cliffs, Nj, Prentice Hall Inc., 1988.

[7] Casas, E. F.–Leung, C.:
OFDM for Data Communication Over Mobile Radio
FM Channels – Part I:
Analysis and Experimental Results.
IEEE Transactions on Communicaations,
Vol. 39. No.5., May 1991.

[8] Casas, E. F. - Leung, C.:
OFDM for Data Communication Over Mobile Radio
FM Channels – Part II: Performance Improvement.
IEEE Transactions on Communicaations,
Vol. 40. No.4., April 1992.

Hírek

A **Siemens PenPhone** egy háromsávos mobiltelefon és egy toll keveréke. Az írótollat formázó, 14 centiméteres „tollofon” képes felismerni és elmenteni a kézzel írott számokat és üzeneteket – függetlenül attól, hogy mire jegyeztük le azokat. Ha éppen nem esik a kezünk ügyébe semmilyen írófelület, a beépített hangfelismerő is aktiválni tudja a készüléket. Emellett kihangosítót, valamint hangvezérlő funkciót is beleépítettek, és Bluetouth-szal kapcsolódik kézi számítógépünkhöz vagy a fejhallgatóhoz.

A **Bluetooth Advanced Pen Input** MMI lehetővé teszi, hogy igazán kreatív MMS-üzeneteket készítsünk. Segítségével belerajzolhatunk vagy jegyzetelhetünk a képüzenetünkbe. A rajzokat és a szavakat automatikusan olyan méretűvé alakítja a készülék, hogy MMS-ben elküldhető legyen, így aztán semi sem szab gátat a fantáziánknak.

Az **Assisted Global Positioning System** (A-GPS) technológiát a G3 mobilok számára fejlesztette ki a Siemens. A GPS vevő és a cellurális hálózat közötti kommunikációra épülő technológia lehetővé teszi a helymeghatározáshoz kapcsolódó alkalmazások szélesebb körű használatát. Így a telefon képes lesz navigációra, flottairányításra, nyomonkövetésre, de kipróbálhatjuk rajta az interaktív, többszereplős játékokat is. Ezentúl pedig már nem fordulhat elő velünk az sem, hogy eltévedünk egy idegen városban, hiszen a telefonunk mindig pontosan tudni fogja, hol vagyunk.

Routing protokollok hatékonysága

KURUC GÁBOR
Vodafone Magyarország Rt.
gabor.kuruc@vodafone.com

LÓJA KRISZTINA
BME, Távközlési és Médiainformatikai Tanszék
loja@math.bme.hu

Reviewed

Kulcsszavak: késleltetés és sávszélesség, gráfok, Nash-egyensúly

A routing kérdései élesen vetődnek fel napjaink mobil távközlésében. Az új és egyre intelligensebb rendszerek lehetővé teszik, hogy több alternatív útvonalat használjanak fel a forgalom továbbítására egyidőben. Így ezek a hálózatok egy többszörös elérésű hálózatot alkotnak, melyeknél fontos az optimális forgalomirányítás megtalálása. A problémák hasonlóak fix és mobil hálózatokban egyaránt. Mindezek felvetik a kérdést: található-e optimális megoldás, és ha igen, akkor az egyértelmű-e?

1. Absztrakció

A cél egy olyan absztrakt hálózat megalkotása, mely lehetővé teszi a routing algoritmusok modellezését és összehasonlítását. Így ebben a modellben elhanyagoljuk a routerek közti adminisztratív jelzés-kapcsolatot. Mivel a cél a QoS vizsgálata, ezért csak QoS-t igénylő fix sávszélesség-igénnyel jellemezhető forgalmat tételezünk fel (Mivel a QoS-t igénylő valósidejű forgalom teljes ideje alatt fent kell tartani az igényelt sávszélességet).

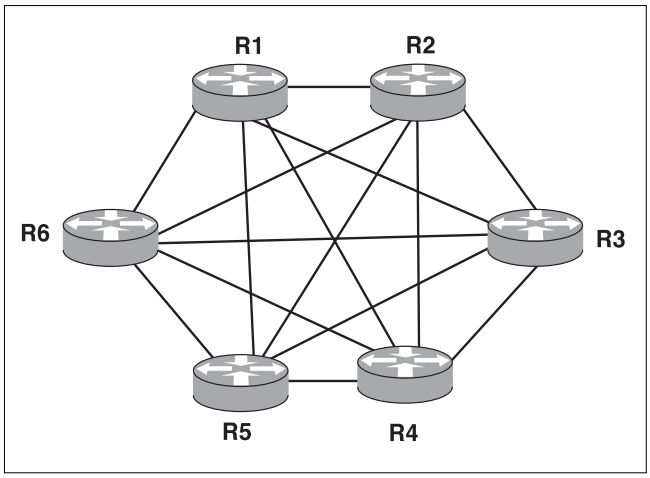
Vizsgálataink során a QoS igényeket maximális megengedett késleltetéssel (d_p) és sávszélesség igénnyel (w_p) jellemezzük P útvonalon.

Tételezzünk fel egy zárt rendszert, ahol R darab router irányítja a forgalmat. A $G(V,E)$ gráf topológiában $||V||= R$, a gráf pontjai a routereknek felelnek meg és E jelöli az élhalmazt.

1.1. Egyszerűsítések

A routerek tároló és feldolgozó képességét tekintsük korlátlannak. A routerek információcseréje nem jelent többletforgalmat.

1. ábra Egy 6 routerből álló hálózat



A gráfban lévő élek száma:

$$\|E\| = \frac{\|V\|^2 - \|V\|}{2}$$

Egy forgalomnak többször is érinteni ugyanazt a routert nincs értelme, ezért ezeket az útvonalakat kizárjuk. Ebben az esetben két router közötti útvonal maximum R-1 szakaszból állhat.

$$k = \sum_{n=0}^{R-2} \frac{(R-2)!}{(R-2-n)!}$$

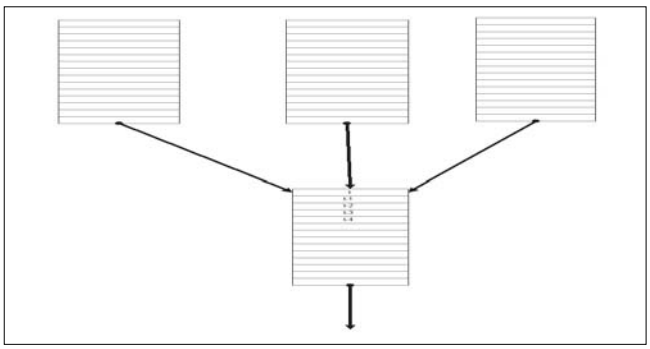
Maximum k darab útvonal képzelhető el két router között. A szakaszok minőségét egy B_l a forgalom függvényében rendelkezésre álló maximális sávszélességgel és d_l késleltetéssel jellemezhetjük. $\hat{B}_l$ az l ($l \in E$) szakasz névleges sávszélessége, hasonlóan $\hat{B}_p$ a p útvonalon elérhető névleges sávszélesség, vagyis a szakaszokhoz tartozó legkisebb névleges sávszélesség. Természetesen p útvonal jellemzőit az őt alkotó l szakaszok jellemzői határozzák meg [1,2].

$$\hat{B}_p = \min_{l \in p} \hat{B}_l$$

$$d_p = \sum_{l \in p} d_l$$

1.2. Késleltetés és sávszélesség

A késleltetés több tényezőből tevődik össze. A legegyszerűbben megérthető az átviteli közegben a jel korlátos haladási sebességéből származó késleltetés. Ez független a vonal sávszélességétől és a kihasználtságtól, csak a közegtől és a távolságtól függ. Ez a késleltetés elhanyagolható, ezért nem képezi részét vizsgálódásainknak. A jeltovábbítási sebességből (sávszélesség) és a terhelésből adódó késleltetés viszont meghatározó. Ez a gyakorlatban azt jelenti, hogy a kimeneti interfészen lévő várakozási sor hosszát növeli a beérkező adatmennyiség, és csökkenti a kimenő adatmennyiség. A várakozási sorban összegyűlt, továbbításra váró adatok mennyisége határozza meg a késleltetési időt.



2. ábra Várakozási sorok a kimenő interfészeken

A *2. ábrán* látható, hogy a routerek kimenetén lévő sorokból a szakaszok sebességétől függően kerülnek ki az adatok, hogy a következő router kimenetén egy újabb sorba kerüljenek.

Ha a bitsebesség reciprokát vesszük, akkor megkapjuk az egy bit átviteléhez szükséges időt. Minden bitet át kell vinni, így az összes idő az összes forrásból érkező összes bittel arányos.

$$d_l = \frac{\sum_i w_i^l}{\hat{B}}$$

Vagyis d_l egy szakasz késleltetése, feltételezve, hogy $1/\hat{B}_l$ időnként kapuzza ki a biteket az átviteli útra.

Feltesszük, hogy véletlenszerű, kvantitatív, csomagokra bontott adatfolyamok együtteséről van szó, és egy szakaszhoz Poisson-eloszlás szerint érkeznek a csomagok. Ezek továbbításának ideje az időegység alatt érkezett adatmennyiség és a bit-idő szorzata.

A d_p teljes útvonalra értelmezett késleltetés számításánál elhanyagoljuk a nem forgalmi viszonyokból adódó konstans késleltetéseket. Így a késleltetés az útvonal szakasz-késleltetéseinek összege, vagyis:

$$d_p = \sum_{l \in P} \frac{\sum_i w_i^l}{\hat{B}_l}$$

Itt a szakaszokon a más útvonalon, más forrással és nyelővel rendelkező jelfolyamok terhelését is beszámítjuk, hiszen egy szakasz eltérő útvonalak számára is lehet közös. Ahol nincs a routerek között összeköttetés, ott $\hat{B}_p = 0$. Egy forgalom igényre jellemző a *max* d_i és *min* w_i.

Az összes lehetséges útvonal, ami a két routert összeköti, egy *P* halmaz elemei. Maguk az útvonalak is meghatározzák azon szakaszoknak egy halmazát, melyek részei az útvonalnak:

$$P = < p^1, p^2, ..., p^i > \quad \text{és} \quad p^i = < l_1^i, l_2^i, ..., l_{n_i}^i >$$

Ez azt jelenti, hogy P^i útvonal *l* szakaszokból áll,

$p^i \subset E$, ahol és $d^i = \sum_{l \in p^i} d_l \le d_k$

ahol a választható útvonalak száma:

$$\|P\| = \sum_{n=0}^{R-2} \frac{(R-2)!}{(R-2-n)!}$$

Vagyis $||P||$ darab útvonalból azok az elfogadhatóak, melyek a forrást és a nyelőt kötik össze és kielégítik a *d* késletetés- és *w* sávszélesség-kritériumot.

A forgalmat kezdeményezők célja a saját forgalmuk késleltetésének minimalizálása. Ha az útvonalakat azok kiindulási pontjában vizsgáljuk meg a késleltetés szerint, vagyis a költséget az átviendő forgalom és a különböző útvonalokon rendelkezésre álló sávszélesség szerint ítéljük meg, könnyen megtaláljuk a helyileg gazdaságos megoldást. Az a kérdés, hogy ha *n* darab forgalmunk van egy adott hálózatban, hogyan lehet megtalálni azt a forgalmi elrendezést, ami a legkisebb közös költséggel (SC – Social Cost) jár. Ez az érték azt mutatja meg, hogy milyen felvett költséggel jár az összes szereplő részére az elfogadható költség biztosítása egy többszörös elérésű hálózatban.

$$SC(W,F) = \sum_{<p_1 \dots p_n> = H^n} \left(\prod_{k=1}^{n} f_k^{p_k} \cdot \max_{p \in P} \sum_{l \in p} \frac{\sum_i w_i^l}{\hat{B}_l} \right)$$

A H^n egy olyan halmaz, ami az *n* darab forgalomhoz tartozó útvonalhalmaz elemeiből P^1-től P^n-ig és minden $P^i = < p^i_1, p^i_2, ..., p^i_{k_i} >$ a teljes kombinációt tartalmazza.

Tehát minden kombinációt megvizsgálunk, ami az összes forgalom egy-egy lehetséges útvonalát jelenti. (Ha útvonalak felvételekor egy korábban meghatározott, absztrakt hálózatot használunk, akkor minden forgalomhoz azonos számú (*k*) útvonalat lehet találni. Így k^n darab kombinációt kell megvizsgálni.) A forgalmak darabszáma *n*, a forgalmi halmaz *W,* és *F* az útvonal-választás valószínűségi halmaza. *W* forgalmi halmaz meghatároz *n* darab forgalmat (w_1, w_2, …, w_n), amelyeknek eltérő sávszélesség és késleltetés igénye van, illetve különbözhet a forrás és nyelő routere [3].

Az *F* halmaz meghatározza a kívánt indító- és célrouterek között választható útvonalakhoz tartozó választási valószínűséget (f_1, f_2, …, f_n). Vagyis minden útvonal más-más valószínűséggel lesz használatba véve. Nagy forgalom esetén ez megadja a forgalom megosztásának arányát. Ha a protokoll nem támogatja a forgalom megosztását, akkor csak egy útvonalat fog kijelölni a továbbítására, vagyis csak f_k^p érték lesz 1, a többi pedig nulla.

A forgalmi viszonylatokhoz választható útvonalak összes lehetséges kombinációját megvizsgálva, a kombináció választásának valószínűségét összeszorozva a fellépő maximális késleltetéssel, megkapjuk ehhez a forgalomhoz és választási eljáráshoz tartozó várható késleltetést. A választásokhoz tartozó valószínűségek szorzata megadja, hogy egy adott forgalmi helyzet kialakulásának mi a valószínűsége.

Természetesen f_k^p értéke csak akkor tér el nullától, ha az útvonal megfelel a forgalom számára, vagyis rendelkezésre áll megfelelő sávszélesség.

Ha *R* a routerek száma, és a forgalmakat irányonként megkülönböztetjük, tehát

$p_{(a,b)} \neq p_{(b,a)}$, $w_{(a,b)} \neq w_{(b,a)}$, akkor

$$\|P\| = (R-1)\cdot R\cdot \sum_{n=0}^{R-2} \frac{(R-2)!}{(R-2-n)!}$$

(irányított teljes gráf) a lehetséges útvonalak száma az *R* darab router között.

Hangsúlyozni kell azt a különbséget, hogy míg az irodalomban általában a késleltetések összegét minimalizálják [1], mi a legnagyobb késleltetést vesszük figyelembe. Ezt az teszi indokolttá, hogy a valós idejű, például beszédforgalomnál mindenki számára biztosítani kell az előírt minőséget.

2. Routing protokollok döntési mechanizmusa

A jelenleg használt dinamikus routing protokollok megpróbálják a legrövidebb, legnagyobb sávszélességet biztosító, vagy egyéb legkisebb szubjektív költséget jelentő útvonalat megtalálni. Ezek hajlamosak egy útvonalat, vagy útvonal-szakaszt túlértékelni, és a rá irányított túl nagy forgalommal elrontani a jellemzőit. Léteznek QoS-alapú útvonalirányító eljárások, melyek több útvonalat választanak, de véletlenszerűen választják ki a forgalomhoz az útvonalat, és nem veszik figyelembe a foglalásokat.

2.1. Nash-egyensúlyi folyamok

A különböző útvonalakon haladó forgalmak együtt alkotják a hálózati folyamot. Egy hálózati folyamot Nash-egyensúlyinak (vagy Nash-folyamnak) hívunk, ha egy felhasználó sem tud úgy útvonalat változtatni, hogy javítson a késleltetésén. Nash-egyensúlyi folyam minden hálózatra létezik és lényegében egyértelmű, azaz minden Nash-folyamnak azonos az összegzett késleltetése, amit úgy kapunk, hogy minden szakaszon összeszorozzuk a késleltetést a forgalommal, majd ezt összegezzük.

Nash-folyam esetében bármelyik két útvonalat tekintve igaz az, hogy ha az egyik útvonal forgalma pozitív, azaz nullánál nagyobb, akkor késleltetése nem lehet nagyobb a másik útvonalnál. A Nash-folyam különböző útvonalain a késleltetés és forgalom szorzata azonos, ha a forgalom tetszőlegesen kis egységekre bontható (feltesszük, hogy sok user használja a hálózatot és az egyes felhasználók forgalma egyenként elhanyagolható).

Mivel előfordulhat olyan folyam, melyben saját késleltetését útvonalváltással egyik forgalom sem tudja csökkenteni, azonban a többi késleltetését igen; a Nash-folyamok nem feltétlenül optimálisak az összegzett késleltetés tekintetében. Erre egészen egyszerű példa adható egy forrással, egy nyelővel és mindössze két közöttük haladó párhuzamos éllel. Az egyik él késleltetése a forgalomtól függetlenül legyen 1, a másikon a késleltetés a forgalom értéke. Egységnyi forgalmat kell eljuttatni a forrásból a nyelőbe. Optimális az a folyam lenne, melyben mindkét élen 1/2 egységnyi forgalom halad (így az összkésleltetés 1/2*1/2 + 1/2*1 = 3/4), a Nash-folyam esetében a forgalom egésze az első élen halad, így az összegzett késleltetés 1.

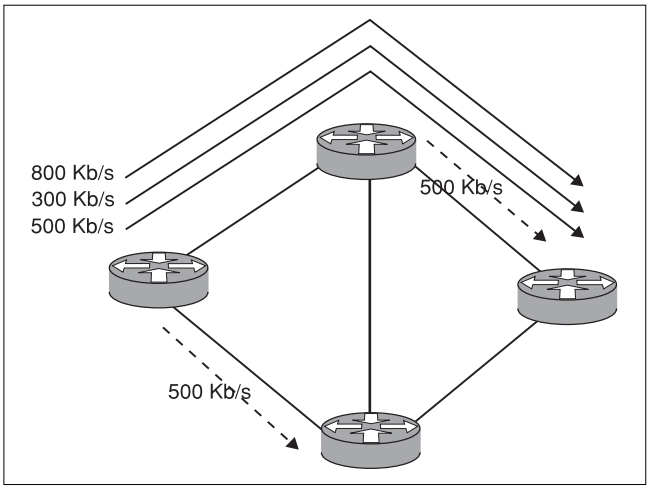
2.2. Példák a routing protokollokra

Hagyományos SPF (Shortest Path First) routing

Nézzünk egy egyszerű SPF routing példát. Tegyük fel, hogy valamennyi összeköttetés 1,5 Mb/s átviteli kapacitású. Mivel a router csak a vonali költségeket figyeli, mind egy útvonalra küldi a forgalmat, hisz csak egy legrövidebb utat ismer és minden forgalmat egyként kezel.

A probléma az, hogy nem áll rendelkezésre a kívánt sávszélesség. De vizsgáljuk meg a SC értéket is.

SC = 1,6/1,5 + 2,1/1,5 = 3,7/1,5 = 2,466.



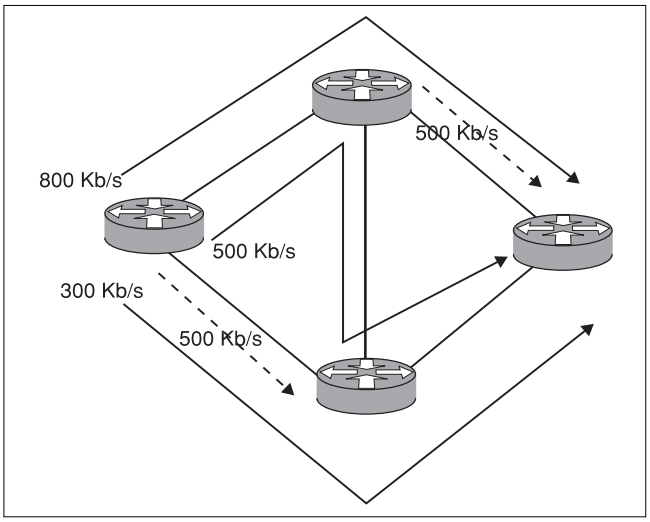
3. ábra Példa SPF routingra

Látható, hogy ez a megoldás nem optimális és nem is Nash-folyam, hiszen ha valamely forgalom a másik routeren keresztül menne a nyelőbe, akkor minden forgalom késleltetése csökkenne.

Egyszerű QoS-routing

Nézzük meg ugyanezt a példát QoS-alapú routinggal, ami csak lokálisan vizsgálja a költségeket.

4. ábra Példa QoS routingra



Ez már figyelembe veszi a szükséges sávszélességet és a meglévő terheléseket.

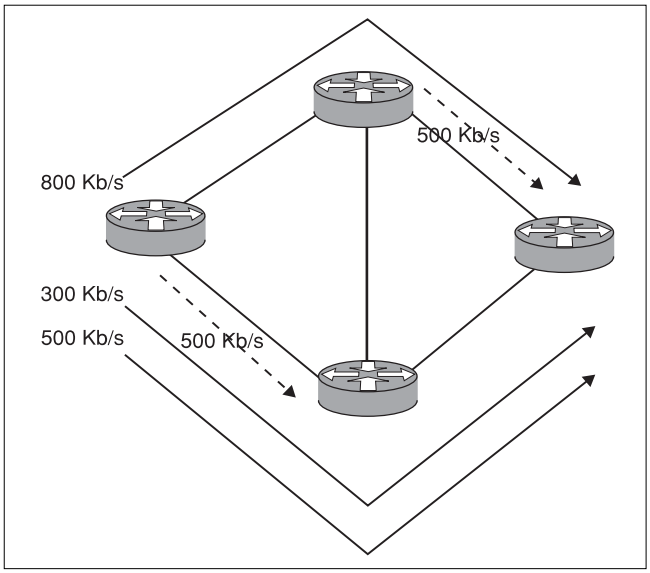
SC = max (1,3/1,5 + 1,3/1,5; 1,3/1,5 + 0,5/1,5 + 0,8/1,5; 0,8/1,5 + 0,8/1,5) = 2,6/1,5 = 1,73.

Így a 1,5 Mb/s átviteli sebességű vonalak már elégségesnek bizonyulhatnak. A QoS-routing jól működik. Azonban az együttes költség túl magas, hiszen egy forgalom egy hop-pal többre kényszerült. Ez Nash-folyam, mert egyik forgalmat sem lehetne más útvonalra terelni úgy, hogy késleltetése csökkenjen. Látni fogjuk, hogy mégsem ez az optimális megoldás.

Egy optimális QoS-routing

Az ideális elosztás a következő lehetne, de ehhez a routernek túl kellene látnia a saját határain:

SC = max (1,3/1,5 + 0,8/1,5; 1,3/1,5 + 0,8/1,5) = 2,1/1,5 = 1,4.



5. ábra Optimális QoS routing

Látható, hogy a két köztes router közötti kapcsolat itt kihasználatlan marad. Ha ezt a szakaszt az előző esetben kitöröltük volna a gráfból, jobb megoldást kaptunk volna. Ehhez hasonló egyszerű példát adott Braess olyan hálózatra, melyben új útvonal hozzáadása a hálózathoz növeli a költséget (a késleltetések összegét) a Nash-folyamban. Ezt a jelenséget hívjuk Braess-paradoxonnak [4,5,6].

Ezen a példán a döntések minden forgalomhoz egyértelműek. Ellenben ha valós folyamokról van szó, ahol a döntési mechanizmus egyértelműen a költségek minimalizálását tűzi ki célul, kis valószínűséggel elküldhet egy forgalmat olyan kerülőútra, ami biztosítja a SC minimalizálását, de a kiválasztott forgalom szempontjából túl nagy késleltetést okoz.

2.3. Nash-folyamok és optimális folyamok

A Nash-folyam és az optimális folyam késleltetésének viszonyáról a következőket tudjuk [1]. Ha a késleltetés lineáris függvénye a forgalomnak minden élen, akkor a Nash-egyensúlyi folyam késleltetése legfeljebb 4/3-a az optimális folyam késleltetésének. Ez a korlát éles, ezt mutatja a 2.1-es szakaszban ismertetett példa. Látható, milyen kevés szerepet játszik a hálózati topológia, hiszen ez a 4/3-os arány a két linket tartalmazó hálózatban állt elő, és a két késleltetés aránya nem lehet nagyobb, akármilyen bonyolult hálózatot vizsgálunk. Ha csak azt tesszük fel a késleltetésről, hogy nemnegatív, folytonos és nemcsökkenő függvénye a forgalomnak, akkor ez az arány tetszőlegesen nagy lehet. Ha például két él vezet a forrásból a nyelőbe, és az első élen a késleltetés a forgalom mennyiségének *k*-adik hatványa, a másik élen pedig a forgalomtól függetlenül 1, akkor a Nash-folyam költsége 1, mert a forgalom egésze az első élen halad, pedig tetszőlegesen kis költséggel is lebonyolítható a forgalom, ha az első élen 1-ε forgalom halad, a másik élen pedig ε, ahol ε kis pozitív szám. Itt ismét egy két szakaszból álló példa mutatja, hogy a hálózat komplexitása nem játszik szerepet. A késleltetésfüggvények majdnem minden osztályára igaz, hogy a legrosszabb Nash/optimális arány megvalósítható kétszakaszos hálózaton. A Nash-egyensúlyi folyam késleltetése legfeljebb akkora, mint a kétszer akkora forgalmat lebonyolító optimális folyamé [1].

Az optimális folyam minimalizálja az összegzett késleltetést, viszont „igazságtalan” egyes forgalmakkal szemben, azaz lehet olyan forgalom, ami sokkal nagyobb késleltetést szenved el az optimális folyamban, mint a Nash folyamban [2]. Tegyük fel, hogy két él vezet a forrásból a nyelőbe, az első késleltetése 2(1-ε), a másiké megegyezik a forgalommal. A Nash-folyamban minden forgalom a második élen halad, így az összkésleltetés 1, az optimális folyamban ε (ε kis pozitív szám) egységnyi forgalom halad az első élen és 1-ε egységnyi a másikon, így az összegzett késleltetés $1-\varepsilon^2$. Látható, hogy a Nash-folyam összkésleltetése nagyobb, de minden forgalom késleltetése egy, míg az optimális folyamban az optimum elérése érdekében az első élre kényszerített csomagok késleltetése 2-2ε.

Tételezzük fel, hogy a forgalomtól függő késleltetés ($l_e(x)$) és a forgalom (x) szorzata konvex minden élen. Ennek a forgalom szerinti parciális deriváltját hívjuk határköltség-függvénynek: $d/dx(x^* l_e(x))$. Egy folyam optimális, ha Nash-egyensúlyt képez ugyanabban a hálózatban, ugyanakkora összforgalom mellett, ha a késleltetés a határköltség-függvény [2].

3. Routing-költség

Tételezzünk fel *n* darab adatfolyamot, amely a hálózaton keresztül halad. Ezeket az adatfolyamokat a *W* halmaz $<w_1, w_2, \ldots, w_n>$ elemei reprezentálják. A továbbiakban feltételezzük, hogy minden w_i-re és B_l-re igaz, hogy

$$\max_i w_i < \min_l \hat{B}_l, \quad \text{ahol} \quad w_i \in W \quad \text{és} \quad l \in E .$$

Ez azt jelenti, hogy minden fellépő forgalom sávszélessége egyenként kisebb, mint bármelyik szakasz sávszélessége. Tehát torlódást csak több különböző, egy-

időben fellépő forgalom okozhat. Egy önálló adatfolyam csak más adatfolyam lefoglalt sávszélessége miatt kényszerülhet más utat választani.

Ha van egy $w_{(s,t)}$, vagyis egy *s*-ből *t*-be tartó forgalmunk, akkor az kijelöl *P*-ből egy $P^{s,t}$ halmazt, melynek elemei $<p^{s,t}_1, p^{s,t}_2, \ldots, p^{s,t}_x>$ csupa olyan útvonal, ami megfelel a forgalom továbbítására. Ez a halmaz tartalmazza az összes útvonalat, mely elvezethet *s*-ből *t*-be (természetesen ezek az útvonalak csak olyan útvonalak lehetnek, melyeken rendelkezésre áll a kívánt sávszélesség). Minden $p^{s,t}_x$ meghatároz egy $L^{p(s,t)x}$ halmazt, melynek elemei $<l_1, l_2, \ldots, l_i>$ a routerek közötti szakaszok. $L^{p(s,t)x}$ az *E* élhalmaznak egy részhalmaza.

$$L^{p(s,t)_x} \subset E$$

Ha két *w* forgalomnak a célja, illetve forrása nem azonos, akkor *P* halmazuk eltérő és nem lehet a halmazokban azonos útvonal. De két eltérő *p* útvonalnak lehetnek közös szakaszai (*l*-ek). Két forgalom, w_1 és w_2 akkor okoz torlódást, ha *l* szakaszon $(w_1+w_2) > B_l$. A routing protokollok célja ennek a helyzetnek az elkerülése.

Fogadjuk el, hogy egy routing protokoll leírható egy olyan függvénnyel, ami a hálózatról ismert információkból (*L* és $\{B_l\}$ halmazból) az *F* döntési halmazt állítja elő (f^p általában 1 vagy 0 egy egyszerű routing protokollnál). Bonyolultabb routing protokollok figyelembe tudják venni a vonali terheltséget, tehát közvetetten a *W* halmaz által reprezentált terhelést is. Ezek szerint a *W* forgalmi halmaz meghatároz egy *w*-kből álló forgalmi halmazt. w_i kijelöl egy P^w útvonalhalmazt, mely a forgalom irányításának megfelel. P^w halmaz elemei $<p^w_1, p^w_2, \ldots, p^w_x>$ Ezáltal a L^{P_i} halmaz elemeinek w_i-vel növekszik a terhelése. Ez visszahat a többi *w* forgalmakhoz tartozó $P^{s,t}$ halmazra, melyek visszahatnak az *F* döntési halmazra.

Az a routing protokoll fog a legjobb hatásfokkal működni, ami olyan játékszabályok szerint tudja a *w*-khez tartozó $p^{s,t}$-ket társítani, hogy az együttes eredmény a legkisebb SC értéket eredményezze.

$$SC(W,F) = \sum_{H^n} \left(\prod_{k=1}^{n} f_k^p \cdot \max_{p \in P} \sum_{l \in p} \frac{\sum_i w_i^l}{\hat{B}_l} \right)$$

4. Az útvonalválasztás valószínűségi változókkal

Mint az előző fejezetekből kiderül, a SC értéke, mely a szállítani kívánt forgalomhoz és routing protokollhoz tartozó költséget reprezentálja, két tényezőtől függ. Az egyik az elképzelhető útvonal-kombinációkhoz tartozó maximális késleltetés, a másik a kombinációhoz tartozó választási valószínűség. Ezek szorzatainak az összege határozza meg a kollektív költséget. Az útvonalak maximális késleltetése attól függ, hogy a kiválasztott útvonal-kombináció a különböző forgalmakat miként osztja meg a kiépített szakaszokon. Ha a legrövidebb útvonalat ajánlja mindenkinek (SPF), akkor a szakaszkésleltetés lesz nagy a terheléstől. Ha túl sok szakaszt illeszt be az útba, akkor az útvonalat alkotó szakaszok együttes késleltetése lesz túl nagy [3].

4.1. Legjobb variáció

Kérdés, hogy milyen esetben létezik egy és csak egy optimális megoldás. A variációk minden w_i forgalomhoz tartozó útvonalakból egy-egy útvonal kiválasztásával kapott halmaz. Ha veszünk egy egyszerű protokollt (SPF), akkor az minden w_i-hez csak egy útvonalat fog helyesnek találni, az összes többit elutasítja. Így az *f* értékek 0 vagy 1-esek lesznek. Az *f* értékek szorzata pedig csak akkor lesz 1, vagyis 0-tól különböző, ha azt a kombinációt veszi fel, amely azokat az útvonalakat tartalmazza, melyeket az adott forgalomhoz a legjobbnak ítélt meg a protokoll.

$$\prod_{k=1}^{n} f_k^p$$

Ebben az esetben a döntést olyan események befolyásolják, amiket az útvonalak struktúrája, illetve a források és nyelők elhelyezkedése, azaz a hálózat felépítése fixen meghatároz, tehát semmilyen valószínűségi esemény bekövetkezése sem befolyásolja, így a forgalmak bekövetkezése és időzítése sem.

4.2. A többesélyes út

Abban az esetben beszélhetünk több útról, ha valamilyen okból a lehetséges útvonalakból nem egynek ítél teljes bizalmat a dinamikus routing protokoll. Például ha a vonali terheléstől függően változhat az útvonalválasztás (QoS routing). Így a *W* halmazban található forgalmak időzítése eltérő útválasztásokat eredményezhet.

Lehetőség van a forgalmakat elosztani több útvonal között. Ebben az esetben *f*-ek értékei 0 és 1 között lehetnek, attól függően, hogy a szóba jövő útvonalak közül melyiket milyen valószínűséggel fogja kiosztani az útvonalhalmazhoz tartozó w_i forgalomnak (milyen arányban osztja meg a forgalmat az útvonalak között).

5. A választások értéke

5.1. Direkt választás

Az 4.1-es fejezetben taglaltaknak megfelelően egyszerű a választás. A routing protokollok itt csak a hálózat felépítéséről gyűjtött információk szerint, előre meghatározott útvonalon továbbítják az információt. Itt a közös költséget csak az befolyásolja, hogy a protokoll milyen hatékonysággal találja meg a megfelelő utakat.

Ezek a megoldások is fontosak lehetnek olyan hálózatoknál, ahol az igény egy egyszerűbb routing. Ebben az esetben is érdemes olyan routing protokollt használni, ami az adott forgalmi viszonyok mellett a legkisebb SC értéket eredményezi.

Ezt azok a protokollok tudják nyújtani, melyeknek a legalaposabb áttekintésük van a hálózat felépítéséről, és figyelembe veszik a többi router döntési mechanizmusát is.

5.2. Több útvonalból történő választás

Itt a helyzet alaposan megváltozik, és sok érdekességet nyújt. Egy adott w_i forgalomhoz tartozó különböző p_i útvonalakhoz tartozó f_i valószínűségi változók érdekes képet mutatnak. Összegük 1, mivel a forgalomnak el kell mennie valamelyik irányba minden körülmények közt.

A forgalmak lebonyolításánál a router itt is megpróbálja a kisebb költségű útvonalakat előnyben részesíteni. Ezeknek az *f* értékeknek forgalmi halmazként vett kombinációiból csak azok befolyásolják a közös költséget, amelyik útvonal kombináció *(H)* valamilyen részét a forgalomnak szállítja tehát:

$$\prod_{k=1}^{n} f_k^p > 0$$

Ahol ez az érték nulla, az azt jelenti, hogy a kombináció tartalmaz egy olyan útvonaltervet, mely nem felel meg a továbbítandó forgalomnak.

Ez esetben következőkre kell figyelemmel lenni:

- A kiválasztott kombinációt alkotó utak hossza.
- A forgalmak által közösen használt szakaszok.
- A felhasznált szakaszok sávszélessége a rá irányított forgalomhoz viszonyítva.

Az SC értéket ezeknek a feltételeknek a figyelembe vételével lehet csökkenteni.

Ha ismerjük a forgalmak egymásra hatását, akkor kiszámíthatóak azok a játékszabályok, ami alapján a protokoll a forgalmakhoz útvonalat társít, és a kívánt minimális SC értékhez tartozó *F* halmazt állítja elő.

A *W* halmaz elemeinek útvonalanként egymásra hatása próba-sávszélesség foglalással is meghatározható, de léteznek már olyan eljárások, melyek alapján feltérképezhető a topológia. Ezek után a forgalmi osztályokra bontott minta-*W* halmazra a kívánt SC értékek érdekében meghatározhatók az irányítási szabályok.

6. Eredmény

A leírtak figyelembevételével lehetséges olyan protokollt alkotni, ami a helyi statisztikákból, illetve a többi routertől szerzett információkból megtalálja a minimális költséghez tartozó forgalmi elrendezést. Szükséges hozzá a hálózati topológia és a többi résztvevő által statisztikai, vagy egyéb megfontolások alapján megalkotott forgalmi osztályok, ezek segítségével lehet megtervezni az útvonalat.

Mint láttuk, a Nash-folyam általában nem optimális. Az optimális folyam azonban csak az összegzett költségeket minimalizálja, egyes csomagok késleltetése sokkal nagyobb lehet, mint a Nash-folyamban. Ez mutatja, hogy akármilyen tetszetős az optimális routing, a gyakorlati alkalmazásban nem alkalmazható, ha biztosítani akarjuk mindenki részére a szolgáltatást. Ellenben látható, hogy a Nash-folyamok 30%-kal nagyobb költséget eredményezhetnek a hálózatban, ami költségérzékeny esetben nem megengedhető.

Az igazi megoldást a kettő között kell keresni. Ezért a dolgozatban definiált SC értékünk a legnagyobb késleltetést veszi figyelembe, hiszen a távközlési hálózatban minden forgalomnak időben el kell érnie a címzettet.

Az optimális routing költségszámításában a közös költséget az egyének költségeinek összegeként értelmezik. Ennek optimuma viszont eredményezheti bizonyos forgalmak kiéheztetését, ha ez más forgalmaknál nagyobb előnnyel jár. Ez valósidejű forgalmaknál nem felhasználható. De léteznek olyan elemek, mint például a routing protokollok feldolgozásának erőforrás-igénye, aminek kielégítését segítheti egy ilyen megközelítés.

Irodalom

[1] Tim Roughgarden, Éva Tardos:
How Bad Selfish Routing?
www.cs.cornell.edu/timr/papers/routing.ps,
Journal of the ACM 49(2), pp.236–259. 2002.

[2] Tim Roughgarden:
How Unfair is optimal Routing?
www.cs.cornell.edu/timr/papers/unfair.pdf,
Proceedings of the 13th Annual Symposium
on Discrete Algorithms, pp.203–204. 2002.

[3] Marios Mavronicolas:
Game-Theoretic Approaches to Network Routing:
A Primer Tutorial for Euro-Par (Germany, 2002.)
http://europar.upb.de/tutorials/tutorial01.html

[4] S. Das, M. Gerla, S. Lee, G. Pau, K. Yamada, H. Yu:
Practical QoS Network System with Fault Tolerance
www.cs.ucla.edu/~nrl/hpi/papers/2002-spects-0.pdf,
Proc. International Symposium on Performance
Evaluation of Computer and Telecom. Systems,
San Diego, 2002.

[5] S. Chakrabarti, A. Mishra:
QoS Issues in Ad Hoc Wireless Networks
www.sce.umkc.edu/~beardc/wireless03/IEEEPapers.htm
IEEE Communications Magazine,
No.2, pp.142–148. February, 2001.

[6] Dean H. Lorenz, Ariel Orda:
QoS Routing in Networks with Uncertain Parameters
www-ee.technion.ac.il/~deanh/infocom98.ps.gz.,
IEEE/ACM Transactions on Networking,
Vol. 6. No.6, pp.768–778. 1998.

[7] Csopaki Gyula, Kuruc Gábor:
Útvonalválasztás, kapcsolástechnika: merre haladunk?
Híradástechnika, 2003/10. pp.16-19., 2003.

A hozzáférés-korlátozott DVB CATV műsorterjesztés alapjai

WEIN TIBOR, műszaki menedzser

HFC Technics Kft.
t.wein@hfctechnics.hu

Kulcsszavak: interaktív fizető tévézés, titkosítási megoldások, kódolás

A többségben hozzáférés-korlátozott műsortartalmak terjesztése, és ennek elektronikai/informatikai infrastruktúrája csak a digitális műsorszórás rendszerébe integráltan valósítható meg. A digitális technika a műsorkínálat nagyságrendi felduzzadását, valamint az interaktív televíziózás műszaki lehetőségeit is magával hozta. Ez a járulékos információs szolgáltatások iránti igényt is felveti. A cikk a vezetékes DVB-be integrált fizető TV alapszolgáltatások rendszertechnikai megoldásait ismerteti.

1. Bevezető

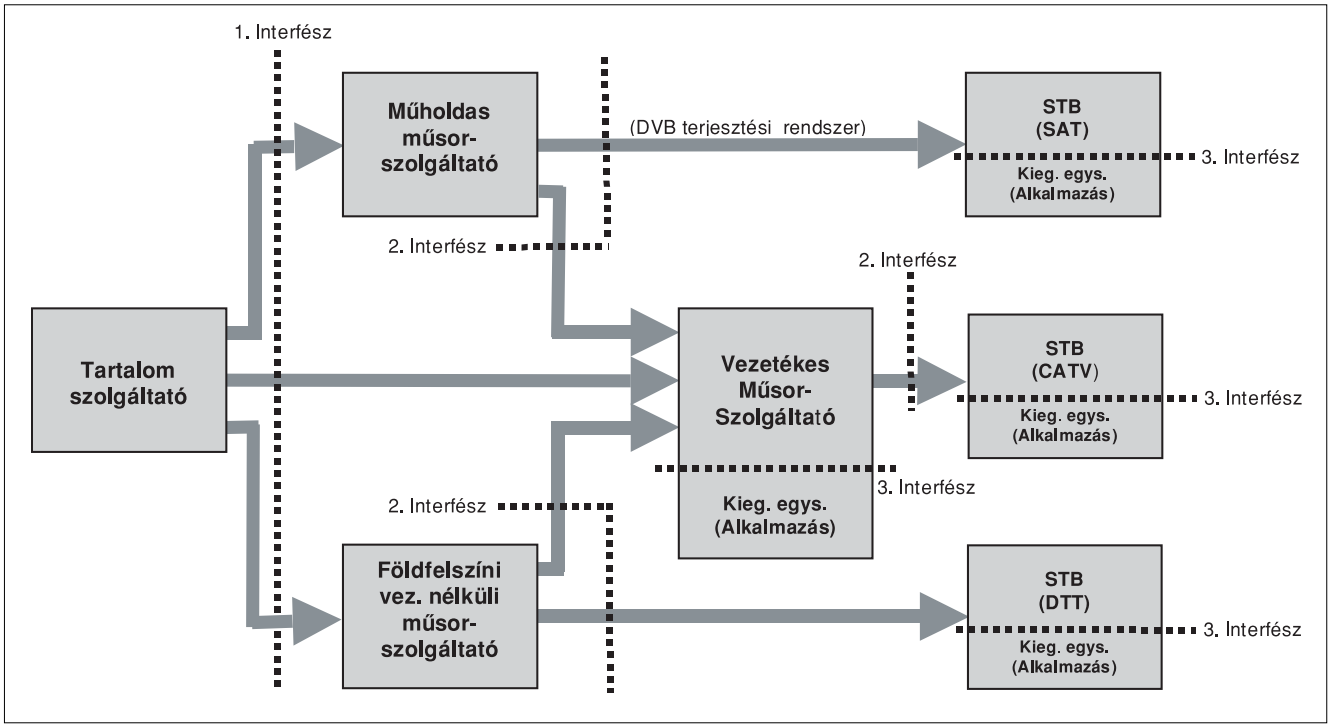
A műsorszórásban és -elosztásban alkalmazott hozzáférés-korlátozás a szerzői jog védelmét jelenti. A hozzáférés-korlátozás infrastruktúrájának megjelenése és elterjedése a felhasználói oldal szempontjából, jóllehet, népszerűtlen, ám elkerülhetetlen folyamat. A vállalkozási alapú műsortartalom előállítás és terjesztés költségeinek megtérülése és kezelése ma már csak hatékonyan működő üzleti modellekre épülhet. Az adminisztratív alapú, közvetett díjbeszedési rendszerek az információs társadalom korában túlhaladottak, a fizetési fegyelem fenntartásának eszközeként egyre hatástalanabbak. Az interaktív fizető tévézés, mint szolgáltatási üzletág kiépítése és működtetése természetesen megfelelő szabályzást igényel.

2. Az átviteli modell

Az *1. ábra* a digitális TV átviteli modelljét szemlélteti. Mint az ábrán látható, a digitális TV átvitel a tartalomszolgáltatók és -terjesztők, valamint a terjesztők és felhasználók közti hagyományos csatlakozási felületek (1. és 2. interfész) mellett egy továbbit (3. interfész) is definiál. Ennek rendeltetése a járulékos alkalmazásokkal kapcsolatos adatok leválasztása az átviteli rendszeren továbbított DVB jelfolyamról. Az átviteli lánc és az alkalmazás közé iktatott 3. interfész az API, a DVB vevőberendezés és a járulékos alkalmazásokat megvalósító kiegészítő egység(ek) csatlakozási pontja.

Az interaktív műsorterjesztés fejlődése folyamán a visszirányú átvitel igénye az 1. és 2. interfészeket is API funkciókkal ruházza fel. (Az ábrán látható átviteli modell

1. ábra A digitális TV átvitel modellje



Fogalmak, meghatározások

API	Applications Programing Interface	Szabványosítás alatt álló átjárás a DVB és az MHP alatt futó alkalmazások között
ASI	Asynchronous Serial Interface	Alapsávi DVB jelfolyamok szabványos csatlakozási felülete
CA(S)	Conditional Access (System)	Hozzáférés-korlátozás rendszer
CAM	Conditional Access Module	Kártyaolvasót tartalmazó PCMCIA/PC modul, melynek feladata az ECM/EMM üzenetek szűrése, konvertálása és továbbítása
CAT	Conditional Access Table	A hozzáférés-korlátozó rendszertől függő, a felhasználói adatokat és a CA leírókat tartalmazó táblázat
CI	Common Interface	Szabványos (EN50221) interfész a CAM és a DVB vevő között
CW	Control Word	Kódszó (kriptografikus kulcs)
CSA	Common Scrambling Algorythm	MPEG-2 kódolású DVB jelfolyam-titkosításhoz alkalmazott algoritmus
DTT	Digital Terrestrial Television	Az OFDM modulációt alkalmazó, DVB-T szabványú földfelszíni digitális televíziózás
ECM	Entitlement Control Message	Hozzáférési kritériumokat és kódszavakat tartalmazó titkosított üzenet (CA rendszertől függően általában 40 és 200 bájt közötti hosszúságú)
ECW	Even CW	Az ECM által szállított páros kódszó
EIT	Event Info Table	Kezdetek, végek és időtartamok időrendi esemény-táblázata
EMM	Entitlement Management Message	A kódkártyát meghatározott hozzáférési kritériumok alapján engedélyező titkosított üzenet, amely az aktuális jogosultsági adatokat tartalmazza
EPG	Electronic Program Guide	Elektronikus műsorkalauz vagy műsorfüzet
FEC	Forward Error Correction	Előre irányú hibakorrekciós eljárás
FTA	Free To Air	Titkosítás nélkül terjesztett programok
IRD	Integrated Receiver & Decoder	DVB-S/-T műholdjeleket videó/audió jelekké visszaalakító professzionális DVB vevőegység
MHP	Multimedia Home Platform	Általános interfész definíció az interaktív digitális alkalmazások és terminálok között
MPEG-2	Moving Pictures Expert Group	Digitális videó tömörített átviteli szabványait kidolgozó munkacsoport
Multicrypt	Multicrypt descrambling	Azon DVB vevő meghatározása, amely egynél több CAS-t kezel, így különböző hozzáférés-korlátozó rendszerek bármelyikével titkosított programok (PES-ek) helyreállítására képes
NIT	Network Information Table	A terjesztő hálózatokra vonatkozó információkat tartalmazó táblázat
NVOD	Near Video On Demand	„Majdnem” igény szerinti videó
OCW	Odd Control Word	Az ECM által szállított páratlan sorszámú kódszó
OFDM	Orthogonal Freq. Division Multiplexing	Ortogonális frekvenciaosztásos multiplexelés
PAT	Program Association Table	A programok azonosítása programszámuk alapján
PCMCIA	PC Module CI Access	A DVB CI és a CAM közötti csatlakozási pontra vonatkozó szabvány (hitelkártya méretű számítógépes kiegészítők csatlakozási felülete)
PCR	Programme Clock Reference	Videó kódolót vezérlő 27 MHz-es órajelből származtatott időzítő jel (90kHz)
PES	Packetised Elementary Stream	A program kódolt audio/video/adat jelfolyama
PID	Packet Identifier	A TS-ben továbbított különböző PES-ek azonosítója
PMT	Program Map Table	A programok elemi jelfolyamainak (PES) azonosító táblázata
PSI	Program Specific Information	A PES-eket és ezek PID-jeit egymáshoz rendelő táblázat, Segítségével a különböző programok elemi jelfolyamai (PES) követhetők nyomon az MPEG TS-ben, A PSI tartalmazza a PAT, PMT, NIT, CAT, ECM és EMM információkat
QPSK	Quadrature Phase Shift Keying	Több állapotú fázisbillentyűzés
RST	Running Status Table	A futó műsorok táblázata
SAS	Subscriber Authorisation Server	Az előfizetői jogosultságokat lefordító CA alrendszer
SCI	Smart Card Interface	A CAM modul szabványos kódkártya interfésze
SDT	Service Description Table	A műsorokat leíró táblázat
SMS	Subscriber Management Server	Az előfizetői adatokat és számla-egyenlegeket kezelő CA alrendszer
SI	Service Information	Szolgálati információk
STB	Set Top Box	Jelátalakító előfizetői vevőkészülék
Simulcrypt	Simulcrypt scrambling	A PES-ek titkosítási eljárása (többszörös CW-továbbítás)
Singlecrypt	Singlecrypt scrambling	A PES-ek titkosítási eljárása (egyenkénti CW-továbbítás)
TDT	Time & Date Table	A pontos időt és dátumot egyezményes formátumban szállító táblázat
TS	Transport Stream	Egy vagy több program PES-eiből multiplexelt összetett jelfolyam
VOD	Video On Demand	Igény szerinti videó

így kétirányúvá válik.) A visszirány ekkor a műsorszolgáltatástól részben független, de szintén hozzáférés-korlátozott „e-...” szolgáltatások (e-banking, e-gaming stb.) adatainak is hordozója lehet. A műsorterjesztés és ezen új szolgáltatások adatfolyamai hozzáférés-korlátozásának megvalósítása azonban közös platformon célszerű.

Jelen cikk a fent vázolt fejlődési folyamat első fázisával foglalkozik, azaz a DVB hozzáférés-korlátozó rendszerek szolgáltató – felhasználó irányú kommunikációjára épülő alapszolgáltatások elvi megoldásait ismerteti.

3. A hozzáférés-korlátozó rendszerek elemei

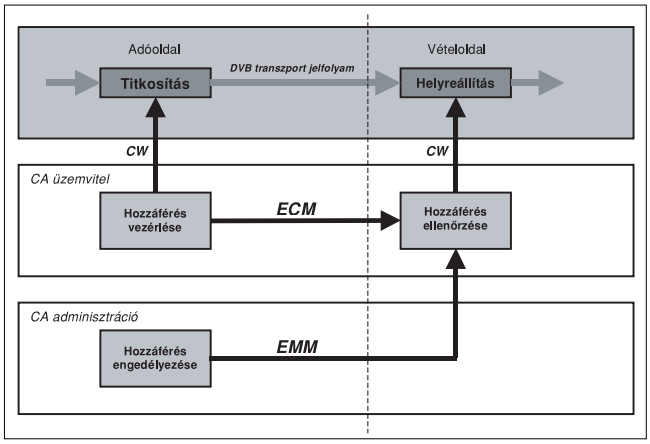
3.1. A hozzáférés-korlátozási alkalmazások kiegészítő egységei

A hozzáférés-korlátozás, mint alkalmazás elsődleges kiegészítő egységének rendszertechnikai elnevezése a **CAM,** amely egy PCMCIA szabványú dugaszolható csatlakozással ellátott modul. Funkciója a titkosított DVB jelek helyreállításának vezérlése a hozzáférési jogosultságok alapján. A PCMCIA felülettel a CAM a DVB vevő CI-jéhez csatlakozik. A CAM típusok többségének másik interfésze egy szabványos kódkártya olvasó interfész (SCI). A különböző CAS-ek CAM-jai ezért nem csereszabatosak. Léteznek azonban már univerzális hardverrel megvalósított CAM típusok is, melyekbe több CAS alkalmazásai letölthetők.

Az API interfész CAS specifikus megvalósítása a DVB vevőben a **CI,** amely lehetővé teszi az eltérő hozzáférés-korlátozó technológiák alkalmazását. A CI a DVB jelfolyamba ágyazott hozzáférési jogosultsági adatokat továbbítja a CAM számára. Egyes továbbterjesztői és végfelhasználói a DVB vevők CAM funkcióit költségtakarékossági céllal szoftver emuláltan (is) megvalósítják. Ezek az adott CAS-hez beépített kártyaolvasóval (is) ellátott típusok. A CI ebben az esetben virtuális.

A térítésköteles műsorkínálathoz való hozzáférési jogosultsági adatok tárolásának elterjedt megvalósítási formája a CAM-ba dugaszolható **kódkártya**. Az ellenőrzés kódkártyás megvalósítási formája különböző kriptografikus eljárások alkalmazásával a környezet manipulálhatatlanságát hivatott biztosítani. A vételoldali hozzáférés ellenőrzését a kódkártyába épített mikroprocesszor hajtja végre. A kódkártya adatait a gyártók az interfész specifikáció (ISO 7816) kivételével – érthető okból – gondosan titokban tartják.

2. ábra A hozzáférés-korlátozás jelzésrendszer-modellje



A műsorjel hozzáférés-korlátozásának lépései a DVB jel átvitel előtti titkosítása az adásoldalon, és a szelektív felhasználói helyreállítás vezérlése a vételoldalon. A **titkosító rendszert** általában a DVB multiplexer egység foglalja magában, melynek egy további szerepe a DVB TS szinkronizációja. A hozzáférés-korlátozás jelzésrendszerének modellje a *2. ábrán* látható.

3.2. Vezérlő rendszer

Szerepe a DVB jel titkosítása szabványos DVB titkosító algoritmussal (CSA) az adóoldalon, valamint – a hozzáférés jogának meghatározása és fennállása esetén – a helyreállítás vezérlése a vételoldalon. Mint az alábbiakban látni fogjuk, a DVB CA titkosítási rendszere hierarchikus, mivel az CSA-val titkosított DVB jelek vételoldali helyreállítását titkos adatokat (CW) szállító és ugyancsak titkosítást alkalmazó jelzésrendszer vezérli. E jelzésrendszer működése alábbi fejezetekben ismertetett információhordozó elemekre épül (v.ö. 2. ábra).

A titkosítás **kódszavak (CW)** segítségével történik. A DVB titkosító algoritmus (CSA) szimmetrikus, az adóoldalon használt kódszavakat ezért továbbítani kell a CAM felé. A CSA-al titkosított DVB jel helyreállításának vezérléséhez használt CW-t rendszerint 10-30 másodpercenként változtatják. A kódkártya ellátása a számára szükséges további információkkal valamint a CAM ellátása a kódszavakkal (a kódkártya közreműködésével) az alábbi két üzenettípus segítségével történik.

Az **EMM** hordozza azon információkat, melyek feltöltik és frissítik a kódkártya memóriáját az igényelt szolgáltatásra vonatkozó jogosultságokkal, hozzáférési kezdet/vég dátumokkal, kriptografikus kulcsokkal stb. Funkcióját tekintve az EMM a tartalomhoz vezető ajtó zárjának „kulcslyuka”.

Az **ECM** a CAM számára küldött **jogosultság-ellenőrző üzenet,** amely a CW-ket titkosítva szállítja. Az ECM ezen kívül tartalmazza az adott programra vonatkozó szolgáltatói, program-hivatkozási és jogosultsági információkat (például program-azonosító, kriptografikus változók, aktuális dátum és idő). A kódkártya ezeket az információkat összeveti a memóriájában tárolt előfizetési adatokkal és dönt a hozzáférés jogosultságáról. Amennyiben a hozzáférés engedélyezett, a kódkártya a helyreállított CW-t kiadja a CAM számára. Az előbbi analógia szerint az ECM a tartalomhoz vezető ajtó zárjának a „kulcsa”.

3.3. Átviteli elemek

A DVB átvitelnél legelterjedtebben alkalmazott szabványos kódolási eljárás az MPEG-2. Az adóoldalon a

stúdióból, vagy videó/audió szerverből induló DVB szabványos kép és hang forrásanyag az alábbi utat járja be:

- MPEG-2 tömörítés/kódolás
- Az MPEG-2 jelfolyamok és a kísérő adatfolyamok multiplexelése TS-ekbe
- Az átviteli közegnek (műhold, kábel, földfelszíni, esetleg egyéb szélessávú) megfelelő moduláció és frekvencia konverzió

A terjesztési rendszerek útján átvitt DVB/MPEG 2 jel (v.ö. 1. ábra) beszerzési, illetve továbbterjesztési eszközei az alábbiak:

- analóg továbbterjesztés:
  IRD, QPSK-PAL konverterek,
- digitális továbbterjesztés:
  QPSK-QAM konverterek,
- végfelhasználó: STB (6. fejezet).

3.4. Adathordozó elemek

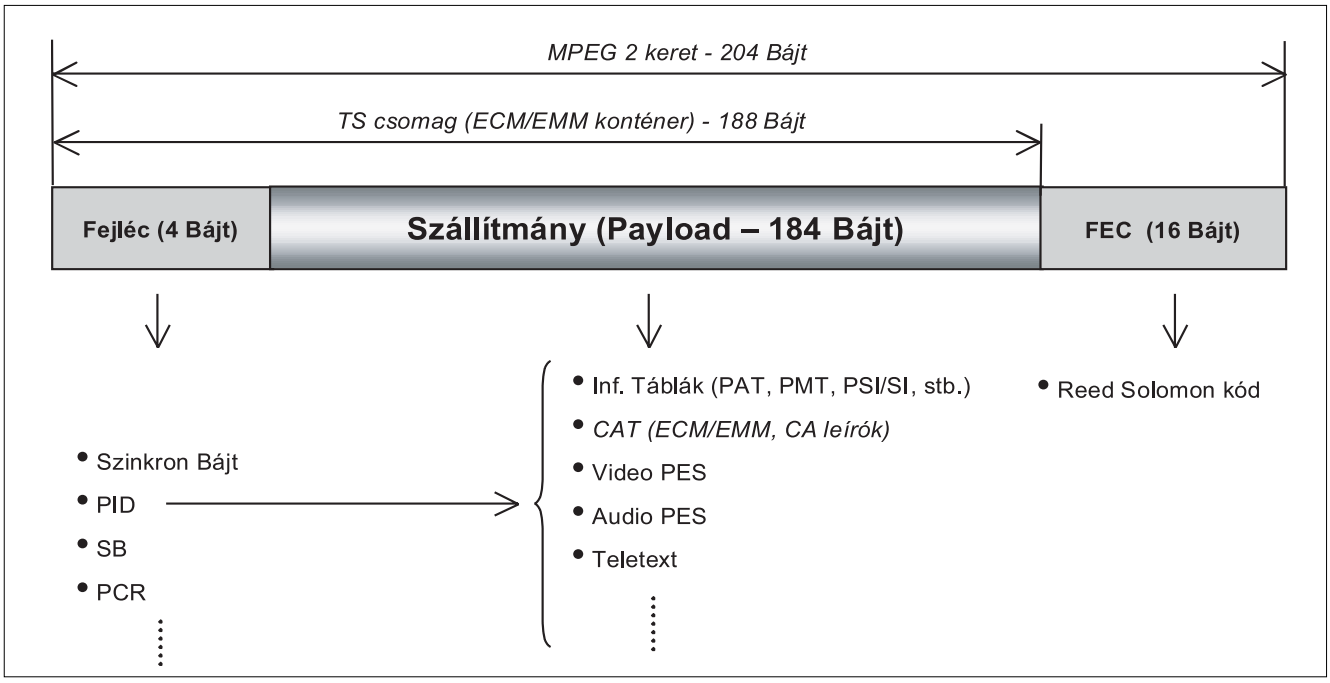
A DVB informatikai mechanizmusa rendkívül összetett, a szállított számtalan fajtájú és hatalmas bitmennyiségnek a hozzáférés-korlátozással kapcsolatos része szinte elenyésző. A DVB információhordozó struktúráját az ITU–T H.222.0 ajánlása határozza meg. Jelen cikk ezt csak olyan mélységben tárgyalja, amely a beleágyazott hozzáférés-korlátozással kapcsolatos üzeneteket (ECM, EMM) szállító adatcsomagok továbbítási mechanizmusának szemléltetéséhez szükséges. Az MPEG-2 kódolású TS-ek keretszervezési vázlata a *3. ábrán* látható. Az ábrán a fentieknek megfelelően csak az alapvető fontosságú, illetve a hozzáférés-korlátozással kapcsolatos információfajták vannak feltüntetve.

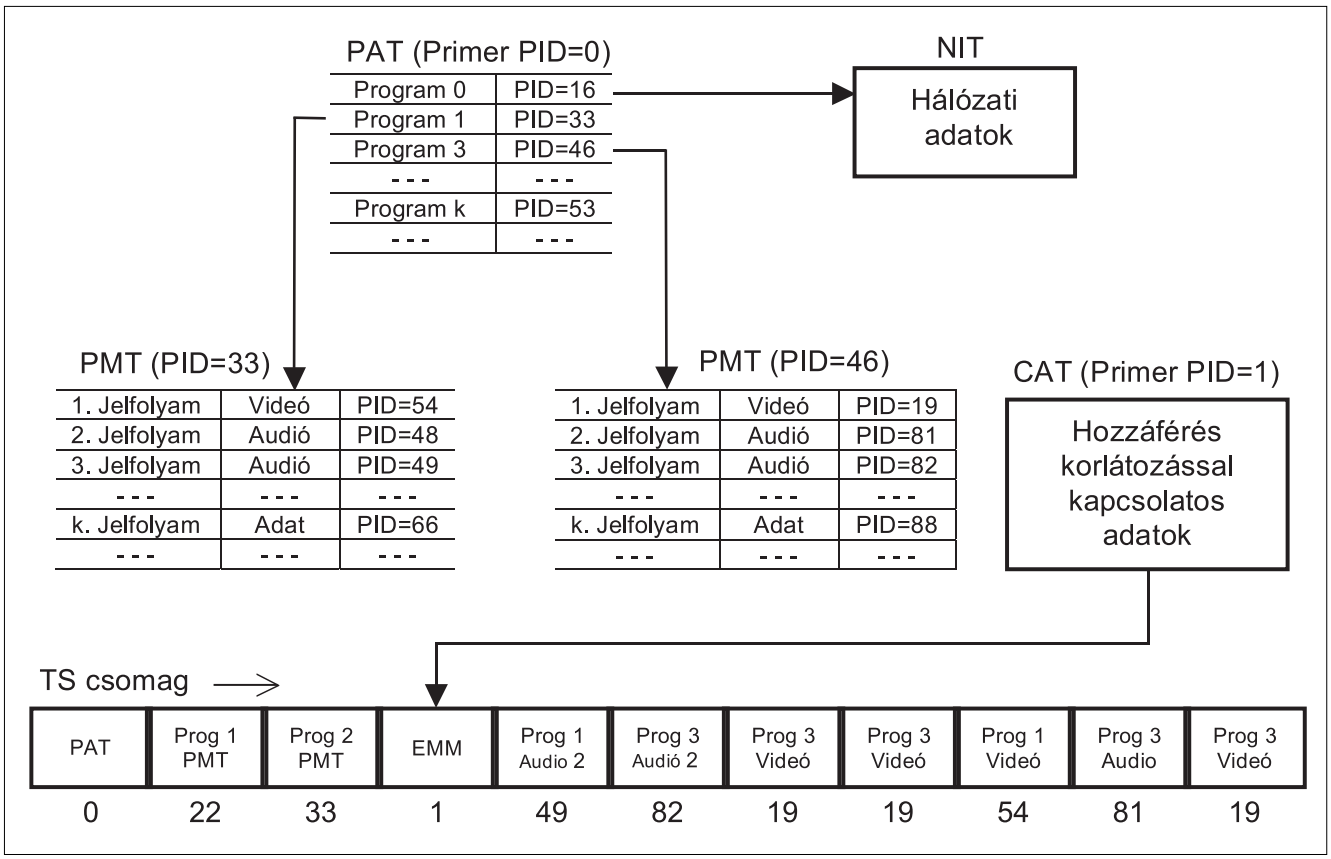
A TS csomagokat azonosító kódokat (PID) egy a fejlécben átvitt 13 bites mező hordozza. A DVB demultiplexer a különböző információfajtákat hordozó TS csomagokat ezek segítségével különbözteti meg. Egy adott TS-en belül minden PES-hez tartozó TS csomag PID-je azonos. A demultiplexer egy adott (például TV) program összetartozó adatfolyamait a hozzá tartozó (videó, audió, adat/felirat/teletext stb.) PES-ek PID-jeinek felhasználásával választja ki. Ha a TS hozzáférés-korlátozással kapcsolatos adatcsomagokat is továbbít, ugyanez érvényes ezek kiválasztására is. A csomagok helyes kiválasztásának feltétele, hogy a demultiplexer a TS csomagok és a PES-ek egymáshoz rendelését lássa. Ehhez a megfelelő PID-eket ismernie kell. Az egymáshoz rendeléseket a TS-ben kötelezően továbbított PAT (PID=0), illetve egy, vagy több PMT tartalmazza.

Mind a PAT-ot, mind a speciális rendszerinformációkat szállító további táblázatokat (CAT, NIT, SDT, EIT, TDT, RST stb.) egységes PID-del ellátott adat PES-ek szállítják. Ezek az úgynevezett rögzített értékű primer PID-ek, melyek a DVB szabvány szerint a speciális rendszer információkat tartalmazó táblázatokat hordozó csomagok (PSI, SI stb.) azonosítására szolgálnak. Ezek közé tartoznak hozzáférés-korlátozással kapcsolatos adatcsomagok (CAT) is. A speciális célú primer PID-ek értékeire a DVB szabvány a 0-31 mezőt tartja fenn. A 13 bites PID-ek értéke 0..2^13-1, azaz 0...8191 lehet. A változó értékű PID-ek mezeje ennek megfelelően a 32-es értékkel kezdődik. A kitöltő null-csomag PID azonosítója szintén foglalt, ennek értéke a 8191 (binárisan 111 1111 1111). A különböző videó, audió és adat PES-ek PID-jei ennek megfelelően 32 és 8190 közötti értékűek.

A demultiplexer a változó PID-ekhez a primer PID-ek által azonosított adat PES-ekben szállított táblázatokhoz való hozzáférés útján juthat. Ezen információkat a DVB szabvány szerint minden TS-nek periodikusan szállítania kell.

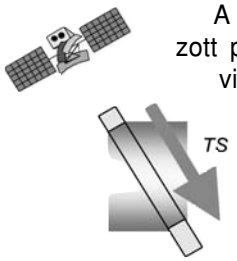
3. ábra MPEG-2 TS-ek keretszervezése





4. ábra A PID-es TS csomag azonosítás struktúrája (példa)

A hozzáférés-korlátozással kapcsolatos adatcsomagok azonosítói ebben a sorrendben a második helyen találhatók. Az ECM-eket és EMM-eket hordozó adatcsomagok PID-jeit a primer PID=1-el meghatározott hozzáférés-korlátozási adattáblázat, a CAT tartalmazza *(4. ábra)*.

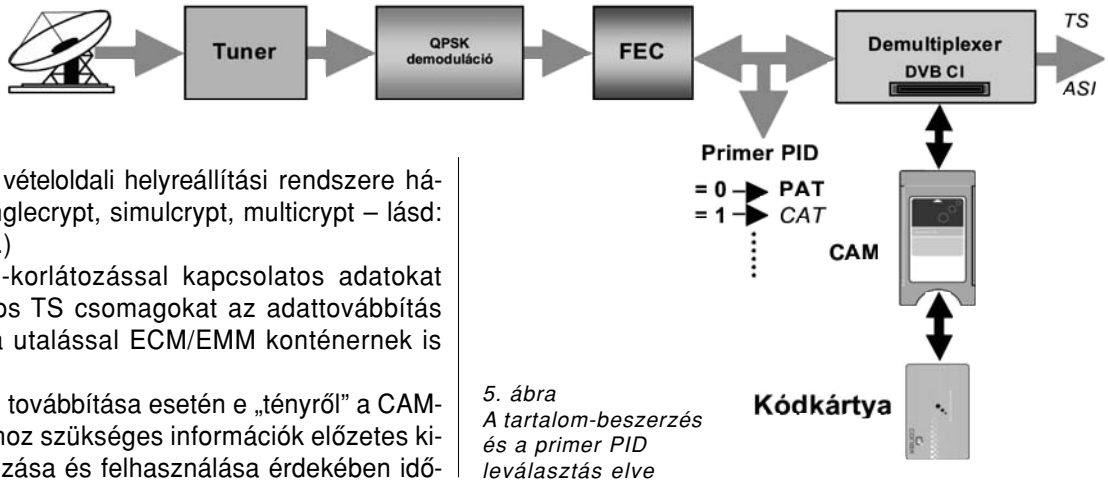


A CAT-ot csak hozzáférés-korlátozott programok jelfolyamaiban kell átvinni. A CA leírók a számukra fenntartott adatmezőkben szállított, csak a kódkártyák számára érthető titkos adatok. Ha a CAT egy CA leírót tartalmaz, az alkalmazott hozzáférés-korlátozás single-crypt, ha többet, simulcrypt rendszerű. (Ezek vételoldali helyreállítási rendszere háromféle lehet: singlecrypt, simulcrypt, multicrypt – lásd: meghatározások.)

A hozzáférés-korlátozással kapcsolatos adatokat szállító 188 bájtos TS csomagokat az adattovábbítás mechanizmusára utalással ECM/EMM konténernek is nevezik.

Tikosított PES továbbítása esetén e „tényről" a CAM-ot a helyreállításhoz szükséges információk előzetes kinyerése, feldolgozása és felhasználása érdekében időben „értesíteni" kell. A feladatot a fejlécben átvitt kétbites helyreállítás vezérlő jel, az SB látja el, melynek azonban ez nem az egyetlen szerepe.

A CSA-al titkosított DVB jel helyes helyreállításához mindig az aktuális CW-re van szükség, amelynek változásait nem lehet szinkronban tartani a CW-t tartalmazó ECM üzenetek, illetve a kódkártya által helyreállított CW megérkezésével. Az ECM-ben ezért általában egyszerre 2 CW-t továbbítanak, amelyből az egyik az aktuálisan használt CW, míg a másik a CW következő értékét adja. A SB másik feladata a CW változásainak pontos (csomagszintű) jelzése a titkosítás helyreállításakor.



5. ábra
A tartalom-beszerzés és a primer PID leválasztás elve

4. A továbbterjesztett tartalom titkosítási megoldásai

Az előfizetői jogosultságot rendszerint a műsorszolgáltató adja ki, a vezetékes műsorszolgáltató hatáskörén kívül. Előfizetőinek hozzáférési jogosultságát ezért utóbbinak is ellenőrzése alá kell vonnia. Jelen fejezet ennek lehetőségeit ismerteti.

4.1. Tartalom beszerzés

A műholdas tartalom beszerzés lépései, melyek a transzmodulációs megoldás kivételével bármely funkciót ellátó DVB vevő esetében azonosak, az *5. ábrán* láthatóak (az előző oldalon). A kivételként említett QPSK-QAM transzmoduláció esetén a műholdas TS eredeti titkosítását nem állítják helyre, így az ábrán feltűntetett CAM-nak és kódkártyának ebben az esetben nincs szerepe. A tartalombeszerzési eljárás egyes lépéseire a zajos távközlési közeg miatt van szükség. A megfelelő minőségű műholdas DVB átvitel alapvető feltétele, a szinkronizáció és hibajavítás biztosítása, amely nélkül a hozzáférés-korlátozás hibátlan működése sem biztosítható.

A DVB kétféle szinkronizációs elemet továbbít. Egyik az MPEG 2 keret szinkron bájtja, a másik a PCR, mint önálló PID-del továbbított PES. A kétféle szinkronizáció nincs kényszerkapcsolatban. A DVB keret szinkronizmusát a fejlécben átvitt szinkron bájt biztosítja, míg a videó/audió jeleket visszaállító MPEG dekódolás szinkronizmusának alapja a PCR.

Fentieknek megfelelően, első lépésben a tunert kell a TS-t szállító transzponder SAT frekvenciájára hangolni. A következő lépések a TS szimbólum sebesség szinkronizálója, majd a redundáns hibajavító információk feldolgozása, melynek eredményeként az MPEG 2 keretekből előállnak a TS csomagok (v. ö. 3. ábra). Az így kézben tartott minőségű MPEG 2 keret fejlécében elhelyezett primer PID-ek szoftveres elérése, illetve a további jelfeldolgozás e lépések után lehetséges.

Az eredeti TV formátum (PAL) visszaalakítása a DVB jel **analóg továbbterjesztése esetén** az előbbi lépéseket követően a továbbterjesztőnél történik. Ekkor a TV jelet le kell bontani alapsávra. Az analóg titkosítás rendszertechnikája bármely megoldás esetén független a beszerzett digitális tartalom titkosítási eljárásaitól. E megoldások túlhaladottak.

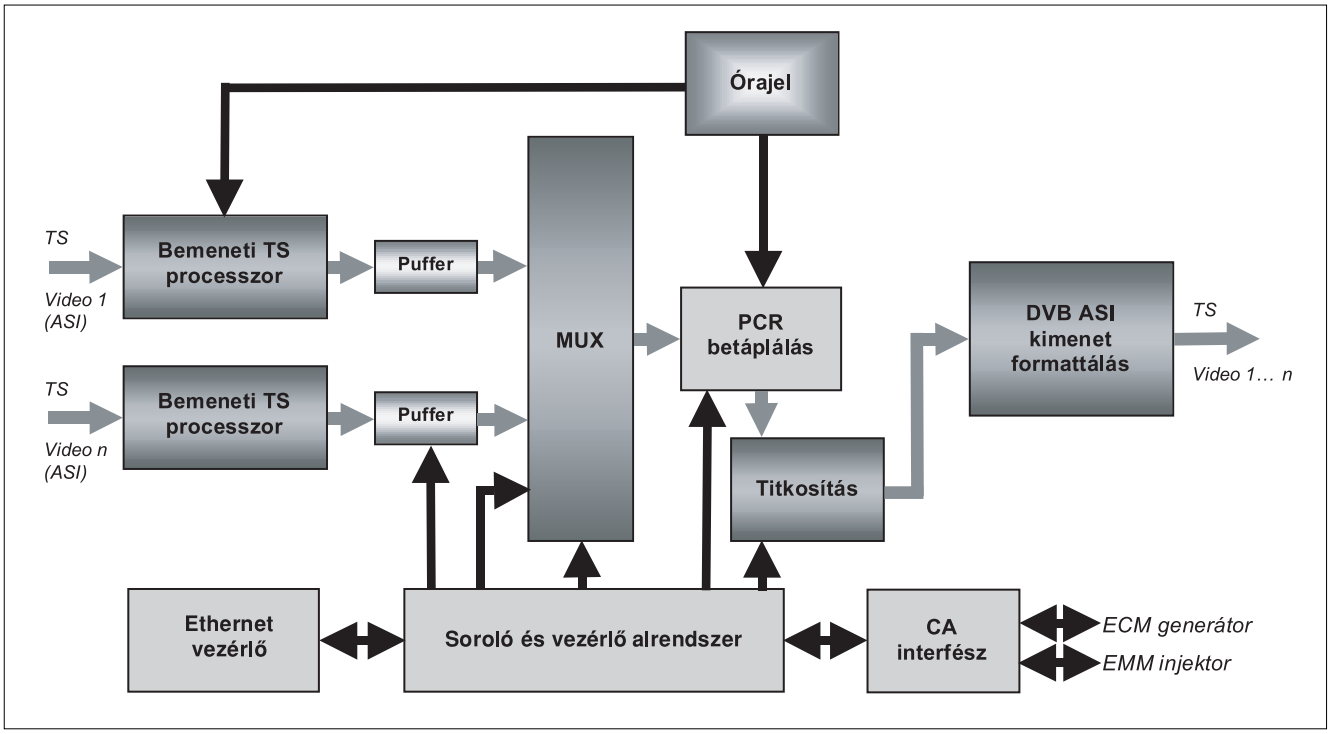
Az érdekeiket időben felismerő vezetékes tartalomtovábbterjesztők hosszú távú célja az analóg megoldás kiváltása. Az analóg titkosítású programok műholdas sugárzása gyakorlatilag már megszűnt.

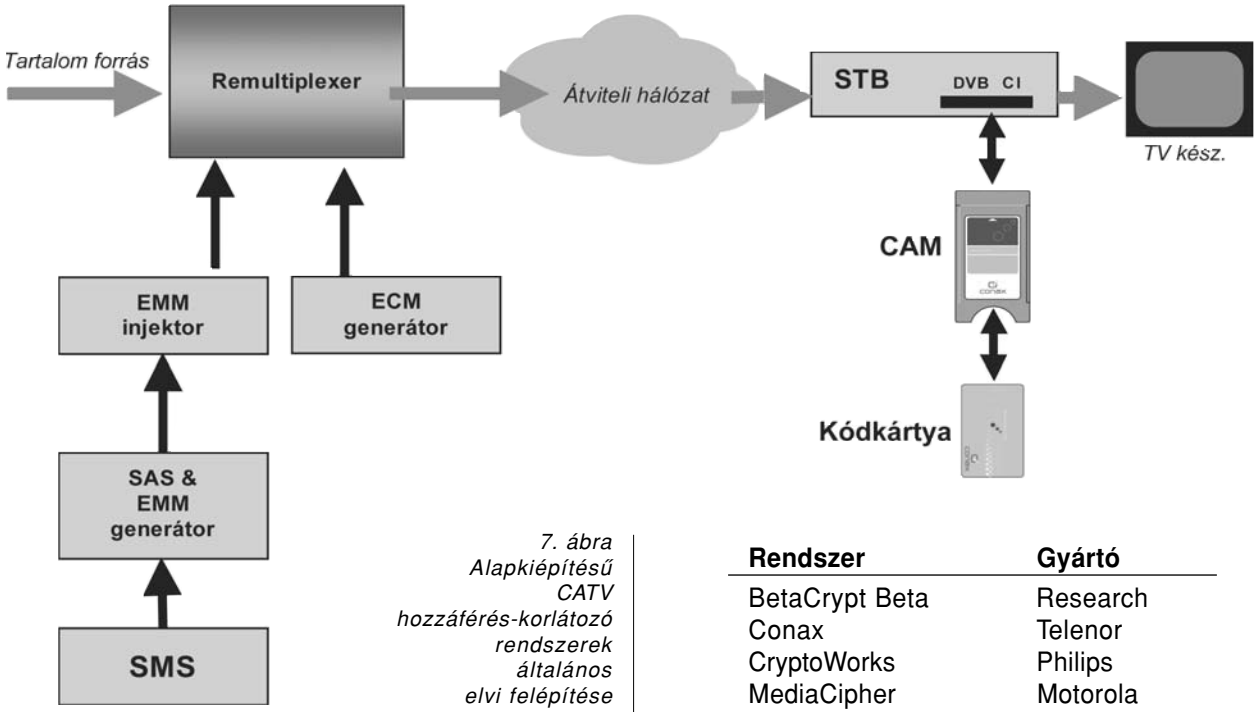
4.2. Továbbterjesztés

A műsortartalom DVB formátumú, hozzáférés-korlátozott, vezetékes továbbterjesztése esetén a szolgáltatói bevételszerzés műszaki megoldása az eredeti jogosultsági és szolgáltatásra vonatkozó adatok felülírása, vagy újragenerálása.

Ha a vezetékes szolgáltató a továbbítandó műholdas TS-ek összeállítását nem kívánja változtatni, akkor ezek közvetlen QPSK-QAM transzmodulációja a megfelelő megoldás. A továbbterjesztői hozzáférés-korlátozás itt egy, a kábeles szolgáltatóhoz rendelt azonosító, az Operator ID, melyet a műholdas szolgáltató bocsát a továbbterjesztő (CATV) szolgáltató rendelkezésére, az együtt járó kódkártyákkal. A transzmoduláció a műholdas TS titkosításának helyreállítása nélkül történik, az

6. ábra MPEG-2 TS-ek remultiplexelési folyamata





7. ábra Alapkiépítésű CATV hozzáférés-korlátozó rendszerek általános elvi felépítése

eredeti hozzáférés-korlátozás e továbbterjesztési megoldás során nem változik. Nagyobb vezetékes műsorszolgáltatók a saját műszaki/üzleti szempontjaik alapján kiválasztott titkosított tartalmakat saját CAS titkosításával terjesztik tovább. A továbbterjesztés így nem történhet változatlan szervezéssel.

A remultiplexer és a hozzáférés-korlátozó rendszer közti együttműködés elvét a *6. ábra* szemlélteti.

A demultiplexelés és remultiplexelés közötti átjárás hagyományos megvalósítása az ASI interfész. E megoldás hátránya, hogy a programok, vagy -csomagok jelfolyamának egymástól független kezelését nem teszi lehetővé. Digitális trönkökkel összekötött CATV hálózatok korszerű közös tartalom forrása az ATM alapú programbank (Híradástechnika 2003/8. sz.). Az ATM alapú demultiplexelést és remultiplexelést megvalósító processzor egységek működésének leírása és elvi felépítésének szemléltetése itt található.

5. Az alapszolgáltatású DVB CATV hozzáférés-korlátozó rendszerek felépítése

5.1. Az európai rendszerek

Az Európában alkalmazott digitális hozzáférés-korlátozó rendszerek működése a közös DVB titkosítási algoritmus (CSA) alkalmazásán alapul, így rendszerelemeik és működési mechanizmusaik egyezőek. A rendszerek közti különbség a jogosultságokkal kapcsolatos adatokat tároló előfizetői egységekben alkalmazott titkosítási eljárásokban rejlik. Az Európában alkalmazott CATV DVB hozzáférés-korlátozó rendszerek a következők:

Rendszer	Gyártó
BetaCrypt Beta	Research
Conax	Telenor
CryptoWorks	Philips
MediaCipher	Motorola
Mediaguard	Seca
Nagravision	Nagra-Kudelski
Viaccess	France Télecom
Videoguard	NDS

A további rendszerek védjegyzett működési elvei az előbbiektől eltérőek és biztonságuk érdekében szigorúan titkosak. Az egyes gyártók még különböző megoldásaik együttműködésének kizárására is törekszenek annak érdekében, hogy eladott rendszereik biztonsága bármelyik feltörése esetén a lehető legkisebb mértékben váljon veszélyeztetetté.

5.2. Rendszerelemek

A vezetékes műsorszolgáltatói hozzáférés-korlátozó rendszerek egyszerű fizető TV szolgáltatást támogató alapkonfigurációja a fenti, *7. ábrán* látható. A rendszerelemek funkciói az alábbiak:

Adóoldal

• *SMS adatbázis:* az előfizetői adat állomány nyilvántartása, az előfizetők számla egyenlegeinek követése (interfész a banki számítógépes nyilvántartás felé) és az EMM-ek kiadásának kérése a SAS tól.

• *SAS alrendszer:* a jogosultságok kiosztásának felügyelete, a kódkártya állomány állapot-fenntartása, hozzáférést biztosító jogosultsági adatok szolgáltatása a kódkártya számára.

• *EMM generátor:* a titkosított EMM-ek előállítása a SAS-tól kapott információk alapján, ezek betáplálása a DVB multiplexerbe.

• *EMM injektor:* a SAS felől érkező EMM-ek vételezése, az EMM kiadások sorolásának felügyelete és az EMM-ek betáplálása a DVB multiplexerbe.

• *ECM generátor:* a jogosultságok ellenőrzéséhez szükséges információ csomagok (dátum, programcsomag, CW) képzése és titkosítása.

Vevőoldal

• *CAM:* az ECM/EMM-ek szűrése, konvertálása és továbbítása a kódkártya felé, a CSA-al titkosított DVB jelek helyreállítása a CW felhasználásával.

• *Kódkártya:* a program-hivatkozási és jogosultsági információk tárolása, az ECM-ek és EMM-ek titkosításának helyreállítása és értelmezése a hozzáférési jogosultságok meghatározásához.

A leírt alapkonfiguráció az előfizetőnek egy, vagy több hozzáférés-korlátozott programhoz (TV csatornákhoz, vagy csatorna csoportokhoz) biztosítanak hozzáférést egy meghatározott (például hónapos, vagy éves) időtartamra. A hozzáférés, illetve a rákövetkező előfizetési időtartamra szóló újraengedélyezés kritériuma a számla kiegyenlítése.

5.3. Működési mechanizmus

Jelen fejezet a *8. ábrának* megfelelő elvi felépítésű, alapkiépítésű hozzáférés-korlátozó rendszerek működési mechanizmusát ismerteti.

Adóoldali adatgenerálás, vételoldali feldolgozás

Adóoldalon

– a DVB multiplexer előállítja a kódszót (CW) és az ECM generátort annak egy ECM-be történő beágyazására kéri.

– Az ECM generátor előkészíti az ECM tartalmát, a titkosított kódszavakat (CW) és a hozzáférési paramétereket, továbbá a szolgáltató-azonosítókat, a program-hivatkozást és az együtt járó jogosultsági információkat, kriptografikus változókat, valamint a digitális aláírást.

Vevőoldalon

– telepítésekor a kódkártya bizonyos információk megadásával (pl. CAS típusa, kártya sorozatszáma, a kártyán lévő szolgáltatók azonosítói stb.) regisztrálja magát a CAM-ba, amely ezután ezeket az információkat a kódkártyának szóló üzenetek kinyerésére használja. A kódkártya ettől kezdve rendre helyreállítja az érkező ECM-et, majd összehasonlítja a pillanatnyi dátumot és időt, a szolgáltató azonosítót, valamint a program-hivatkozási és jogosultsági információkat a saját memóriájában tároltakkal. Amennyiben az adott programhoz való hozzáféréshez jogosult, a kódkártya kiadja a CW-t a CAM számára a DVB TS helyreállításához.

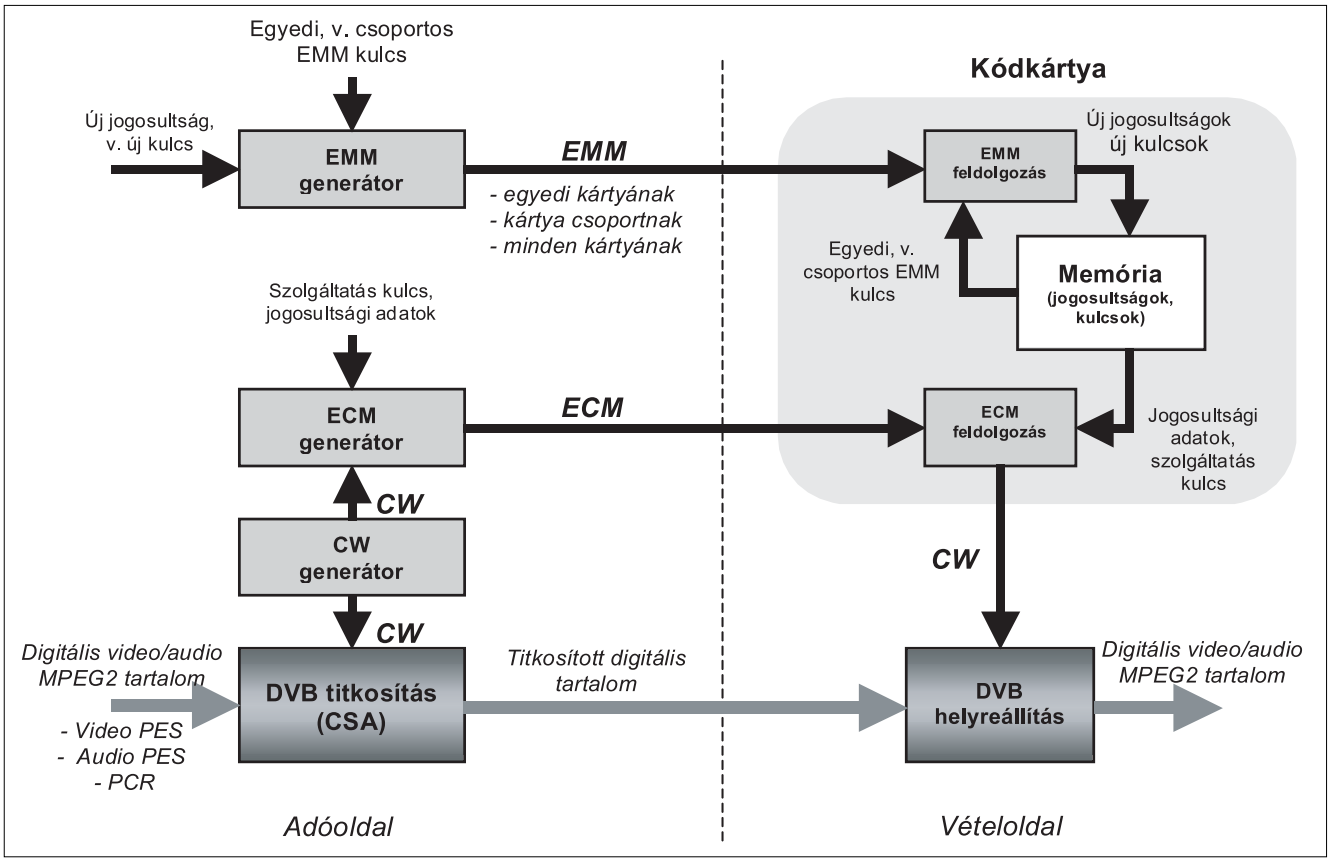
– A CAM a kapott kódszavak felhasználásával végrehajtja a PES-ek helyreállítását.

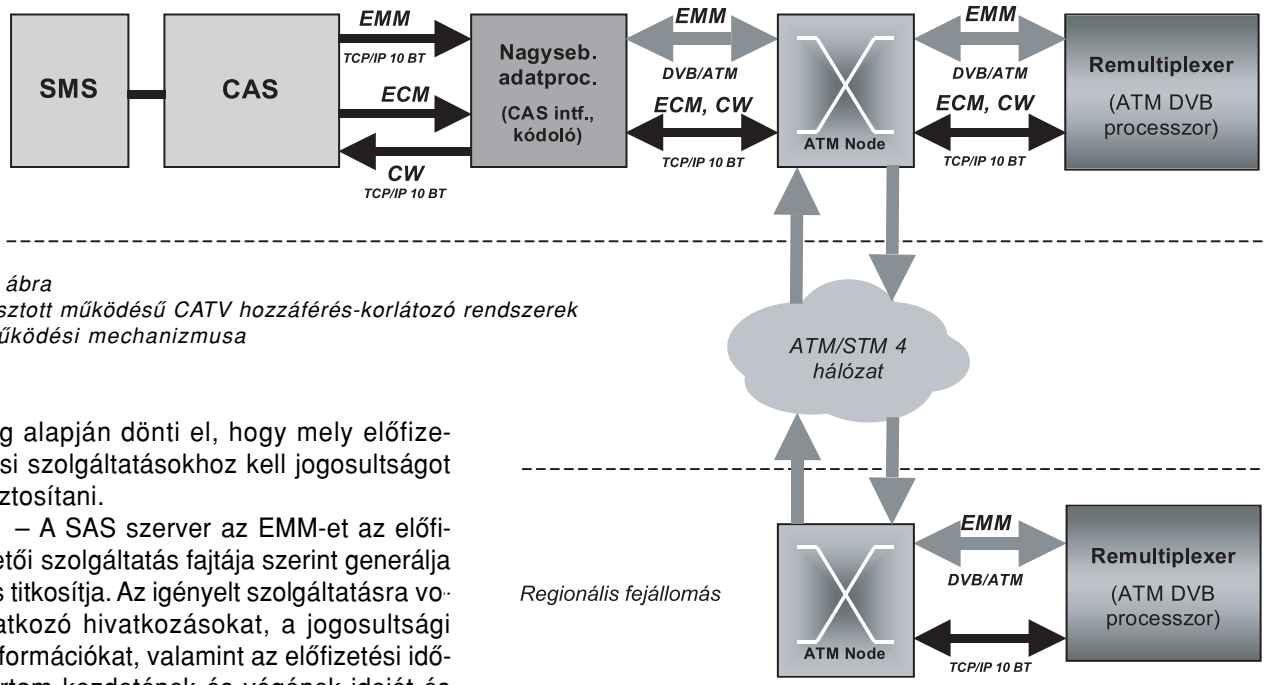
A jogosultságok kiosztása és frissítése

Adóoldalon

– az előfizetői menedzsment rendszer (SMS) nyilvántartja valamennyi felhasználót és kódkártyát. Az SMS a SAS szervertől az EMM-ek előállítását kéri. Az SMS az előfizető által igényelt szolgáltatás és a fizetési egyen-

8. ábra Alapkiépítésű DVB CATV hozzáférés-korlátozó rendszer működési mechanizmusa





9. ábra
Osztott működésű CATV hozzáférés-korlátozó rendszerek működési mechanizmusa

leg alapján dönti el, hogy mely előfizetési szolgáltatásokhoz kell jogosultságot biztosítani.

– A SAS szerver az EMM-et az előfizetői szolgáltatás fajtája szerint generálja és titkosítja. Az igényelt szolgáltatásra vonatkozó hivatkozásokat, a jogosultsági információkat, valamint az előfizetési időtartam kezdetének és végének idejét és dátumát az EMM tartalmazza.

Vevőoldalon

– a CAM a beérkező EMM-eket a kódkártya felé továbbítja, amely helyreállítja azokat, majd frissíti memóriáját az érkezett információval, az igényelt szolgáltatásra vonatkozó hivatkozással, a jogosultságokkal, valamint az előfizetési időtartam adataival.

5.4. Architektúrák

A DVB alapú CATV hozzáférés-korlátozó rendszerek fő gazdasági előnye az igények szerinti konfigurálhatóság. E rendszerek az osztott üzemet is lehetővé teszik, azaz egy közös hozzáférés-korlátozó rendszert több CATV szolgáltató is üzemeltethet. Ehhez azonban szükséges a szabványos kommunikációs mechanizmusra épülő SMS–SAS interfész, amely az együttműködést más típusú SMS-ek számára is lehetővé teszi. Az SMS ugyanis nem feltétlenül a hozzáférés-korlátozó rendszer gyártójának terméke. Előfizetői adat és számlanyilvántartással minden szolgáltató, minden körülmények között rendelkezik. A DVB alapú hozzáférés-korlátozó rendszer beruházásánál azt kell tehát mérlegelnie, hogy áttér-e egyúttal a hozzáférés-korlátozó rendszer gyártója által ajánlott SMS alkalmazására, vagy megoldja meglévő SMS rendszere és a hozzáférés-korlátozó rendszer közötti együttműködés esetleges problémáit.

A rendszer osztott távműködésének feltétele a SAS és ECM generátorok, valamint az EMM injektorok azonos helyű telepítése a szolgáltatási területet behatárolja. A szabványos kommunikációs mechanizmusra épülő SMS–SAS interfész e feltétel kielégítése mellett több SMS egyidejű csatlakoztatását is lehetővé teszi. Az osztott távműködés további feltételei:

– rugalmasan konfigurálható EMM kiadási rendszer, meghatározott prioritásokkal,

– az EMM-ek irányíthatósága valamennyi, vagy kiválasztott multiplexer telephelyre,

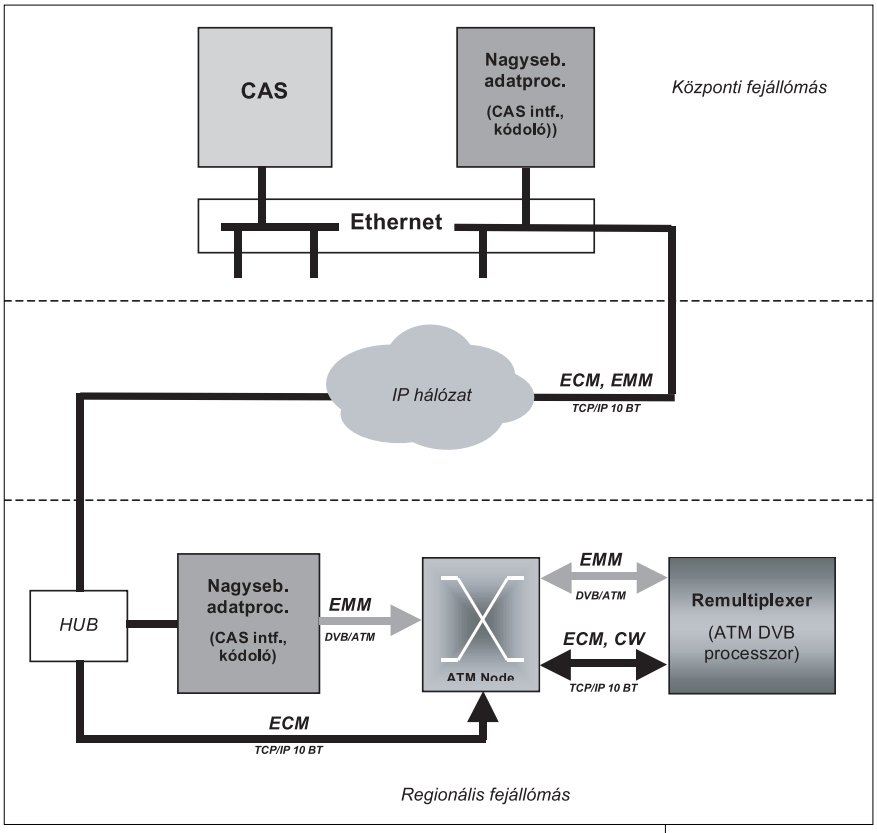
– a jogosultságok hozzárendelhetősége egy-egy alap-jelfolyamhoz, programhoz, vagy csoporthoz.

Az osztott működésű hozzáférés-korlátozó rendszerek legkönnyebben az ATM alapú programbankok hálózati architektúrájába integrálva alkalmazhatók *(9. ábra),* melyet a már hivatkozott ATMux™ rendszer leírása ismertet.

Az ATM program bank és a hozzáférés-korlátozó rendszer közötti ATM-DVB konverziót és az adatkommunikációt itt egy nagyteljesítményű adatprocesszor biztosítja. Az egység feladata a kapcsolatok felépítése és fenntartása az ECM generátorokkal, illetve EMM injektorokkal, az ECM és EMM jelfolyamok kezelése, valamint az ECM-ek és kódszavak szinkronizációja az ATM DVB processzorok beépített titkosító egységei számára.

Osztott működésű hozzáférés-korlátozó rendszermegoldás közös átviteli hálózatba nem kötött, de együttműködni szándékozó szolgáltatók számára is rendelkezésre áll. Ezt a megoldást mutatja be a következő oldalon a *10. ábra,* ahol a központi adatprocesszor a hozzáférés-korlátozó rendszerrel Ethernet hálózat segítségével tartja a kapcsolatot, és a hozzáférés-korlátozáshoz az ECM és EMM adatfolyamokat IP formátumban állítja elő.

A távoli fejállomás(ok)on az EMM adatfolyamokat az ott elhelyezett adatprocesszor konvertálja és ágyazza a DVB/ATM jelfolyamba. Az ECM-eket az adathálózati csomópontból (HUB) közvetlenül az ATM node 10 BT interfésze felé irányítják, ahonnan útja már azonos a 9. ábrán láthatóval.



10. ábra IP alapú centralizált CATV hozzáférés-korlátozó rendszerek működési mechanizmusa

6. Előfizetői végberendezések (STB)

A tartalom szolgáltatók és továbbterjesztők távlati célja egyaránt az, hogy a szociális célúakon („must carry") kívül minden műsortartalom hozzáférés-korlátozással jusson az előfizetőhöz. A közvetlen díjbeszedési rendszer megvalósításának járható útja tehát a „kábeles" STB megjelenése minden CATV-hez csatlakozó háztartásban.

A STB-ok jelenlegi változatai jelfeldolgozás szempontjából terjesztési rendszer (SAT, CATV, DTT) specifikusak. A STB alapvető szerepe mindhárom rendszerben a DVB jelek PAL/RGB jelekké alakítása. A műszaki távlat azonban a mindhárom terjesztési rendszerhez alkalmas univerzális, az adatforgalom szempontjából, pedig interaktív STB-ok megjelenése és elterjedése. A STB-ok CATV-s (vagy CATV-hez is alkalmas univerzális) változatai az adott CATV hálózatban alkalmazott hozzáférés-korlátozás kiegészítő egységeit is értelemszerűen tartalmazzák. Az alapszolgáltatású CATV-s STB-ok felépítése a *11. ábrán* látható.

Az interaktív STB-ok felépítése kábelmodemmel egészül ki. A STB-ok a CATV hálózatok visszirányán, különböző szabványos adatátviteli formátumokban (DOCSIS, EuroDOCSIS/QPSK moduláció) így már az előfizetéssel, számlázással, szolgáltatáskérésekkel és jogosultságokkal kapcsolatos adatokat is képesek lesznek a szolgáltatók felé közvetíteni (beleértve a jövőben várható járulékos új szolgáltatások, mint a NVOD, VOD, PPV stb. időzítéseivel kapcsolatosakat is).

A STB lényegében egy speciális számítógép TV-s alkalmazásokhoz. Fő részei az alábbiak:

Számítógép alrendszer: az alapvető számítástechnikai funkciókat látja el. Magában foglalja a standard számítógépegységeket, mint a CPU, a memória, valamint (interaktív változatoknál) a kábelmodemet.

TV alrendszer: feladata a DVB formátumú TV jelek feldolgozása. Magában foglalja az DVB jelfeldolgozás egységeit, a TV/VCR és audió csatlakozásokat, valamint a remodulátor és RF összegző egységeket.

Hozzáférés-korlátozó alrendszer: A CATV-s változatok egy CI-t, vagy (egyes készülék típusok esetében) beépített kártyaolvasót tartalmaznak. (A SAT típusok egy, vagy két CI-t tartalmazhatnak. Utóbbi esetben csak az egyik beépített.)

A digitális moduláció típusától függő specifikus STB-k:

– közvetlen műholdas műsorszórás (SAT),
– vezetékes (tovább)terjesztés (CATV),
– földfelszíni műsorszórás (DTT).

A vezetékes műsorterjesztéshez a QAM demodulátorral (is) ellátott STB típusok használatosak.

A STB-okban alkalmazott szoftverek referencia modellje a MHP, elhatárolt rétegei az alábbiak:

Alapszoftver: részei az operációs rendszer, boot loader, TV-s alapalkalmazások, middleware és az átviteli modell tárgyalásánál tárgyalt CA alkalmazás

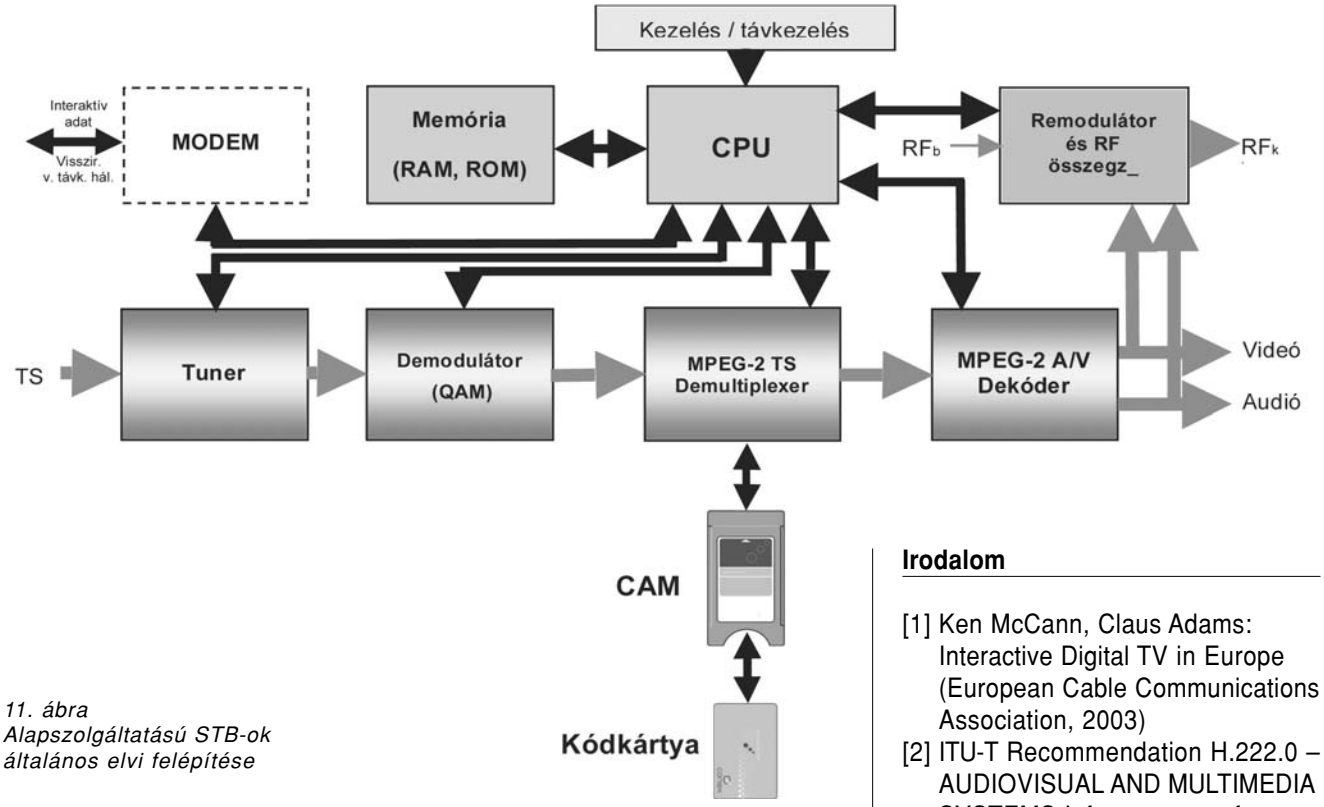
Hardver meghajtók: interfész a hardver és szoftver között. (A gyártók szállítják.)

Alkalmazások: a felhasználói igények szerinti funkciókat látják el, mint pl. EPG (a későbbiekben pedig az interaktív TV-s alkalmazások)

A helyreállított DVB TS-ből az MPEG demultiplexer kiválasztja és dekódolja (kitömöríti) a venni kívánt program videó és audió jelfolyamát. A PAL formátumú alapsávi videó, és audió tartalom visszaállítása az MPEG-A/V dekóder segítségével történik. A STB-ok adat- és információfeldolgozási mechanizmusa sem tartogat újat. Hozzáférés-korlátozott program esetén a CSA-al titkosított DVB TS helyreállítása a kódkártya által kiadott CW felhasználásával ezúttal is a CAM-ban történik.

7. A hozzáférés-korlátozott műsorterjesztés kockázatai

A hozzáférés-korlátozás, mint a bevezetőben is említett bevételforrás, a jogtalan haszonszerzést is jelentheti. Ez akkor valósul meg, ha a hozzáférést elősegítő eszközök kalóz terjesztése miatt a szolgáltató jelentős



11. ábra
Alapszolgáltatású STB-ok általános elvi felépítése

mértékű bevételtől esik el. A hozzáférés-korlátozás önmagából adódó második célja tehát ennek megelőzése, vagy visszaszorítása egy tűrhető mértékre.

A jogosultságokkal kapcsolatos adatok adótól vevőig történő átvitele a műsorterjesztés részét képezi. A cél e pont-multipont viszonylatú egyirányú információfolyam védelme. Bár a digitális televíziózás az interaktivitás felé halad, ahol a felhasználó oldali STB a szolgáltatók központi szervereivel a 6. fejezetben említettek szerint kommunikálhat, maga a tartalomkézbesítés továbbra is egy egyirányú kommunikáció marad.

Az adatok védelme a szolgáltató érdeke. Célkitűzése ezért lényegesen különbözik a kétirányú kommunikációnál érvényesektől, mint például a GSM esetében, vagy az on-line banki tranzakcióknál, ahol a biztonság sérthetetlensége a felhasználó érdeke. A kommunikáció biztonságában a jelen esetben nem érdekelt végfelhasználó, a tartalomhoz, mint termékhez, ha csak lehet, térítésmentesen szeretne hozzájutni. A jel-lopással kapcsolatos jogszabályoknak és betartatásuknak egyelőre számos törvényhozás kevés érvényt szerez, így a fizető TV magas bevételi lehetősége vonzza a jól felszerelt, képzett és szervezett kalózkodást. Ezért minden szolgáltató arra törekszik, hogy a felhasználónál telepített eszközök lehetőleg olcsók, de manipulálhatatlanok legyenek.

Irodalom

[1] Ken McCann, Claus Adams: Interactive Digital TV in Europe (European Cable Communications Association, 2003)
[2] ITU-T Recommendation H.222.0 – AUDIOVISUAL AND MULTIMEDIA SYSTEMS Infrastructure of audiovisual services – Transmission multiplexing and synchronization – Information technology (Generic coding of moving pictures and associated audio information systems)
[3] Guide to MPEG Fundamentals and Protocol Analysis (25W-11418-4 Tektronix, 2002)
[4] Georgieff Zsolt, Wein Tibor: ATMux™ – műsorterjesztés digitális transzporthálózaton, Híradástechnika, 2003/8.
[5] Conax CAS5 System Description (021115 Conax AS, 2002)
[6] Stefler Sándor: Hogyan tovább Set-Top-Box-ok? Híradástechnika, 2001/10.
[7] How to choose STBs (20020927 Conax AS, 2002)

Hírek

Az internetes hálózati berendezések legnagyobb gyártója, a **Cisco Systems** új termékeket mutatott be. A díjnyertes IP-alapú alközponti rendszer, a Cisco CallManager 4.0 lehetővé teszi a Cisco Video Telephony (VT) Advantage 1.0 megoldás alkalmazását, amellyel a felhasználók valós idejű személyes videokapcsolattal egészíthetik ki telefonbeszélgetéseiket. Szintén most mutatkozott be a Cisco MeetingPlace szerver, amelynek segítségével IP-telefonon, hagyományos telefonkészüléken vagy számítógépen keresztül vehetnek részt és szervezhetnek a felhasználók hang- videó- és webkonferenciákat. Az új megoldások fokozott biztonságot nyújtanak a vállalatok számára.

Xyscom rendszer üzembe helyezése Bárdudvarnokon

DR. LAJTHA GYÖRGY

lajtha.gyorgy@ln.matav.hu

A Hungarocom dr. Eisler Péter vezérigazgató irányításával érdekes, új távközlési rendszerrel lépett piacra a Kaposvár közelében lévő Bárdudvarnokon. *A rendszer műszaki ismertetését a Híradástechnika 2003/11. számában olvashattuk.* Akkor már a berendezés túl volt a fejlesztésen, sőt a genfi World Telecomon a világ bármely tájáról érkező látogatók megtekinthették. Márciusi számunkban Löcher János doktorandusz számolt be ennek a rendszernek főbb jellemzőiről, most pedig az újság első részében Dárdai Árpád cikkét olvashatják az OFDM rendszerről, mely lehetővé tette, hogy a Xyscom közel érzéketlen legyen az összeköttetés zavaraira.

A Xyscom három, már korábban is létező technológiát egyesít. Lehetővé teszi a távközlést a hagyományos vezetéken, rádióösszeköttetésen, valamint a 220 V-os villamos hálózaton. Az új technológiával nemcsak telefonálni lehet, hanem biztosítja a felhasználók számára az Internet hozzáférést is. Bárdudvarnokon 2003 őszén kezdték meg a rendszer telepítését, amely február óta működik 15 előfizetővel.

A rendszer ünnepélyes átadását április 2-án a helyi iskola épületében tartották. Forintos László polgármester tájékoztatást adott arról, hogy a rendkívül szétszórt falu 16 településrészével feltétlenül igényli ezt a rendszert. Ez példa lehet más területek számára is. A világháló elérésétől a mérőórák leolvasásáig minden távközlési szolgáltatásra képes. Ezzel a község végre részesévé válhat „az intelligens Somogy megyének“, melyről Gyenesei István, a Megyei Közgyűlés elnöke tartott beszámolót. Az új távközlési rendszer jelentős lépés az intelligens megye-programban, amelynek továbbfejlesztése a megyei önkormányzat kiemelkedő feladata. A bárdudvarnoki tapasztalatok alapján további somogyi települések – mint például Marcali, Barcs és Tab – környékét is új távközlési rendszerekkel akarják ellátni.

A megjelentek számára dr. Eisler Péter ismertette a rendszert. A Hungarocom tervei közt szerepel, hogy Kadarkút-Nagybajom kistérségének területén 18 további községben telepítsék ősszel a rendszert. Felszólalt dr. Varga Csaba is, a Stratégiai Kutatóintézet igazgatója, aki erre a lehetőségre támaszkodva az információs társadalom vidéki kiépítését már realitásnak tartja.

Tanulságos, hogy egy műszaki alkotás a terület elkötelezett vezetőinek támogatásával, a lakosság számára az információellátás és szórakoztatás területén sok segítséget jelenthet. A gazdaság vérkeringésébe való bekapcsolódás pedig talán még újabb munkalehetőségeket és vállalkozásokat is megindíthat.

Katasztrófavédelem és üzletmenet-folytonosság az információtechnológiában

A DR/BC tervezés alapjai

GODÁNYI GÉZA, biztonságtechnikai szakértő

Kulcsszavak: fenyegetések, üzembiztonság, Üzletmenet-folytonossági Terv, költséghatékonyság

Az IT rendszerek szerepének növekedésével a hagyományos, IT-központú katasztrófavédelem (Disaster Recovery) helyett egyre inkább a legfontosabb üzleti folyamatok összes működési feltételének folyamatos biztosítására koncentráló, átfogóbb, úgynevezett üzletmenet-folytonosság (Business Continuity) kerül előtérbe. Az üzleti igényeknek megfelelő, de ugyanakkor a lehető legkisebb anyagi terhet jelentő BC/DR folyamatok és az azokat kiszolgáló informatikai infrastruktúra megtervezése összetett feladat, amelynek az egyes alkalmazások üzleti folyamatokra gyakorolt hatásának elemzésén kell alapulnia. Az alábbiakban az EMC ISC módszertanára támaszkodva rövid áttekintést adunk a BC/DR tervezés fő területeiről, valamint a tervezést befolyásoló legfontosabb tényezőkről.*

Bevezetés

Az információs technológia egyre jobban átszövi mindennapi életünket. A legtöbb üzleti vállalkozás működése már elképzelhetetlen informatikai infrastruktúra nélkül. Ebből az is következik, hogy az informatikai rendszerek folyamatos működésének biztosítása egyre több szervezet számára bír stratégiai jelentőséggel, így komoly erőforrásokat mozgósítanak e cél elérésére.

A számítógépes alkalmazások üzemképtelenségének leggyakoribb okai (hardver hibák, emberi tévedés, figyelmetlenség), valamint azok következményei megfelelő technológiákkal, üzemeltetési szabályokkal és azok betartásával jórészt kivédhetők, ugyanakkor az egyetlen számítóközpontra épülő infrastruktúra nagyobb természeti katasztrófákkal (áradások, földrengések stb.) szemben továbbra is sérülékeny marad. A fokozott üzembiztonság több számítóközpont kialakításával elérhető, ám ennek horribilis költségei a vállalatok nagy részét sokáig visszatartották ettől a lépéstől.

A világ azonban sok tekintetben nagyot fordult az elmúlt évek során: egyrészt egyszerűbbé és olcsóbbá vált a több telephelyes infrastruktúra kialakítása (a colocation/hosting központok és DR szolgáltatók megjelenése, valamint a kommunikációs technológia fejlődése révén), másrészt egyre nagyobb külső nyomás nehezedik az üzleti szereplőkre a biztonság növelésére (egyebek mellett hatóságok és felügyeleti szervek előírásai miatt).

Eközben tanúi lehettünk a nemzetközi terrorizmus aktivizálódásának, amely a World Trade Center elleni támadásban érte el csúcspontját. 2001. szeptember 11. – sajnálatos mérföldkő az informatikai üzletmenet-folytonosság tervezésében: azóta bármely nagyvállalat számára reális veszéllyé vált egy, a számítógépközpontot teljesen megsemmisítő katasztrófa bekövetkezése.

A biztonságos üzemeltetés tervezőinek technológiai mozgástere tehát egyre növekszik, és nagyobb támogatást is kapnak a vállalati vezetőktől, mint korábban; ugyanakkor a közelmúlt gazdasági visszaesése miatt beszűkültek a források, amelyek hatékony felhasználását a pénzügyi vezetés egyre szigorúbban felügyeli. Az üzletmenet-folytonosság tervezése során tehát alaposan elemezni kell az üzleti igényeket, ezeket össze kell vetni az egyes alkalmazások üzemképtelenségének üzleti hatásaival, és ezek alapján kell kialakítani azt a szabályrendszert és informatikai infrastruktúrát, amely a kockázattal arányos ráfordítás mellett biztosítja az üzleti folyamatok elvárt szintű használhatóságot.

Az üzletmenet-folytonosság tervezésének alapjai

Az üzletmenet-folytonosság fogalma

Amikor az üzleti folyamatokat támogató informatikai rendszer üzembiztonságáról beszélünk, leggyakrabban a „katasztrófavédelem" (Disaster Recovery, DR) és az „üzletmenet-folytonosság" (Business Continuity, BC) fogalmakat használjuk – néha felváltva, felcserélhető értelemben is. Pedig a BC jóval nagyobb területet ölel fel, mint a DR: míg katasztrófavédelem alatt eredetileg az informatikai rendszerek működésének fenntartását értették, addig az üzletmenet-folytonosság az alapvető üzleti tevékenység folyamatos működésének biztosítását (például az ügyfelek kiszolgálása) és a pénzügyi veszteség minimalizálását célozza meg. A BC része az üzleti tevékenységhez nélkülözhetetlen (vagyis *kritikus*) üzleti folyamatok azonosítása, az azokat támogató informatikai alkalmazások feltérképezése és védelme. A BC magában foglalja a célok eléréséhez szükséges folyamatokat, eljárásokat és technológiát, valamint azok megtervezését és kialakítását is.

** Az ISC az EMC Corporation vezetői tanácsadó üzletága*

Az üzletmenet-folytonosság alapvető célja tehát olyan költség-hatékony megoldás biztosítása, amely lehetővé teszi az üzleti tevékenység folytatását nem várt események esetén, és így az üzletmenet-kiesés kockázatát olyan szintre csökkenti, amely az üzleti vezetés számára elfogadható.

Az üzletmenet-folytonosság tervezés célkitűzései

A BC megoldás hatékonyságát két fő mutató segítségével lehet számszerűsíteni:

• **RTO (Recovery Time Objective)**

A katasztrófa bekövetkezése és az összes definiált számítógépes alkalmazás konzisztens újraindulása között eltelt idő.

• **RPO (Recovery Point Objective)**

Az alkalmazások adatait úgy kell helyreállítani az RTO időn belül, hogy azok az RPO időpontnak megfelelő (konzisztens) állapotot tükrözzék, és az összes addig történt változást tartalmazzák. Minél közelebb van ez az időpont a katasztrófa bekövetkeztéhez, annál kisebb az adatvesztés.

Az elsődleges cél a számszerű RTO és az RPO elvárások teljesítése, de emellett a következő célokat is szem előtt kell tartani:

– A kritikus üzleti folyamatok minél rövidebb ideig legyenek csak működésképtelenek.
– Minimalizálni kell a pénzügyi veszteséget.
– Törekedni kell a hatályos törvények és szabályok betartására.
– Minél egyszerűbb döntési mechanizmusokat kell meghatározni a nem várt esemény kezelésére.
– Ki kell dolgozni a normál működéshez való ellenőrzött és rendezett visszatérés szabályait.

Az üzletmenet-folytonossági terv szerkezete

Az üzletmenet-folytonosság tervezése a Business Continuiy Management meghatározó eleme, amely a vállalat üzletmenet-folytonossági stratégiáján alapul. Maga a BC tervezés négy fő terület tervezési folyamatát egyesíti, illetve koordinálja *(1. ábra)*.

1. ábra Az üzletmenet-folytonosság menedzsment modellje

Az üzletmenet-folytonosság tervezés fő elemei

A BC tervezése során csak akkor érhetünk el megfelelő eredményt, ha az előkészítés során az összes releváns információt (előírások, üzleti elvárások, környezeti feltételek stb.) összegyűjtjük, elemezzük és a prioritásokat ezek alapján meghatározva keressük meg a megfelelő kompromisszumot. A tervezés fő elemei:

• Üzleti igények
• Fenyegetések rangsorolása, kockázatok felmérése
• A katasztrófa-események üzletre gyakorolt hatásának elemzése
• Az informatikai alkalmazások és az üzleti folyamatok megfeleltetése
• RTO és RPO előírások
• A jelenlegi BC képesség felmérése
• Az elvárások és a jelen képességek összevetése
• A megoldási alternatívák számbavétele
• A megoldási alternatívák elemzése költséghatékonyság szempontjából
• A BC stratégia és ajánlások megfogalmazása

Az alábbiakban ezeket az elemeket tekintjük át.

Üzleti igények

Az üzleti igények fontossága kézenfekvő, azonban elemzésükre és értelmezésükre nem kizárólag ezért kell különös gondot fordítani. A tapasztalatok azt mutatják, hogy nagyobb szervezetekben a döntéshozók nem képesek teljes egészében átlátni a megvalósítás informatikai összetettségét és buktatóit, illetve felmérni az abból adódó kockázatokat. Az alkalmazásokért és az infrastruktúra működtetéséért felelős vezetők nincsenek tökéletesen tisztában az üzlet prioritásaival. Így tehát e két csoport látásmódja között jelentős szakadék tátonghat *(2. ábra)*, melynek áthidalása az üzletmenet-folytonossági tervezés döntő fontosságú eleme és egyben talán legnagyobb kihívása.

A fenyegetések rangsorolása és a kockázatok felmérése

Az üzemeltetés biztonságát veszélyeztető összes tényezőt számba venni és mindegyik ellen tökéletes védelmet nyújtani nemcsak hogy reménytelen vállalkozás,

2. ábra Szakadék az üzlet és az IT között

de nem is éri meg, hiszen a legtöbb nem várt esemény kivédése jóval többe kerül, mint az általuk okozott kár. Mielőtt tehát a BC megoldást megterveznénk, az üzlettől kapott preferenciák szerint rangsorba kell állítanunk a lehetséges fenyegetéseket, elemeznünk kell az általuk jelentett kockázatot, és ennek alapján kell megkeresnünk az optimális megoldást.

A leggyakoribb fenyegetéseket az alábbiak szerint csoportosíthatjuk:

Nagyobb közüzemi ellátási problémák
- Áramszünet
- Távközlési problémák
- Egyéb közüzemi probléma a számítóközpontban

Természeti katasztrófák
- Viharok
- Földrengés
- Áradás
- Tűzvész

Terrorcselekmények

Emberi hiba

Technológiai problémák
- Szoftverhibák
- Szoftverfrissítés
- Hardver meghibásodások

Ellenséges behatolás
- Vírusok
- Behatolás hálózaton, Interneten keresztül

A kockázatok elemzését hatékonyan segíti az alábbi áttekintő táblázat, amely az egyes katasztrófa-események lehetséges hatásait több üzleti szempont szerint értékeli, esetünkben egy telekommunikációs szolgáltató esetében *(3. ábra)*.

A táblázat háromfokozatú színskálán ábrázolja az egyes események negatív hatását az adott üzleti szempontok szerint.

3. ábra Táblázat a kockázatok értékeléséhez (L = alacsony, M = közepes, H = jelentős)

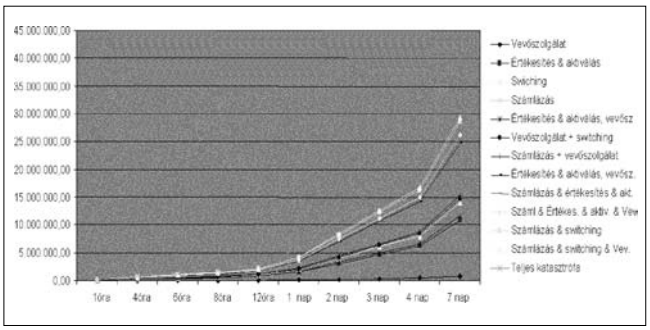
Típus	Esemény	1 óra	6 óra	12 óra	24 óra	3 nap	1 hét
Bevétel-kiesés	áramkimaradás	NA	NA	NA	M	H	H
	Kommunikációs hiba	NA	NA	NA	L	L	M
	földrengés	NA	NA	NA	H	H	H
	Számlázórendszer adatvesztés	NA	NA	NA	L	L	M
Vevők kiszolgálása / imázs	áramkimaradás	NA	NA	NA	L	M	H
	Kommunikációs hiba	NA	NA	NA	L	M	H
	földrengés	NA	NA	NA	H	H	H
	Számlázórendszer adatvesztés	NA	NA	NA	M	M	H
Működési hatékonyság	áramkimaradás	NA	NA	NA	M	M	H
	Kommunikációs hiba	NA	NA	NA	M	M	H
	földrengés	NA	NA	NA	H	H	H
	Számlázórendszer adatvesztés	NA	NA	NA	L	L	M
Összes pénzben kifejezett veszteség	Bármilyen üzemszünet	87.002	522.013	1.044.026	2.088.051	6.264.154	14.616.359

A katasztrófa-események üzletre gyakorolt hatása

A következő lépés a táblázatban szereplő események, pontosabban az általuk előidézett üzemszünet következményeinek alapos számbavétele. Ennek során – az üzlet jellegét és az igények szerinti szempontokat figyelembe véve – minél pontosabban kell meghatározni, hogy az egyes alkalmazások adott idejű üzemképtelensége mekkora veszteséget okoz. Az analízis része az alkalmazások és az egyes üzleti folyamatok összefüggéseinek pontos feltérképezése.

Az eredmények egy összefoglaló grafikon segítségével gyorsan áttekinthetőek; a *4. ábra* erre mutat be egy leegyszerűsített példát.

4. ábra Az alkalmazások üzemképtelenségének pénzügyi hatásai (távközlési szolgáltató esetében)



RTO és RPO előírások

Az üzletmenet-folytonossági megoldások hatékonyságát két paraméterrel lehet számszerűsíteni: az üzemképtelenség maximális megengedett idejét megadó RTO-val, és az adatvesztés megengedett mértékét szabályzó RPO előírással (lásd *„Az üzletmenet-folytonosság tervezés célkitűzései”*).

Mivel a gyakorlatban egy-egy alkalmazás több, eltérő RTO/RPO követelményt támasztó üzleti folyamatot is támogat, az elvárásokat egyenként kell számbavenni, és a megoldást a legszigorúbb feltételek szem előtt tartásával kell kialakítani *(5. ábra)*.

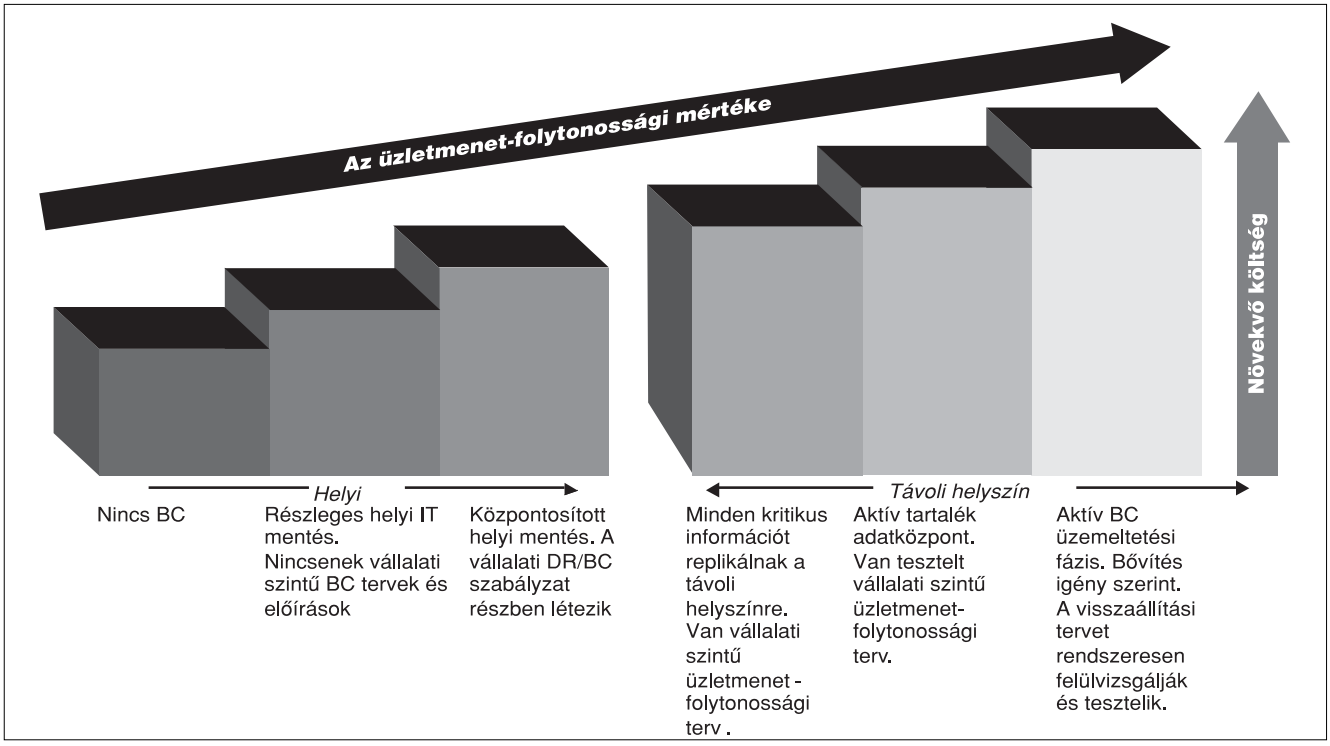
Alkalmazás	Az alkalmazást használó üzleti egységek száma	RTO (óra)	RTO Üzletág 1.	RTO Üzletág 2.	RTO Üzletág 3.	RTO Üzletág 4.	RTO Üzletág 5.	RTO Üzletág 6.	RTO Üzletág 7.	RTO Üzletág 8.	RTO Üzletág 9.	RTO Üzletág 10.	RTO Üzletág 11.
AAPC	1	120										120	
ACT!	1	48										48	
Adobe Acrobat	2												
Ancillary	1												
AOL Instant Messaging	2												
Bloomberg	7												
Business Objects	6											48	
CAL / VS Bidding	1												
CAL / ISO VENET	1												
CBS	1												
CCS	5											48	
CITRIX	1	48											
CLARUS	2												
CPT	1												
CPT-CAL Plant Tracking	1												
CQIG	2												

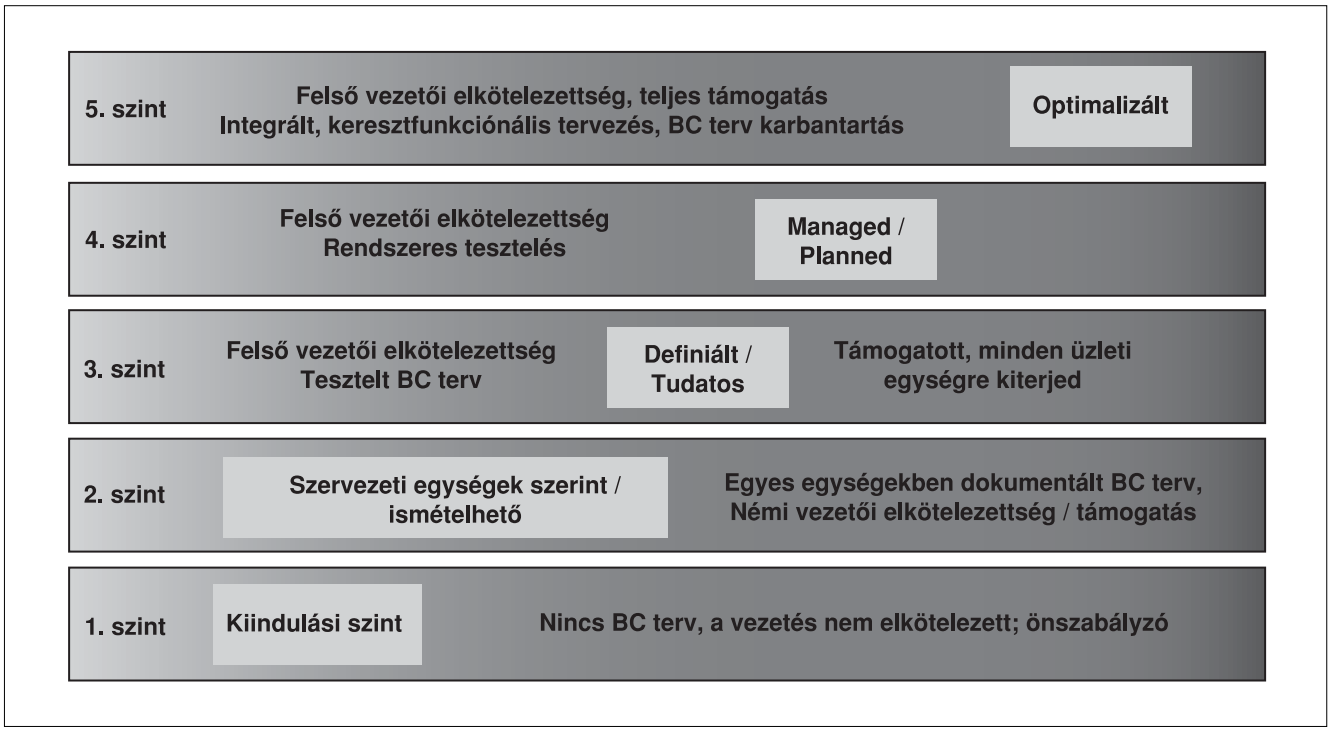
5. ábra RTO mátrix: az egyes üzletágak elvárásai az alkalmazásokkal szemben

A jelenlegi BC képesség felmérése

Az üzletmenet-folytonossági megoldások tervezése során a meglévő BC állapotból kell kiindulni, illetve a meglévő lehetőségeket kell kihasználni. Egy adott szervezet felkészültségét egy nem várt katasztrófa-esemény kivédésére elsősorban személyi-szervezeti és IT szempontból vizsgáljuk. A BC informatikai hátterének színvonala *(6. ábra)* mellett meghatározó a szervezet érettsége, amely értékelésére különböző modelleket dolgoztak ki *(7. ábra)*. Ezek a modellek a vezetői elkötelezettség, a BC folyamatok részletessége és hatóköre alapján osztályozzák, illetve kategorizálják az adott szervezet felkészültségét. Miután a fentiek szerint képet alkottunk az aktuális helyzetről, azt az elvárásokkal összevetve pontosan meghatározhatjuk a fejlesztendő területeket, az elmaradás mértékét és a legfontosabb teendőket. E szakasz végére tehát fel tudjuk vázolni, mi is pontosan az elvégzendő feladat.

6. ábra Az üzletmenet-folytonosság fokozatai





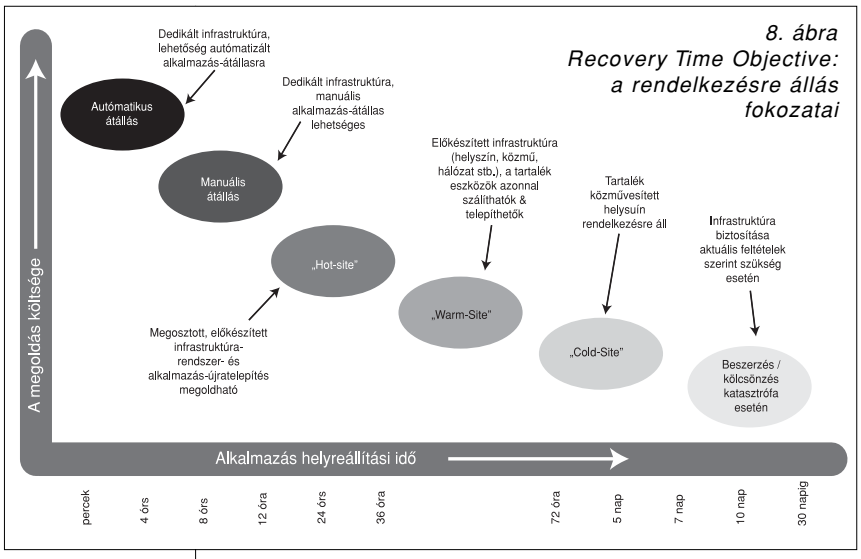
7. ábra Öt fokozatú üzletmenet-folytonosság érettségi modell (A CMU/SEI „Capability Maturity Model for Software" adaptációja)

A megoldási alternatívák elemzése a költséghatékonyság szempontjából

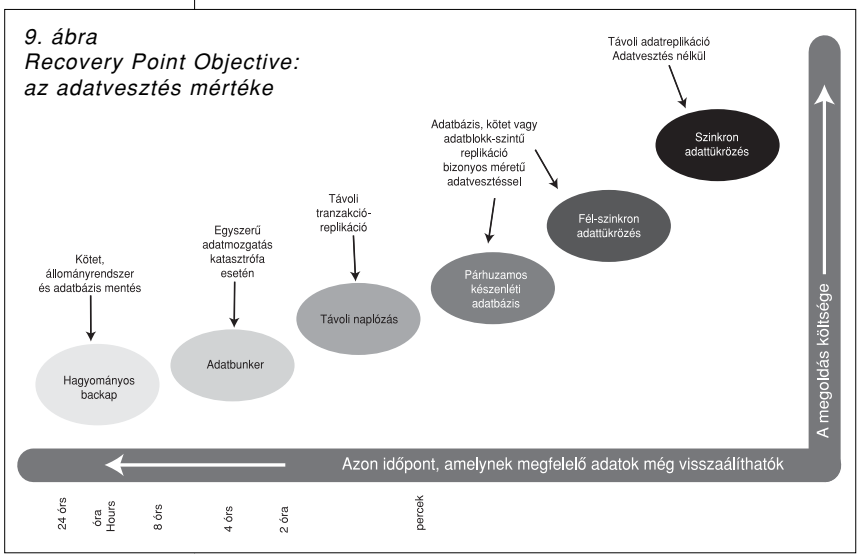
Az üzletmenet-folytonossági megoldások tervezésének döntő szakasza az optimális technológiai/szervezeti megoldás kiválasztása. A már említett RTO és RPO elvárások behatárolják a szóba jöhető technológiai megoldások körét: ha például az RPO szerint katasztrófa esetén nem veszhet el egyetlen tranzakció adata sem, mindenképpen szinkron adattükrözést (pl. EMC SRDF vagy MirrorView) kell alkalmaznunk *(8. és 9. ábra)*.

Mivel azonban a költségvetés nem korlátlan, a cél többnyire nem a technikailag legtökéletesebb megoldás kiválasztása, hanem az igényeket a lehető legkedvezőbb költségszint mellett kielégítő alternatíva megkeresése.

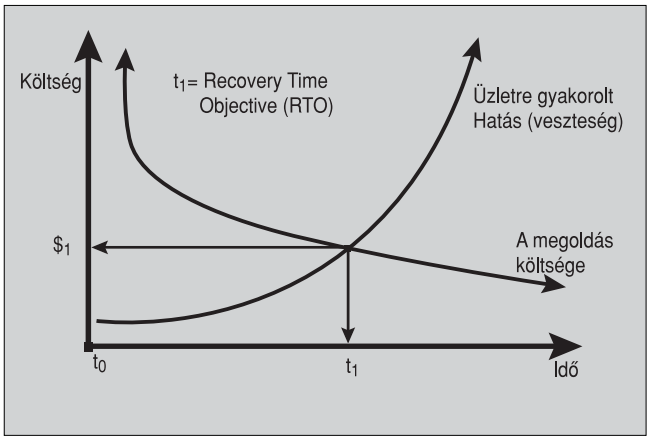
A fenti példánál maradva: hiába teszi lehetővé a szinkron adattükrözés az adatvesztés nélküli helyreállítást, ha ennek az ára adott esetben horribilis lehet (dedikált optikai kapcsolat, felsőkategóriás központi adattároló infrastruktúra, alkalmazás-integráció stb.)



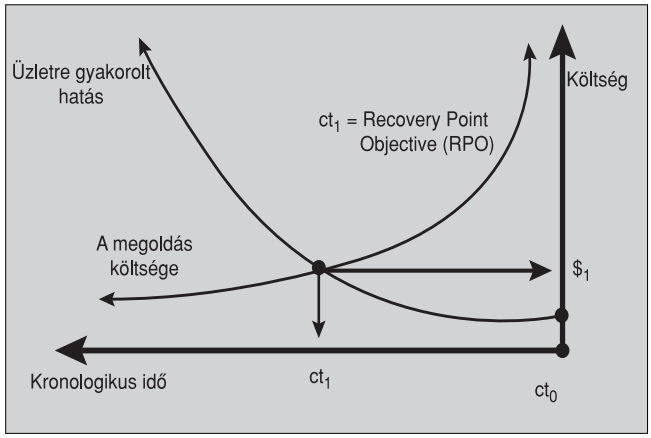
8. ábra Recovery Time Objective: a rendelkezésre állás fokozatai



9. ábra Recovery Point Objective: az adatvesztés mértéke



10. ábra A Recovery Time Objective és a megoldás költsége



11. ábra A Recovery Point Objective és a megoldás költsége

Nemcsak a megvalósítási költség abszolút mértéke lényeges, de az arányos ráfordítás is: nincs értelme milliárdokat költeni egy nagy használhatóságot garantáló technológiai megoldásra, ha az üzleti kockázat ennek csupán töredéke *(10. és 11. ábra)*. A cél az optimális ráfordítás mellett maximális biztonságot garantáló alternatíva megvalósítása.

Mi a siker titka?

A tapasztalatok szerint az üzletmenet-folytonossági megoldások megvalósításának sikere és a működtetés hatékonysága az alábbi alapvető tényezőkön múlik:

Vezetői elkötelezettség

Nem érhetünk el eredményt, ha nem kapunk támogatást a legfelsőbb szintű döntéshozóktól. Az üzletmenet-folytonosságnak a vállalati stratégia szerves részét kell képeznie.

Hatékony, rendszeresen ellenőrzött Üzletmenet-folytonossági Terv

A vállalati stratégiához igazodóan részletes üzletmenet-folytonossági tervet kell készíteni, azt rendszeresen felül kell vizsgálni és hozzáigazítani a megváltozott belső és külső körülményekhez. Az élet számtalanszor bebizonyította, hogy a legaprólékosabb BC terv is csak akkor ér valamit, ha azt a valóságban is kipróbálták és rendszeresen tesztelik.

Oktatás és gyakorlás

A dolgozóknak tudatában kell lenniük a BC tervben rájuk háruló feladatoknak, és azok önálló végrehajtását rendszeresen gyakorolniuk kell; ennek hiányában egy valódi katasztrófa-esemény egészen biztosan káoszt eredményez.

Hírek

A **Gazdasági Versenyképesség Operatív Programja** (GVOP) fogalmazta meg a gazdasági versenyképesség növelését célzó azon pályázati lehetőségeket, amelyek többek között hozzájárulnak az információs társadalom és gazdaság fejlesztéséhez is. A fejlesztésre 2004-ben összesen 7,66 milliárd forint uniós forrásokat is tartalmazó támogatás áll rendelkezésre. Március 11-én beérkezett az IT Információs Társadalom Közhasznú Társasághoz az első olyan pályázati munka, melynek beküldője európai uniós forrásokat is tartalmazó támogatás elnyerésére pályázott. Ez a „Vállalaton belüli elektronikus üzleti rendszerek” elnevezésű pályázatra érkezett. Amennyiben az első pályázatot benyújtó vállalkozás tervezett projektjét és ennek megvalósítását a szakmai bírálóbizottság megfelelőnek ítéli, úgy a cég 10 és 50 millió forint közötti, vissza nem térítendő támogatást nyerhet el.

A csehországi Hradec Kralovéban konferenciát tartottak a visegrádi együttműködés tagországai. A tanácskozáson az Európai Bizottság képviselőjétől vette át a **„EuropeCrest 2004 – a legjobb európai honlapok”** díjat Nyíregyháza a város honlapjáért. A díjátadáson Jambrik Mihály államtitkár a Magyar információs társadalom stratégiáról tartott előadást és kétoldalú tárgyalásokat folytatott partnereivel.

Elektronikus szavazás – messze még az út vége

BOROVITZ TAMÁS

borovitz.tamas@ittk.hu

Kulcsszavak: biztonság, ellenőrizhetőség, e-kormányzat, kényelem és veszélyek

Sokszor halljuk manapság: „A" országban elektronikus szavazásokat tartottak, vagy: „B" település önkormányzati választásain a szavazók online adhatták le voksukat. Különböző technológiai megoldások, más és más tapasztalatok és problémák mindenütt. Akadnak szenvedélyes pártolók és – persze – heves ellenzők. Tekintsük át, mi minden tartozik az e-szavazás fogalomkörébe, majd pedig nézzük meg, milyen érveket hoznak fel az e-voksolásra való átállás mellett és ellen.

1. Változatok e-voksolásra

A szavazási procedúra informatizálása nem új jelenség, hiszen számos országban régóta bevett szokás a szavazatok elektronikus összesítése; évek óta működik az egyes választókörzetek eredményeiből országos választási végeredményt produkáló rendszer.

Az e-szavazás alatt azonban többnyire a voksolás azon formáit értjük, amikor nyilvános szavazóhelyen vagy otthonunkban leadott szavazatunk nem tollal a szavazócédulára elhelyezett ikszelés formájában, hanem – PC vagy kéziszámítógép, érintőképernyő, mobiltelefon stb. segítségével – elektronikus úton történik.

Az e-szavazás három leggyakoribb típusa:

• A szavazóhelyiségben zajló online szavazás, amelynek során a szavazatok menetét választási bizottság felügyeli. A hagyományos procedúrával szemben azonban itt a választópolgárnak nem feltétlenül saját szavazókörzetéből kell leadnia a voksot.

• A nyilvános kioszkban (postán, könyvtárban, művelődési házban, bevásárlóközpontban stb.) leadott voksok, illetve a

• távszavazás (internetes szavazás), amely lehetővé teszi, hogy akár otthonunkból is szavazhassunk a számunkra szimpatikus jelöltre, pártra stb.

A távszavazás elterjedt (de nem elektronikus) formája ezen kívül a voksok postai úton történő elküldése is.

2. Mitől jobb vagy rosszabb, mint a hagyományos?

Az e-szavazás imént felsorolt formáinak története nem nyúlik vissza a régmúltba, azonban az elmúlt néhány év is számos olyan esettel szolgált, amelyek bőségesen kínálnak pro és kontra érveket az elektronikus voksolás támogatói, illetve ellenzői számára.

Megkíséreltük összegyűjteni azokat az argumentumokat, amelyek a leggyakrabban elhangzottak az e-szavazás kapcsán.

PRO

1. Kényelmes. Az egyik leggyakrabban hangoztatott érv az e-voksolás mellett a kényelmi tényező; hogy a választópolgárnak (a gyakran hétvégén megrendezett szavazáskor) ne kelljen kimozdulnia otthonából. Az állampolgárok politikai életben való aktívabb részvételét sürgető pártok és kormányok számára a komfortos körülmények közti szavazás biztosítása is egy fontos lehetőség a „mozgósításra".

2. Idő és költségkímélő (a választópolgár számára). A kényelem mellett az sem elhanyagolható szempont, hogy a számítógépe segítségével otthonából szavazó állampolgár – azzal, hogy nem szükséges ellátogatnia az urnákhoz – időt és költséget is megtakarít.

3. Költségkímélő (a kormányzat számára). Természetesen a választásokat kiíró (ön)kormányzat számára a legjelentősebb tényezők közé tartozik a költséghatékonyság. A nyomdai költség, a papírurnák előállítása és helyszínre szállítása mind jelentős kiadást jelentenek, melyek ilyen módon megspórolhatók. A kézi szavazatszámlálás kiküszöbölése pedig jelentős időmegtakarítást von maga után.

4. Részvételt biztosít a hagyományos voksolásból részben kizárt személyek számára. Talán a legfontosabb érv az e-választások mellett. Az információs társadalom programok és stratégiák alapvető eleme, hogy mindenki számára egyforma lehetőséget kell biztosítani az IKT-eszközökhöz való hozzáférésre. A fogyatékkal élők, a betegek, a mozgásukban korlátozott idősek számára az elektronikus szavazási lehetőség biztosíthatja a demokráciában való részvételt. Ugyanígy az otthonuktól távol dolgozók, a külföldön tartózkodók stb. is élhetnek szavazati jogukkal ilyen módon.

5. Növelheti a részvételi arányt. Az e-választás megrendezését fontolgató kormányzatok komoly reményeket fűztek a választások részvételi arányának megnövekedéséhez. Angliában például akkor határoztak először az online voksolás teszteléséről, amikor az országos választásokon történelmi mélypontra zuhant az urnákhoz járulók aránya. A kitűzött cél tehát az volt, hogy

az online is leadható szavazatok jelentősen emeljék meg a részvételi arányt. (Sajnos ez a várakozás, mint később kiderült, nem igazolódott, erről bővebben az ellenérveknél írunk).

6. Maga a Web is aktivizál. A WWW sokak számára a demokrácia gyakorlásának alapvető eszközévé vált. Állampolgárok milliói nap mint a nap a világhálón – fórumokon, csevegőszobákban stb. – vitatják meg az aktuális politikai kérdéseket, fejtik ki álláspontjukat saját honlapokon, blogokon. Ennélfogva természetes „elvárás" lehet, hogy akik gyakorlottak az e-véleményalkotás terén, azok a demokráciában való részvétel legfontosabb pillanatát, a szavazást is online kívánják véghezvinni.

7. Modern. Az információs technológiai eszközök, valamint a kommunikáció modern csatornái iránt fogékonyak számára fontos lehet, hogy a szavazásnak az újszerű, informatizált módját választhatják. Az e-szavazást tesztelő kormányok úgy vélték, hogy éppen az IKT-eszközök alkalmazása révén érhetik el azt, hogy a választásokon való részvétel illetve a politika iránti érdeklődés szempontjából rendszerint passzívabbnak bizonyuló fiatalokat is rábírhatják a szavazásra.

A Harris Interactive 2000-es adatai alá is támasztották ezeket a vélekedéseket: a felmérés ugyanis azt mutatta, hogy az online szavazás némiképp összefügg az életkorral: míg a 65 év felettiek 36 százaléka nyilatkozott úgy, hogy szívesen szavazna az interneten, addig a 18-24 éves korosztály esetében ez az arány 62 százalék volt.

8. Választási lehetőséget kínál. A demokrácia a választás lehetőségét kínálja, épp ezért fontos, hogy az állampolgárok ne csak jelöltek, pártok stb. közül választhassanak, hanem aközött is, hogy a voksolás hagyományos vagy elektronikus formáját kívánják választani. Amennyiben pedig az e-szavazás mellett döntenek, akkor arról is határozhassanak, otthoni PC-jük vagy mobiltelefonjuk, esetleg kéziszámítógépük vagy egy utcai terminál legyen az eszköz, amely segítségével leadják voksukat.

9. Áthidalja az írástudatlanság és a nehezen olvasható kézírás problémáját. A világ számos pontján még mindig jelentős probléma az írástudatlanság. Az elektronikus szavazás egyes változatai azonban lehetőséget adnak egyszerű szavazóbillentyűk használatára, esetleg számkombinációk beütésével is kiválasztható a szimpatikus párt/jelölt.

Egy másik probléma is kiküszöbölhető a szavazógépekkel: gyakran hiába veszik a fáradtságot az állampolgárok, hogy felkeressék az urnákat, mert az általuk kitöltött cédulák sokszor érvénytelenek maradnak. A szavazatszámlálók nem tudják egyértelműen eldönteni, melyik jelöltre kívánt voksolni az illető, ilyenkor természetesen érvényteleníteni kell a szavazatot. Az e-szavazásnál ilyen eset (elvileg) nem fordulhat elő. (Az ellenérveknél bebizonyosodik, hogy sajnos mégis előfordulhat.)

Nézzük, mely érveket szokás felhozni az elektronikus szavazásra való átállás ellenében:

KONTRA

1. Azonosítás vs. Anonimitás. Ami a problémákat illeti, az első számú gond az online voksolás biztonságának kérdése: az elektronikus szavazás ugyanis jóval magasabb biztonsági szintet követel meg, mint például az online vásárlás. A biztonsági megoldások kapcsán rendszerint szóba kerül a biometrikus technikák (az írisz- vagy az ujjlenyomat-azonosító eljárások) alkalmazásának lehetősége, azonban így sérülne egy másik, a választásokkal kapcsolatban létfontosságú követelmény: az anonimitás. Azonosítani kell a szavazásra jogosultakat, biztosítani kell, hogy mindenki csak egyszer szavazhasson, de úgy, hogy közben ne derüljön fény arra, hogy a voksolás során használt azonosító mely választópolgárhoz tartozik. Az ellentmondásra megoldás lehet a rendszer kettéválasztása. Először – az adatkezelési elveknek megfelelően – létre kell hozni a személyes adatokból generált szavazási azonosítót a hozzá tartozó jelszóval együtt, majd ezek után egy másik rendszernek kell kiértékelni a szavazás eredményeit. Ebben az esetben a szeparáltság biztosítja azt, hogy az állampolgárok anonim módon szavazhatnak.

2. Egyéb biztonsági és technikai problémák. Emellett természetesen ki kell emelnünk, hogy a biztonsági problémát nem csak a más helyett leadott szavazatok (azaz az „ellopott" személyazonossággal való visszaélés), vagy éppenséggel az egy választás alatt egy személy által többször is leadott voksok jelentik, hanem a kiélezett politikai helyzetben szinte menetrendszerűen jelentkező hackertámadások. A kiberhadviselés ma már sajnos mindennapossá vált, elég, ha csak az iraki háborúban vagy az izraeli-palesztin viszály nyomán elkövetett rendszer vagy szájt-feltörésekre gondolunk. Az e-választási rendszerekbe vagy akár az eredményeket nyilvántartó szájtokra történő behatolás alapjaiban rengetheti meg az egész demokratikus rendszert. Számos elektronikus választási kísérlet kudarcát pedig olyan „hétköznapi" problémák okozták, mint a rendszer lassúsága vagy lefagyása, a hálózatok jelentős részének ráadásul egy esetleges áramszünet is gondot jelenthet. A biztonsági problémák kiküszöbölésén sokat javíthatna a rendszerek (előzetes) vizsgálatának lehetősége, ám azok felépítése (pl. a forráskód) legtöbbször kereskedelmi megfontolások miatt nem tanulmányozható.

3. A (választói) bizalom hiánya. Az e-kormányzás és az e-demokrácia egyik kulcsszava az átláthatóság: sok esetben éppen az információs technológia eszközei tudnák bebizonyítani, hogy az adott országban működő kabinet tisztességes eszközökkel kormányoz, átlátható pénzügyi folyamatokat működtet. Egy kormányzati weboldalon nyilvánossá tett állami szerződés révén a polgárokban a kitárulkozó, üvegzsebű, tiszta és elszámoltatható kormány képe alakulhat ki. Az elektronikus szavazás iránti bizalomról sajnos éppen ennek ellenkezője mondható el: a polgárok, éppúgy mint a választásokban érdekelt felek gyakorta hangoztatják, hogy az online szavazási procedúrába nem lehet belelátni; nem adott a lehetőség annak ellenőrzésére, hogy a vokso-

lások végeredménye valóban a leadott szavazatok összességéből adódik, nem pedig külső beavatkozás, csalás során kialakult eredmény. A bizalom hiánya kapcsán merült fel a szavazógépek nyomtatóval való ellátásának szükségessége. Az ellenőrző szelvényre nyomtatott voksok ugyanis lehetőséget adnak az újraszámlálásra, így az elsőre kialakult végeredmény könnyen alátámasztható vagy megcáfolható. A printerek ellen felhozott érvek: a viszonylag magas nyomtatási költség és a folyamat lassúsága.

4. Befolyásolás lehetősége. És, ha már a bizalom kérdését említettük: az sem kedvez túlságosan az e-választások végeredményének feltétel nélküli elfogadásának, hogy nehezen ellenőrizhető, hogy otthonában (vagy akár egy bevásárlóközpontban felállított terminált használva) önállóan szavazott-e a polgár, vagy valaki esetleg befolyásolta a kattintás pillanatában. (A külső presszió egyébként ma már a hagyományos voksolásnál sem zárható ki, nemrég olvashattuk ugyanis, hogy az eBay-en egy amerikai állampolgár a következő elnökválasztáson leadandó szavazatát árusította… A „vevő" garanciát kapott arra, hogy az „eladó" az urnáknál arra a jelöltre adja le a voksát, amelyikre a voks megvásárlója rábeszéli.)

5. Digitális szakadék. Ha már a pro érvek számbavételekor az elsők közt említettük azt a nagyszerű lehetőséget, amelyet a távszavazás nyújt például a fogyatékkal élők számára, akkor a legkomolyabb problémák közt kell említeni azt, hogy az e-választás nem mindenki számára elérhető. Számos országos és nemzetközi szintű program és stratégia kimondja, hogy az információs társadalomban mindenki számára egyformán kell biztosítani a hozzáférést. Ráadásul a demokrácia „játékszabályaihoz" hozzátartozik, hogy a választópolgárok minden körülmények között leadhassák a voksukat, amennyiben szavazati jogukkal élni kívánnak.

Az e-szavazásból azonban számos csoport kimarad: így a PC-vel vagy internet-hozzáféréssel nem rendelkezők, a szavazás elektronikus változatától ódzkodók (pl. idősek, technofóbok) vagy éppen a digitális írástudással nem rendelkezők. (Természetesen minderre gyakran az a válasz érkezik, hogy ezek a csoportok ettől még nincsenek kizárva a választásokból, hiszen a hagyományos szavazásban részt tudnak venni.) Azt a tapasztalatot sem szabad figyelmen kívül hagyni, hogy az e-választások során a rosszul látó idősebb felhasználók számára több helyütt problémát okozott, hogy nem látták a kurzort. Előfordult az is, hogy egyesek erősebben, hosszabban nyomták meg a szavazógombot, ezért a rendszer lefagyott, ami komoly időveszteséget okozott.

6. Nem emelkedett a részvételi arány. Sajnálatos módon eleddig nem igazolódott be az a várakozás, amely pedig az egyik legfontosabb volt a szavazás online változatának kipróbálása előtt. A választók aktivitása nem emelkedett: nem adta le nagyságrendekkel több szavazó a voksát csak azért, mert elektronikus úton szavazhatott. Az Egyesült Királyságban a 2002-es helyi választások még reménykedésre adtak okot. Három körzetben lehetett elektronikusan is szavazni, a részvétel 8 százalékkal nőtt. 2003-ban egy közvéleménykutatás eredményei is a britek pozitív hozzáállásáról tanúskodtak (60 százalék érezte úgy, hogy az e-választás lehetősége növelné részvételük valószínűségét), azonban a 2003-as kísérletek már nem bizonyították a várakozásokat: kiderült, hogy a postai szavazás növeli a részvételi hajlandóságot, az elektronikus megoldások azonban önmagukban nem járulnak hozzá a részvételi arány jelentős növekedéséhez.

7. Nehezen feldolgozható eredmények. Az e-szavazási rendszerek egyes típusai olyan olyan kimenetet (feldolgozandó voksokat) produkálnak, amelyek értékelése, összesítése még a hagyományos választási struktúrához képest is lassabban zajlik. Floridában például lyukkártyás megoldással lehetett szavazni a 2000-es választásokon, ám, ha a választópolgárok nem nyomták meg kellő erősséggel az eszközt, akkor a szavazócédula nem lyukadt át, csak kidudorodott. A választási bizottságok tagjai pedig nem tudták eldönteni, érvényes-e az ilyen módon leadott szavazat. De ugyanitt említhetnénk azt a szintén amerikai esetet, amikor is 2002-ben a Maryland államban Montgomery megyében, annak ellenére, hogy a választási szakemberek többször elmondták, hogy a berendezések memóriakártyája az eredményeket modemen juttatja el a géptől a választási irodába, a kivehető kártya helyett néhány szavazóbiztos a teljes berendezést magával cipelte a választási irodába. A választások végeredményét emiatt még jóval éjfél után sem lehetett tudni.

8. A szavazás rituális örömeinek hiánya. Az e-voksolás ellenzői gyakran említik ezt az emberi-társadalmi tényezőt is. A szavazásokon való megjelenéshez kapcsolódó „rítusok", a kiöltözés, valamint a választási eredmények összesítésének, kihirdetésének közös figyelemmel kísérése – este, baráti társaságban összegyűlni a televízió előtt stb. – mind olyan, a szavazáshoz sokak számára hozzátartozó kedvelt, tradicionális elemek, amelyek az elektronizált választásokból hiányoznának.

3. e-szavazás másként, e-demokrácia sikertörténetek

Áttekintve a fenti érvek sokaságát, arra a következtetésre juthatunk, hogy az elektronikus szavazás ideje még nem jött el – túl sok probléma tűnik egyelőre megoldatlannak. Az új szavazási módszerek ellen felhozott argumentumok azonban nem szeghetik a kormányzatok és a fejlesztők kedvét, hiszen, bár az e-voksolás kapcsán egyelőre kevés a csak pozitív tapasztalat, az elektronikus demokrácia más terepein már sikertörténetekről is olvashattunk. Az online véleményalkotás egyéb módozatai: az online petíciók, a kisebb közösségeket vagy egész országot érintő kérdések webes megvitatása és a gyakran kézzelfogható eredményt produkáló internetes kezdeményezések a világ számos pontján remekül működnek, ami mindenképp biztató jelnek tekinthető a jövőre nézve.

Észtországban 2001. júniusa óta működik a „Tana Otsustan Mina“ („Ma én döntök“), elnevezésű webkikötő, melynek célja: serkenteni az állampolgárok részvételét a törvényhozás folyamatában. A felhasználók véleményt alkothatnak a parlament által tárgyalt törvényekkel kapcsolatban, de előterjeszthetik saját javaslatukat is. Amennyiben egy, az online viták során kialakuló indítvány legalább 51 százalékos támogatást kap a szájt látogatóitól, az illetékeseknek kötelességük lesz figyelmet fordítani a kérdésre, és megtenni a szükséges intézkedéseket a „követeléssel“ kapcsolatban. A weben pedig ezután nyomon követhető a javaslat további sorsa, az állami adminisztráción keresztül megtett útja. Ha sikeresen átverekszi magát a javaslat, a parlament elé kerülhet, de amennyiben nem fogadják el, a szájton fel lesz tüntetve az elutasítás oka.

Számos e-demokrácia projektet indított 2003-ban az Európai Unió görög elnöksége. Az iraki válság során például felhívta valamennyi tagország állampolgárait, hogy vegyenek részt abban az online szavazásban, amelyben véleményt alkothatnak országuk kormányának az iraki válság megoldásával kapcsolatosan kialakított álláspontjáró. A görögök a jelentős részvétellel lezajlott szavazás után minden hónapban kikérték az állampolgárok véleményét olyan kardinális kérdések kapcsán, mint a bevándorlás, a menekültügy, az EU-bővítés stb., majd az online voksolások eredményeit ismertették a csúcstalálkozókon és a Tanács ülésén. Az e-voksok leadása után, a szavazásban résztvevők – táblázatok és grafikonok segítségével – tájékozódhattak arról, nézeteik összhangban vannak-e a többi tagország és a csatlakozás előtt álló államok polgárainak véleményével.

Skóciában néhány hónapja működik az a rendszer, melynek segítségével az állampolgárok e-petíciót nyújthatnak be, közvetlenül a Parlamentnek. A Skót Képviselőház által elindított elektronikus rendszer lehetővé teszi, hogy az állampolgárok a világhálón megvitassanak egy-egy témát, majd indítványt nyújtsanak be azzal kapcsolatban. A fogalmazványok meghatározott ideig elérhetők a világhálón, mielőtt a parlament elé kerülnek. Az országgyűlés beadványokkal foglalkozó bizottsága ezután megvizsgálja a petíciót, a rendszert kifejlesztő Napier Egyetem szakembereitől kapott jelentéssel együtt, amelyben az adott beadvány támogatottságának mértékéről tájékoztatják a bizottsági tagokat, valamint összegzik a petíció kapcsán folytatott online vita tapasztalatait. Az új e-petíciós lehetőség a törvényhozás nyíltságáról és elérhetőségéről tanúskodik, nem véletlen, hogy a rendszer máris elismerést és érdeklődést váltott ki külföldön.

A példákat szerencsére sokáig sorolhatnánk, és magyar példákat is említhetnénk, gondoljunk csak a peticio.hu szájtra, ahol számos témával kapcsolatban alkothatunk véleményt, szavazhatunk. Ugyanígy az online közösségi döntéshozatal terepe lehet egy internetes fórum, elég, ha pl. az Index törzsasztalának aktív résztvevőire utalunk, akik mozgalmakat indítottak utcanevek megváltoztatására, gyűjtést szerveztek stb, tehát az internet és az elektronikus véleménynyilvánítás eszközének segítségével hatást tudtak gyakorolni szűk vagy tágabb környezetük életére.

Ha a döntéshozók komolyan veszik a „népakarat” efféle megnyilvánulásait, és észbe kapnak, hogy a demokráciában, a politikában ma már nem kevés döntés születik online, akkor talán az elektronikus szavazás fejlesztésére is még több forrást és energiát fordítanak, hiszen az e-szavazás sikere az ő érdekük is.

Irodalom, források

[1] Kaposi Ildikó:
Nemzetközi kísérletek az elektronikus szavazás alkalmazására. E-kormányzat első kézből projekt. Infonia Alapítvány, Budapest 2003.

[2] Borovitz Tamás:
Az e-voksolás jövője.
HP Magazin, 2002. november.

[3] Angol nyelvű online források:

Security Poor in Electronic Voting Machines, Study Warns
www.nytimes.com/2004/01/29/technology/

E-Votes Must Leave a Paper Trail
www.wired.com/news/print/0,1294,61334,00.html

Ireland launches e-voting campaign
www.enn.ie/frontpage/news-9389798.html

For Brazil Voters, Machines Rule
www.wired.com/news/print/0,1294,61654,00.html

E-voting controversy in Ireland
www.australianit.com.au/articles/

[4] Magyar nyelvű online források:

Anglia online választásokra készül
www.index.hu/tech/net/netval/

Online szavazás lesz tavasszal – Angliában
hirek.prim.hu/cikk/23243

Elektronikus szavazás: kudarcok a premieren
index.hu/tech/tudomany/wired/?print

Elektronikus szavazás a gyakorlatban
index.hu/tech/jog/eszavaz/

Interaktív kormányzás Észtországban
www.ittk.hu/infinit/2001/0628/kk1.html

Hibás az amerikai elektronikus szavazórendszer
hirek.prim.hu/cikk/34179/

EU: elektronikus szavazás az iraki válságról
www.ittk.hu/infinit/2003/0220/egov1.html

Az írek többsége az e-szavazás mellett
www.ittk.hu/infinit/2003/0814/egov2.html

Skócia: elektronikus petíció
www.ittk.hu/infinit/2004/0219/indexeg1.html

Mégsem lesz idén elektronikus szavazás az USA-ban
www.terminal.hu/newsread.php?id=09204902043012

Kockázatos az elektronikus szavazás?
szt.hu/hirekőhir.php?id=33814

Hírek

A Sun Microsystems februárban szemináriumot rendezett a leendő EU-tagországok politikusai, kormányzati hivatalnokai számára **„Az e-kormányzat infrastruktúrájának kiépítése”** címmel. A rendezvény célja az volt, hogy az e-kormányzattal kapcsolatos tapasztalatokat megossza a csatlakozó országok döntéshozóival, bemutassa az állampolgár-centrikus e-kormányzati szolgáltatások gyakorlati előnyeit és a megvalósított megoldásokat. A szeminárium első felében Csepeli György, az IHM politikai államtitkára, valamint Bradier Ágnes, az Európai Bizottság e-kormányzati szakértője beszélt az EU e-kormányzati programjairól, majd a Sun szakemberei az Európában működő legjobb gyakorlatokat mutatták be.

Az Európai Unió e-Europe 2005 programjának értelmében az EU tagországainak 2005-re rendelkezniük kell modern, elektronikus közszolgáltatásokkal az e-kormányzat, e-oktatás és e-egészségügy terén. A vállalkozások életében jelentős szerepet kell játszania az e-kereskedelemnek, mindehhez pedig megfizethető, elérhető szélessávú hozzáférésre és biztonságos informatikai infrastruktúrára van szükség. **Eger önkormányzata a 2004. április 6-án átadott e-kompetencia központtal** fontos lépést tett az e-közigazgatás sikeres megvalósítása felé. Az Eszterházy Károly Főiskolán átadott kompetencia központ arra mutat példát, hogy az önkormányzat, a hozzátartozó intézmények, a kistérség és a lakosság közötti információáramlás hogyan valósítható meg a lehető leghatékonyabban szélessávú internetes kapcsolat segítségével.

„A Matáv 2003-ban 10 milliárd forintos nagyságrendű beruházást hajtott verge az internetes piacon kitűzött céljainak megvalósítása érdekében. A beruházás nagy részét a szélessávú internetezés elterjesztésére fordítottuk. Ennek eredményeként a tavalyi évben 175 településre jutott el a szolgáltatás. 2004-ben tovább kívánjuk bővíteni a szélessávú internet lefedettséget. A Matáv hálózatában 2000-ben kezdtük meg a Cisco technológiára épülő IP gerinchálózat kiépítését, amely jól szolgálja a hazai információs társadalom folyamatos fejlődését.” – mondta Sipos Attila, a Matáv hálózatfejlesztési igazgatóhelyettese.

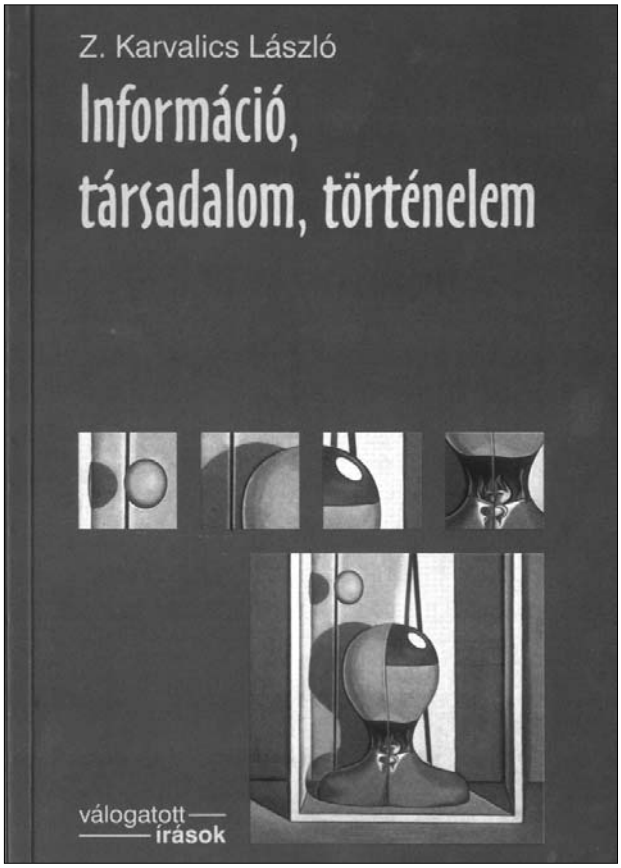
Magyarországon a tavalyi év végén 100 ezer vállalkozás és háztartás rendelkezett szélessávú internetkapcsolattal. Ma már **minden harmadik otthoni internetező szélessávon használja a világhálót, amellyel az EU-ban is az élvonalban vagyunk.** A tavalyi sikerek alapján a Matáv idén további 100 ezer ADSL előfizető bekapcsolását tervezi, így nagymértékben hozzájárul ahhoz, hogy Magyarország a kelet-európai régióban az egyik legmagasabb szintű szélessávú hozzáféréssel rendelkezzen. A megnövekedett igények kiszolgálására 2003 novembere és 2004 márciusa között sor került az országos IP gerinchálózat decentralizálására, valamint a budapesti gerinchálózat bővítésére 2 Gb/s-ről 10 Gb/s-ra. A hálózati fejlesztésekhez a Matáv Európában az elsők között helyezte üzembe a Cisco a 720 Gb/s kapcsolási teljesítményű CATALYST6500 kapcsolóját. A budapesti hálózatban található Giga Switch Routerek között meglévő 1 Gbit/s összeköttetések kapacitását az új 10 Gbit/s kártyák telepítésével jelentősen megnövelték.

Megállapodást kötött az Informatikai és Hírközlési Minisztérium és a Microsoft. A megállapodás a közoktatási intézmények munkaállomásain, továbbá az általános iskolai és középiskolai oktatók otthoni számítógépein biztosítja a mindenkori legfrissebb Windows operációs rendszer és Microsoft irodai programcsomagok jogtiszta használatát. A megállapodás értelmében megkezdődik a programcsomagok telepítéséhez szükséges Microsoft Windows XP Professional frissítés és Microsoft Office 2003 Professional CD-k, valamint a kapcsolódó dokumentációk és tankönyvek kiszállítása. A megállapodás egyben szoftveramnesztiát is jelent, mivel a szerződés értelmében a Microsoft úgy tekinti, hogy a kedvezményezettek február végéig már meglévő gépein biztosított a frissítési alap függetlenül attól, hogy ezt legális licenccel igazolni tudják-e vagy sem.

Könyvet ajánlunk

Információ, társadalom, történelem

Olvasva Z. Karvalics László könyvét, első érzés az irigység. Szinte nem tudja az ember elképzelni, hogy milyen módon tud időt szakítani egy sokfelé elfoglalt szakember ennyi könyv, cikk elolvasására, a világ sok részének megismerésére és miként tudja az agyában ezt a sok ismeretet elraktározni. A fejében lévő tárolóból mindig a megfelelő információkat hívja elő ahhoz, hogy a különböző esetekhez analógiákat, példákat találjon.



Könyvét olyan érdekes formában írta meg, hogy a legbonyolultabb informatikai, vagy történész megállapításokat megfelelően összekötve, irodalmi idézetekkel alátámasztva, regényként lehet olvasni. Úgy jutunk hozzá az információval kapcsolatos szakmai és történeti ismeretekhez, hogy közben határozottan élvezzük az analógiákat, a bevezető kis történeteket és a kiragadott idézeteket. Az információ és kommunikáció kapcsolatáról írt első rész minden fejezetét egy Kevin Hawk: Testvérek című könyvének idézetével vezeti be. Olvasottságára jellemző, hogy amikor ezt meg akartam keresni a több mint 200 hivatkozást tartalmazó irodalomjegyzékben, nem találtam. Ugyanígy nincs benne az irodalomjegyzékben Shannon, vagy Orbán Ottó. Ezek és sok más a szerző fejében már kiérett és szinte sajátjának tekintett megállapítások. Már ezekért az idézetekért is érdemes végigolvasni a könyvet.

Az első rész az „Információ társadalom elmélete felé” a sok könnyed megállapítás után a legfontosabb problémákat fejtegeti: az információ mérhetőségét és az elképzelt mérések hasznosságát. Eközben is találunk hivatkozásokat Kolmogorovra és Aquinói Szent Tamásra. Már ez a páros is mutatja, hogy mennyire különböző nézetekből igyekszik az igazságot megfogalmazni. Számomra nagyon tanulságos volt a pénz és idő összevetése, hangsúlyozva, hogy az idő talán még nagyobb érték, mint a pénz.

A következő rész címe „Információs rendszerek – információ történelem”. Szintén meglepő kutatási eredményekkel végződik, mert a kőkorszaki eszközök új értelmezését olvashatjuk. Megtudjuk, hogy a szilánk nem melléktermék, hanem nagyon fontos eszköze volt a kőkorszaki embernek. De tanulságos az is, hogy könyvégetéssel nem lehet forradalmi tanokat elpusztítani, de még a szerzők elégetése sem segít. Az érdemi nagy megállapítások mellett nem szabad elhanyagolnunk két másikat sem. Az egyik az információs minta bevezetése, másik a professzionális módon tárgyalt könyvtárrendezés problémája. A fejezet végére beválogatott Harold Adams Innis megemlékezés nemcsak mint tiszteletadás érdekes, hanem az újságíró számára is programot ad. Az adatbiztonság és a galambok, vagyis a i.e. III. évezred biztonsági megoldásai azt igazolják, hogy a galambokat is lehet idomítani.

A könyv harmadik része Az „Információs Társadalom” kihívásai nyomában már napjaink gondjait tükrözi. Szinte minden fejezet olyan problémát vett fel, ami azért érdekes az idősebb generáció számára, mert mind a tévtanokat, mind azok bukását átélte. Itt különösen a teleházzal kapcsolatos történetek kötik le az olvasó figyelmét.

A szerző szokásos könnyed, csevegő stílusában tanít meg érdekes újdonságokra, vezet be a múlt nem mindig helyesen megismert eseményeibe és mindezek tanulsága képpen, észrevétlenül az információs társadalom problémáival és azok megoldási lehetőségeivel is találkozunk. Bár szakmai értelemben akár tankönyvnek is tekinthető, de ha vacsora után vesszük kézbe, akkor sem tudjuk letenni.

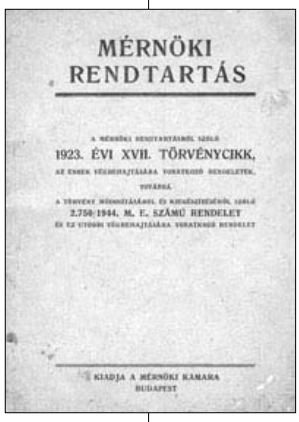
A múlt tanulságait ismerve építsük a jövőt
80 éves a Magyar Mérnöki Kamara

SIPOS LÁSZLÓ, az MMK Elnökségi tagja

siposlaj@axelero.hu

A Magyar Mérnöki Kamara Választmánya március 10-én méltó módon emlékezett meg köztestületünk megalakulásáról. Az 1923. évi XVII. törvénycikk rendelkezett arról, hogy a mérnöki tevékenység és a mérnökség erkölcsi és anyagi érdekének a közérdekkel való egyeztetése érdekében kamara szerveződjön. Nyolcvan éve, 1924. március 8-12. között – dr. Zielinszki Szilárd műegyetemi tanár elnökletével – alakult meg a Budapesti Mérnöki Kamara, amely alapvető változást hozott az akkori mérnökök életében.

A Budapesti Mérnöki Kamara egykori székházának (V. kerület, Szalay u. 4. sz.) homlokzatán elhelyezett emléktábla megkoszorúzásával kezdődött március 10-én a Magyar Mérnöki Kamara Választmányi tagjainak egész napos programja. Ezt követően a Budapesti Műszaki és Gazdaságtudományi Egyetem Oktatói Klubjában tanácskoztak a megyei és tagozati (többek között a Hírközlési és Informatikai) elnökökkel kiegészült elnökségi tagok. Délután megemlékeztünk a nyolcvan éve történt eseményekről, majd a Zielinszki Szilárd életét bemutató könyvet ismerhettünk meg. Legvégül a család, a BME és a MMK vezetői koszorúkat helyeztek el a Műegyetem kertjében található Zielinszki szobornál. Hazaérkezve néhány gondolat fogalmazódott meg bennem, amit most közreadok.


MÉRNÖKI RENDTARTÁS

1923. ÉVI XVII. TÖRVÉNYCIKK,

2.750/1944. M. E. SZÁMÚ RENDELET

KIADJA A MÉRNÖKI KAMARA BUDAPEST

A Révai Nagy Lexikonban olvasható: *„Mérnöki Kamara, a mérnöki karnak önkormányzati alapon, hatósági jogkörrel felruházott szervezete, Budapesti székhellyel egyenlőre az ország egész területére kiterjedő hatáskörrel az 1923. XVII. tc. állította fel. A Mérnöki Kamarába a mérnöki cím használatára jogosult minden állampolgárt fel kell venni. Önálló magángyakorlatot csak kamarai tag folytathat. A tagok összességének ügyeit a közgyűlés, a folyamatos ügyeket a választmány és az elnök intézi.”*

Ez a korabeli szócikk – az 1945 és 1996 közötti kényszerszünet után – ma ismét érvényes, csak a törvényi hivatkozást kell kicserélni, az 1996. évi LVIII. számmal. De nem olyan jó a helyzet, mint nyolcvan éve. A hivatásrendi kamaráknak a mainál lényegesen jelentősebb szerepük kellene legyen a demokratikus közéletben, de még messze vagyunk e kívánatos állapottól. A hatékony demokráciák fontos eleme, a végrehajtásban közreműködő szakmai önkormányzatok ellenőrző szerepe.

Gondjaink megértése, céljaink kitűzése érdekében, érdemes visszatekinteni a múltra.

Az 1867-es kiegyezést követő fellendülés korában vetődött fel először, hogy a műszaki értelmiségnek érdekérvényesítő szervezetet kell teremteni, melyben egyrészt a mérnökök meghatározzák önmaguk helyét a társadalomban, másrészt a társadalom számára védelmet biztosítanak a szakmailag nem kellően felkészült vállalkozókkal szemben. Ennek első formája a Magyar Mérnök és Építész Egylet volt, mely közel ötvenéves küzdelmet folytatott azért, hogy törvény által megerősített köztestületet hozhasson létre.

Az 1945. januárjában betiltott mérnöki kamarát tizenöt évvel ezelőtt, 1989. március 9-én sikerült először egyesületi formában újjáalakítani. Az 1996. évi LVIII. Törvény alapján először a területi – elsőként 1996. november 7-én a Tolna megyei – mérnöki kamarák, majd 1997 januárjában a Magyar Mérnöki Kamara (MMK) alakult meg.

A rendszerváltás évét előszeretettel hasonlítják a kiegyezés évéhez. A cél akkor és most is ugyanaz, törvény által megerősített erős szakmai önkormányzattal biztosítani a műszaki tevékenység magas szakmai színvonalát és a megrendült etikai színvonal helyreállítását. A mai, immár tizenhétezer főt számláló mérnöki kamara a jelenleginél nagyobb szerepet kíván magának a közéletben, ehhez azonban szükséges, hogy a kormányzat felismerje, hogy a szakmai részletkérdéseket nem szabad a politika szintjén szabályozni, azt leginkább az abban dolgozók önkormányzati szervei tudják hatékonyan érvényesíteni.

Dr. Kováts Gábor, a MMK Elnöke vezetésével kezdeményeztük és létrehoztuk a magyar szakmai kamarák érdekérvényesítő fórumát, mely közel háromszázezer szakembert tömörít. Amennyiben a társadalomtól megkapjuk a kellő bizalmat, az európai csatlakozás után jelentősen hozzájárulhatunk hazánk gazdasági felzárkóztatásához és nemzetközi tekintélyünk növeléséhez.

„A világ nekünk dolgozik”

Interjú Dr. Prószéky Gáborral, a MorphoLogic Kft. alapítójával

NAGY BEATRIX HAVASKA

nbh@mailbox.hu

Bár a januári számunkban megjelent interjú mindhárom alanyaként jelentős kutatókat, fejlesztőket ismerhettünk meg, most újra kiemelten foglalkoznunk kell egyikükkel, illetve munkája kapcsán a beszédkutatással. Jelenleg ugyanis sokat hallunk az EU-adminisztráció fordítási nehézségeiről, ahol is közel két tucat nyelvről kell ugyanennyire fordítani, így ez a tevékenység komoly létszámú minőségi fordítót igényel. Ezen a problémán hivatott segíteni a jövőben a gépi fordítás. Most tehát térjünk vissza a beszédkutatás témakörére, amely ennek megoldását is ígéri.

a Szerk.

Gyorsuló világunkban mind fontosabbá válnak a technika újdonságai. Elvárjuk, hogy segítségünkre legyenek nap mint nap, a legegyszerűbb, hétköznapi dolgainkban is. Ezek közé tartozik a számítógépen jól ismert helyesírás-ellenőrző program is. Minden nap használjuk, de sokan nem is tudjuk, hogy ezt is egy magyar cég fejlesztette ki. Vajon miért nem ismerjük ezeknek a zseniális találmányoknak a magyar alkotóit? Ebből a beszélgetésből megismerhetjük a világhíres, magyar helyesírás-ellenőrző program alkotóját.

Mikor jutott eszébe, hogy szükség lenne azokra az ötletekre, amelyek azóta széles körben elterjedtek, és miért gondolta, hogy ezzel nemcsak tudományos elismertséget, hanem az országhatárokon túl nyúló üzleti eredményeket is elérnek?

Amikor elkezdtük, nem jutott eszembe semmi. Biztos, hogy az induláskor nem üzleti motiváció hatására állt össze a csapatunk. Lehet, hogy ez 2004-ban máshogy lenne, de ez még 1991-ben volt. Előtte rövid ideig Hollandiában dolgoztam és beleláttam a nyelvtechnológiába és annak lehetőségeibe. Több mesterséges intelligencia projektben vettem részt olyan helyeken, ahol ezeket „nagyban művelik”. Stanfordban, Helsinkiben akkor már hasonlót csináltak, mint később mi.

Az induláskor sem tudományos elismertségről, sem üzleti gondolkodásról nem volt szó. Többen kezdték már így az életüket. Én is éveken keresztül hallgattam egy kis szoftveres csoportnak az elképzeléseit, akik azt ígérték, hogy egyszer egy magyar helyesírás-ellenőrző programot készítenek. Ez a gondolat több konferencián is elhangzott. Én, aki matematikus és nyelvész is vagyok és ugyanezzel a témával foglalkoztam, elefántcsonttoronyban ültem a tudományommal, és azt nem hasznosítottam. Örültem, hogy szoftveres csoportok végre aprópénzre váltják a tudást, és milyen szép, hogy csinálnak az elképzelésekből valamit. Nekem ez nagyon tetszett, de mindig csak azt hallottam, hogy majd egyszer meglesz...

Erre jött a kisördög és azt mondta: mi el tudjuk ezt készíteni. Meg is csináltuk a helyesírás-ellenőrző programunkat, ami egy kicsit előbb készült el, mint másoké.

Hárman indultunk, most harmincan vagyunk. Így folyamatosan lehetett érezni azokat az üzleti eredményeket, amire mindig büszkék voltunk. Nagyon sokan az akadémiai világból jöttünk, így megtartottuk a tudományos értéket is. Ez tipikus magyar, közép-európai folyamat: ami tudományos, az bizonyára komplikált, lassú. Egy működő rendszer, amivel tudományos konferencián lehet megjelenni, és a piacon is el lehet adni, az némiképp ellentmondásnak tűnt.

Ars poeticánk, vagy ha úgy tetszik missions statementünk – az előbbi ellentmondás feloldása. Azaz: mert valami tudományos, az nem szükségképpen lassú és körülményes.

Mikor gondolt először arra, hogy a számítógépeket el lehetne látni helyesírási programmal, sőt aláhúzással jelezni tudja a nyelvi és mondattani gyengeségeket is?

Az akkori első 100%-ig magyarított szövegszerkesztőbe 1991-ben alkalmaztuk először eredményeinket. Innen kezdve egy láncreakció indult el, egymás után jelentkeztek a neves cégek, így a Word Perfect, a Lotus, majd később a Microsoft. Mindenki ellenőrizte, mi meg egyre javítottunk a minőségén.

Amikor láttuk, hogy ebből termék lesz, eldöntöttük, hogy legalább egy gmk-t össze kellene hozni. Jobb, ha jogi személy a gyártó, és nem magánemberek csinálják. Miután cégesedtünk és a partnerek komolyan vették az eredményeinket, érzékeltük, hogy itt többről van szó, mint egyszerű hobbiról, sőt, amit kitaláltunk, azzal már tudományos értéket is létrehoztunk.

Az említett másik csapat magyar helyesírás-ellenőrző programot akart készíteni. Mi egy nyelvleíró formalizmust hoztunk létre, amiben a magyar *az alkalmazások közül csak az egyik.* Lényegesen több munka, ha az ember egy általános eszközt alkot, viszont a későbbiekben ezerszeresen megtérül. Más nyelvre, más alkalmazásra viszonylag hatékonyan kezdtünk el ebből építkezni. Technikai gyakorlatunkat kis gépeken szereztük meg, így nyugat-európai potenciális versenytársainkhoz képest sokkal jobb helyzetben voltunk, mert létre tudtuk hozni kicsiben azt, amire ők nem voltak rákényszerítve. Több alkalommal azzal nyertünk, hogy a kis

gépeken alig volt hely az operációs rendszer és a futó program mellett, de mi meg tudtuk oldani a problémát.

A külföldi siker a tudásbeli háttéren túl azon alapult, hogy a 90-es évek elején kezdett érdeklődni a világ a szövegszerkesztőbe beépíthető nyelvi programok iránt. Akkor indultak el az első helyesírás-ellenőrzők. Viszonylag jó időpontban léptünk piacra, akkor szakadt fel a vasfüggöny. Ennek következményeként többeknek a magyarokon kívül is fontos lett a magyar nyelv, mert piacot akartak nyerni.

Bár a globalizációtól félnek az emberek, nehogy elvesszen az anyanyelv, de ez az a folyamat, amely támogatja a helyi kultúrákat. Magyarországon úgy lehet csak eladni, ha magyarul van minden kézikönyv, minden leírás. Ez 20 évvel ezelőtt egyáltalán nem így volt. Ez most egy óriási lehetőség. Nemcsak nekünk fontos, hogy magyarul legyen, hanem a külföldi cégeknek is, ráadásul ehhez mi tudunk technológiát gyártani.

Ez az első helyesírás-ellenőrzés csak egy alkalmazása volt a nyelvleírásnak, tehát a két betűköz között egy betűsorozat magyar szónak minősül, ragozott vagy bármilyen módon képzett magyar szónak, akkor az jó, ha meg nem, akkor meg kell mondani, hogy miért nem jó, és mi kell helyette.

Persze a feladatunk ennél sokkal nehezebb, a nagyon bonyolult magyar nyelvet olyan eszközökkel írtuk le, ahogy előttünk még nem tették. Ha a magyar a legbonyolultabb nyelv, akkor ezeket lehet alkalmazni más nyelvekre is. Ha valaki angolból indul, akkor már a németig is alig jut el, mert annyi nehézsége van a német nyelvtannal. Viszont ha a magyarból indul ki, akkor leegyszerűsítéssel jó lesz az a németre is.

Ez volt a későbbiekben az a lépés, ami megengedte, hogy más nyelvekre is írjunk programot. Így ez tényleg nyelvfüggetlen, az eszközöket pedig magunk, az utánunk jövő és az általunk alkalmazott kollegák tudása biztosítja. Lehetne javasolni másoknak is, hogy induljanak ki egy ilyen nyelvből, mint a magyar, de ha nem az anyanyelvük, akkor nem sikerülhet. Tehát nem azért, mert olyan okosak vagyunk a magyar gondolkodásunk miatt – mert abban nem hiszek –, hanem abban, hogy a magyar nyelvet kell leírni. Sokkal több változat szükséges, mint az angolnál, viszont ha megvan, akkor rengeteg minden olyant tudunk, amit mások nem. Például ugyananynyi idő alatt, ugyanolyan hatékonysággal, ugyanakkora helyen oldunk meg egy ezerszer nagyobb problémát.

A kérdés, hogy mikor gondoltam először arra, hogy a számítógépeket el lehetne látni helyesírás-ellenőrző programmal? Hát akkor, amikor más mondta, hogy ő meg szeretné csinálni. Csak aztán nem csinálta, vagy csinálta, de csak lassan.

A zöld aláhúzás egy másik probléma. Ezzel a Wordben mindenki találkozik, sőt ma már a magyar Officeban is. Ezzel a szóhatáron túl lehet látni. A szóhatáron túl az nem feltétlenül azt jelenti, hogy tökéletesen tudom, hogy mi van a mondatban, sőt pont az ellenkezője. Egy ilyen nyelvhelyességi programnak a legnagyobb érdekessége, hogy nem a jó mondatokra működik, hanem a rosszra, tehát nem tudjuk hogyan kell szép nyelvtant írni. Márpedig nekünk a hibákat kell megfogni. Ez igen egyszerűen hangzik: írjunk egy nyelvtant, és ami abba nem fér bele, az lesz a rossz, de ez nem így van.

Miért rossz? Mi hiányzik, miért és honnan? Tehát valószínűsíteni kell, hogy kihagyott egy vesszőt, külön írta, amit egybe kellett volna és így tovább. Ez nem csak annyi, hogy nem jó. A nyelvészek írnak olyan nyelvtant, ami egy adott nyelvre jó, és mindaz ami abba nem fér be, arra vállat vonnak. Nekünk pedig meg kell mondanunk, hogy miért nem, és ez nem egy egyszerű kérdés. Erre megint trükköket kellett elővenni: hogyan lehet szimulálni a magyarul írók hibáit? Általában olyanok írnak számítógépen magyar szövegeket, akik tudnak magyarul. Tehát nem a nyelvtanról van szó, hanem arról, hogy mi az, amit elnéztünk. A rossz magyar mondatokra írt nyelvtan működik a zölddel aláhúzó nyelvhelyesség ellenőrzőben is.

Erre nem mi gondoltunk, hanem adottak voltak a lehetőségek, hiszen akkor már része volt a magasabb szintű helyesírás-ellenőrző rendszer a Microsoft Wordnek. A magyar azt hiszem a hatodik volt a Microsoft nyelvei közül. Szerencsés helyzetben voltunk, hogy korán tudtunk lépni ebben az irányban.

Most, mint sikeres vállalkozók foglalkoznak-e korábbi kutatási eredményeik továbbfejlesztésével, vagy esetleg új területen igyekeznek eredményeket elérni? Hogyan vezetett az út a szakmai tudományos és műszaki eredményektől ennek üzleti alkalmazásáig?

Nem működne a cég, ha nem a korábbi kutatási eredményeink továbbfejlesztésével foglalkoznánk. Sikerült olyan irányokat megcélozni, melyek nem lezárt eredményt, hanem egy jó irányba való indulást kínáltak. Egy kutatás nem pont addig tart, ameddig a pénz.

Ez egy nehéz dolog, mert az üzleti életben, ha valamire nincs pénz, akkor azt nem folytatjuk. Az elején a legnehezebb az volt, hogy a kollegákkal megértessük, bár nagyon jó ötleteik vannak, de mivel a saját pénzünkből élünk, nem tudunk mindent megvalósítani. Ingyen nem tudunk dolgozni, mert akkor meghal a cég. Ezt a 90-es évek elején még sokan nem értették.

A mai napig mi, a három alapító vagyunk a tulajdonosai a cégnek. Semmi külső pénzügyi segítséget nem kaptunk. Senki nem vásárolt ki részeket, semmilyen különleges konstrukcióval nem támogattak bennünket. Ez pont azért van, mert megpróbáltunk nagyon kicsiket lépni. Lehet, hogy más 12 év alatt exponenciálisan felfut, mi viszont egy egyenes vonalú egyenletes mozgással megyünk előre. Nyilván ha nagyon üzletemberesen nézem, ez nem olyan izgalmas, mint egy nagyon gyorsan felfelé ívelő, vagy hirtelen bukni akaró, de értékes vállalkozás. Ez csak annak jó, akit az motivál, hogy amit csinál az jó, és természetesen az is, hogy ebből pénzt szerezzen, de nem extra profitot.

Az a célunk, hogy a még nagyobb kihívásokra még jobb válaszokat adjunk. Lényeges, hogy a kutatási eredményeket mindig összeépítsük a következővel, és próbáljuk ezt szerves egységgé tenni.

Ez már 12 éve működik. Mindig jelentkeznek új területek is, elég csak arra gondolni, hogy 5-6 évvel ezelőtt indult el rohamos fejlődésnek az Internet. 12 éve még csak azok a nyelvi problémák voltak, amiket az ember a saját gépén tárolt, de már lehetett szöveget szerkeszteni. Egy céges hálózatban a gépek összeköthetőek és az Interneten gyakorlatilag korlátlan számú szöveg érhető el. Az emberiség tudása, – még ha nem igaz, akkor is így van –, ott az Interneten, és ennek nagy része szöveg.

Folyamatosan figyeljük, hogy mi történik a világban. Szerencse, hogy a tudományos kapcsolataink miatt ez elég jól megy. Fordító rendszerünkhöz évekig gyűjtöttük a különböző modulokat, melyeket aztán egy nagy dominóként összeraktuk, és három éve elkezdtünk egy gépi fordítás projektet. Bár akkor már 100 emberév mögötte volt, tehát az első 10 év munkája. Ennek a területnek a legnagyobb kihívása a fordítás, az emberi fordítás valamilyen szimulációja, és ha ehhez valamit hozzá tudunk tenni, akkor az összes modul, amit eddig építettünk, nem volt más, mint melléktermék. Azokat technikailag és nyelvileg úgy készítettük, hogy be tudjuk építeni a rendszerbe.

Most is folyamatosan figyeljük az új területeket. Jó, hogy erre, az alapkutatásokra már három éve van állami támogatás, és reméljük, ez így is marad. Ma már vannak olyan kutatás-fejlesztési témák, melyek megemlítik a nyelvtechnológiát, ami 2000 előtt elképzelhetetlen volt. Nem is tudtak róla, így most nagy öröm, hogy feltűnt, és ebbe aktívan be szeretnénk szállni.

Sejtették-e, hogy kiinduló ötletük ekkora hatással lesz a következő évek szakmai társadalmára és mindenki, aki kapcsolatban van a számítógéppel vagy az Internettel, ismeri nevüket és használja eredményeiket?

Menet közben tűnt fel, hogy fontos, amit mi csinálunk: a legnagyobb példányszámban használt Magyarországon írt szoftver a helyesírás-ellenőrző. Ez köszönhető a Microsoftnak és a konkurenseknek is, mert az összes platformon fut.

Ott vagyunk minden ember gépén, több mint 2 millió példányban – befolyásoljuk a magyar helyesírást. Nem akarjuk, de így van. Azt a felelősséget kaptuk, amit az Akadémiának kellene viselnie, viszont azt a támogatást nem kaptuk meg, amit az Akadémiák kapnak. Ezek a felelősségek nem magáncég-típusúak, a világon egyedülálló, hogy ezt egy magáncég vállalja, és hogy a mai napig is, 12 év után sem változott meg a helyzet. A magyar nyelv ügye – a számítógépek kapcsán – kicsúszott az Akadémia kezéből.

Külföldön mennyire ismertek azok az eredmények, melyeket idehaza már bevezettek?

Külföldön nagy szerencsénk van, mert nem adtuk fel a tudományos tevékenységet, így elért eredményeinkről konferenciákon tájékoztatjuk a világot. Ezeket el lehet mondani időről-időre, és elég sok helyen. Ismernek is minket. A tudományos háttértől egy üzleti vállalkozás nem feltétlenül jobb, csak jó érzés, hogy tudományos hátterünk van.

Európában nagyon figyelnek arra, hogy kiknek vannak olyan megoldásai, amelyek több nyelvre használhatók. Szerencsénk, hogy a lengyel, cseh, román stb. megoldásaink rendelkezésre állnak, és persze tudunk fordítani angol, német, spanyol stb. nyelvekre is. Nyugaton megcsinálták a maguk nyelvére, és mivel nekik már a szláv is bonyolult nyelv, – márpedig azt sokan beszélik a most csatlakozók között –, így aztán hamar feltűntünk, és gyakran az érdeklődés középpontjába kerültünk.

Néhány évvel ezelőtt egy belga cég arra épített, hogy a nyelvtechnológia fontos lesz a jövőben. Azt mondták amit én, de ők olyan hangosan mondták, hogy abba a Microsoft-tól kezdve mindenki beszállt. Azokat akik ilyen tevékenységet végeztek, azt bekebelezték. Addig növeltek a céget, míg az fel nem robbant. Egyrészt üzletileg, másrészt etikailag és jogilag. Azóta az egész vezetőség ott van, ahol más nem szeretne lenni. Ez azért volt érdekes, mert rengeteg konkurensünket ették meg menet közben, így azok megszűntek. Ez olyan, mint mikor a nagy hal a kis halak közé kerül, és minden, ami a szája elé kerül, azt felfalja. Ezután a nagy cégek vásárolták fel a darabjait, tehát kevés része maradt önálló. Mindig újabb és újabb kis cégek indulnak el, de a nyelvtechnológia témában többnyelvű alig van. Még ha lett volna, akkor sem élnek meg 12 évet, mert egy nagy megvásárolja őket.

Még gmk korunkban kötöttünk szerződést a Microsoft-tal, ők ellenőrizték az eszközöket, megfelelő volt, megegyeztünk. Eléggé kicsi a piac ahhoz, hogy könnyen találjon egy cég nemzetközi partnereket, akik felkarolják. Világszerte ismertek vagyunk és igyekszünk is rájátszani erre. Például konferenciákat szponzorálunk, ahol a cég neve előkerül. Most utoljára november végén volt Londonban a „Translating and the Computer” című konferenciának a 25. éves évfordulója. Ezt azért támogattuk, mert egyrészt a jubileumra ők is jobban odafigyeltek, másrészt az EU-csatlakozás előtt lényeges elem, hogy ebből a régióból ilyen technológiával ki rendelkezik. Kell a tudományos háttér, személyes vagy céges kapcsolat is, de ilyenfajta akciókra is szükség van. Kétféle termékünk van, az egyik, amit eladunk a hazai és a régió piacán a végfelhasználóknak –, ez az, amit dobozban lehet látni. A másik a technológia, amit eladunk a Microsoft-nak, Lotus-nak, és ők beépítik. A nemzetközi piacon dobozaink nem találhatók meg, mert ott csak a technológia él. Büszkék vagyunk arra a „hu”-ra a Morphologic végén, de az idők folyamán sikerült megvennünk a „com”-ot is mely korábban valami amerikai hardware cég tulajdona volt.

Szeretném kérni, hogy néhány mondatban vázolja, mit tervez a következő 2, 5 és 10 évre? Talán mindenki számára tanulságos, ha csatlakozhat valamilyen módon az ötletgazdag elmék közeli, vagy távoli jövőben várható elképzeléseihez...

Nincs olyan aki helyesen tudna jósolni. Meg tudta valaki jósolni 1989-ben, hogy ez lesz 1994-ben az Internet? Hogy mit tervezek csinálni, azt nem tudom, –

nem szeretném, ha a 2, 5 és a 10 év között az tenne különbséget, hogy valamit máshogy kellene csinálni. Minden a szövegben van, a szöveg meg a nyelvben és ezzel kapcsolatban nekünk reggeltől estig lesz feladatunk. Ha valamit rosszul csinálunk és a Morphologicnak egyszer majd rosszul áll a szénája, akkor az a mi hibánk lesz.

A világ nekünk dolgozik, akkor is, ha mindenfajta recesszióról beszélünk, mert a szövegekkel valamit kezdeni kell, és amióta ez a riport megy, azóta is Gigabájtok születtek az interneten. Olyan mennyiségű az adat, hogy már csak ideig-óráig működik az, hogy mikor egy keresőeszköz visszahoz 20 ezer találatot, megnézzem az elsőt meg a harmadikat meg még egyet, a többit pedig elfelejtem. A dolog egyik fele, hogy túl sok találat van, de valójában nem jól van megfogalmazva a feladat. Feladatunk a jövőben az, hogy, megtaláltassuk az emberekkel azt, amit keresnek, tehát olyan tartalmat tálalni, amire gondoltak, nem pedig olyat, amit leírtak. Nehéz megmondani, hogy mi lesz az eszköz, de az biztos, hogy ebbe az irányba kell menni.

Vannak megoldásaink a fordításnak újabb elven való megvalósítására, ami 2004-ben – legalább az angol és a magyar között – mint eszköz, az első változatban megjelenik a piacon is.

Jó látni, hogy a világ nagy nyelveinek, európai része 80-90%-os lefedettségű az Interneten, tehát azoknak már mindenféle eszközük megvan angolra, vagy franciára. Most ebben a kiegyensúlyozott világban a kínai meg a japán a második és a harmadik legtöbb weboldal, de még csak 20%-kal vannak benne, a többiek még csak ezután jönnek.

A kínai nyelv nem egy, mert nyelvjárások vannak, de egy írásuk van és az Interneten az írás a döntő. Ez több mint egymilliárdos piac, s nyilvánvalóan ehhez eszközök is kellenek. A maláj, a filippínó és a hasonló nyelvekre, szintén kell figyelni és ezek komplex nyelvek az angolhoz viszonyítva. Technológiánk sokkal jobb, mintha az angolból írtam volna át. Ha ügyesen csináljuk a dolgainkat, akkor a következő években azt kell általánosítani, amit már létrehoztunk, azaz a keresés és a fordítás irányába elmozdulni.

A jelenlegi helyzetben van mobiltelefonunk meg e-mail-ünk, – ez a kettő az, ami ellen minden üzletember védekezett. Az üzletembernek azért van titkárnője, hogy hagyják őt békén, majd a titkárnő felbontja a levelet, elolvassa, kidobja, lefordítja, megválaszolja, aláíratja, mindent megcsinál, és csak minimalizálja azt, ami végül is eljut a fontos emberhez. Az e-mail bebújik és az asztalomra kerül, a mobiltelefon akkor is csöng, amikor nem akarom, vagy kikapcsolom, de akkor üzenetek vannak. Pedig hát nyilván azért találtuk ezeket is ki, mert sokkal hatékonyabbak, mint ami eddig volt. Mindenképpen jobb lenne, ha rendszerben benne volna a titkárnő. Ez például egy jó feladat a nyelvi technológiának, hogy mind a mobiltelefonba, mind a számítógépen az e-mail fogadása során a hívásokat megválaszoló, rendszerező, lefordító eszköz előzné meg az emberi beavatkozást. Ez mind-mind a XXI. század technológiájára vár.

Magam is látom a napi 100-200 levelemmel, hogy ezzel nem lehet lépést tartani. Kell egy előfeldolgozóválogató program. Együtt kell működnöm egy olyan kis technikai izével, ami ott ül bent szoftverként, és segíti a munkámat. Nem helyettem dönt, csak könnyíti a döntéseimet. Azt gondolom, hogy ötlet is és lehetőség is van előttünk bőven.

Mit vár a májusi EU-csatlakozástól?

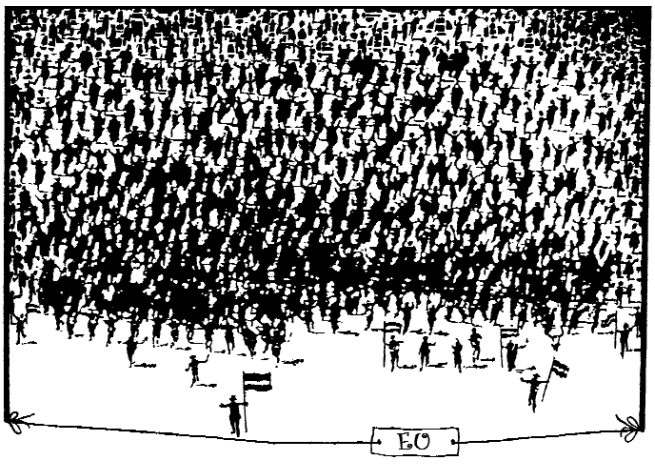
Az eddigi tapasztalatunk az Unióról az, hogy nagyon szigorúak a szabályok. Ha egy jó megoldás az Unión kívülről érkezik, csak azért mert kívülről jött, nem nyer bebocsátást. Ez nincs leírva sehol, de így van. Rendkívül bonyolulttá tették a külső eszközök, technológiák behozatalát. Az Unióban sok profi cég van, bár relatíve a mi témánkban kevesebb.

Jelenleg 11x10 nyelvpár vár az Európai Unióban az egységes fordításra, de májustól újabb 270 új pár kerül közéjük. A 20 nyelv esetén 20x19 = 380 a különbség, vagyis 270 új viszonylat jelenik meg. Tudjuk, hogy ezek nem egyforma súlyúak és nem minden megy direktben, mert sokszor van egy közvetítő nyelv, de a feladat még így is megháromszorozódik.

Azt várom az EU-tól, hogy nem egyik napról a másikra, de idővel megváltozik. Tudomásul kell venni, hogy mi is belül vagyunk. Senki sem gondolja, hogy mi leszünk az Unió közepe, de egy idő után már tudni fogják, hogy ránk számíthatnak. Mert mégiscsak belül vagyunk. Ez az, amit nagyon nehéz megfogalmazni politikailag korrekt módon. Szükség lenne arra, hogy valaki a tényleges értékénél kezdje minősíteni a dolgokat.

Több olyan tenderben vettünk részt Európai Uniós cégekkel, ahol meg volt adva 100 szempont. Valamennyi szempontnál pozitív választ tudtunk adni, és a kiértékeléskor kiderült, hogy ez a legjobb. Mégsem minket választottak. Tehát ha kiskorunkban egy olyan világban éltünk, ahol természetes volt, hogy más szempontok is vannak, mint az a száz, amit felsoroltak, akkor azt kell mondani, hogy az EU-nál is van ilyen. Miért lehet az, hogy valaki nem a legjobbat választja, hanem valami miatt egy másikat?

Azt várom az Uniótól, hogy ez a határ megszűnjön. Nem egyik napról a másikra, de lépésről-lépésre több érv lesz arra, hogy mi belül vagyunk és nem kívül.



INFORMATION TRANSFER BETWEEN POINTS WITH RELATIVELY HIGH SPEED

theory of relativity, Doppler-effect and reflection

In space research and astronautics information transfer between points moving with high speed may cause problems. This article covers two of these potential problems: change of the received frequency due to Doppler effect and change of plate mirror reflection in the function of direction and speed of moving.

EFFECTS OF TROPOSPHERIC SCINTILLATION ON SATELLITE COMMUNICATIONS

attenuation, fading, short-term changes, turbulence

The proposed future satellite data communications services require great bandwidth and excellent usability. The improvement possibilities of transmission parameters are limited mainly by characteristics of the satellite radio channel, especially the attenuation which is highly variable in space and time. The most intensively changing component of this variation is tropospheric scintillation. The paper outlines the effects of this parameters as well as the methods of its prediction and possible ways of protection against it.

UNIFORM TELECOMMUNICATIONS ON NETWORKS WITH DIFFERENT INFRASTRUCTURES

SIP, ENUM, network routing, mobile network

Widely used and popular services of the Internet are appearing in the world of mobile and wireline telecommunications as well. One of them is SIP allowing for users to establish any type of communications connection simply by giving his/her identifier regardless of the actual location of the called person. This service, however, cannot reach the critical mass until it can be reached in a uniform way on different networks.

LET'S TURN TO ENUM!

Addressing, service co-operation, privacy

Voice services on fixed, mobile or IP networks, then e-mail, SMS, MMS, fax, etc. can be considered as access points of a user. However, different access points should often be referred to in different ways. This means that the addressing of electronic mails and SMS messages are different. The use of ENUM can not only solve this problem but also offer many new options. One can pose the question: if ENUM has such a broad field of application why isn't it used more widely?

ORTHOGONAL FREQUENCY-DIVISION MULTIPLE ACCESS

multicarrier modulation, fading proofness, interference proofness, WLAN

This paper deals with orthogonal frequency-division multiple access (OFDM), one of the most important transmission and modulation techniques in the access lines of wireline, wireless and mobile telecommunications as well as of digital broadcasting. OFDM belongs to multicarrier modulation techniques. It can be very useful in several applications, particularly in cases where noise protection and the easy, rapid and economical installation is a major issue.

EFFICIENCY OF ROUTING PROTOCOLS

delay, bandwidth, graph, Nash-equilibrum

Issues of routing are highly focused in today's telecommunications community. New, more and more intelligent systems support the use of several alternative paths for transferring the traffic simultaneously. In this way these networks form a multiple access topology where finding the optimum routing is an important issue. Similar problems are faced both in fixed and mobile networks. The question to be answered is if there is any optimum solution, and if yes, is it clear?

BASICS OF THE CONDITIONAL ACCESS DVB CATV PROGRAMME DISTRIBUTION

interactive pay-tv, cryptography, encoding

The provision and distribution of mainly conditional access content as well as the service provider to user type electronic and information technology infrastructure of the related business models cannot be implemented but with their integration into the system of the digital broadcasting. The development of digital technology has resulted in the expansion of the offered programmes and paved the way for the technical background of the introduction of interactive television. However, these developments raise the question of additional information services. The paper explains the technological solutions of pay-tv services integrated into wireline DVB.

DISASTER RECOVERY AND BUSINESS CONTINUITY IN INFORMATION TECHNOLOGY

risks, availability, business continuity plan (BCP), cost-effectiveness

Along with the increasing role of IT systems, the emphasis is shifting from traditional IT-centric Disaster Recovery to the more comprehensive Business Continuity, this latter focusing more and more on the continuous provision of business-critical processes. The planning of BC/DR processes which are best fit to business requirements but require a possible low financial burden as well as the planning of the underlying information technology infrastructure is a complex challenge which should be based on the analysis of effects the applications have on business processes.

ELECTRONIC VOTING – A LONG WAY FROM THE END OF THE ROUTE

security, accountability, ease of use, risk

One can often hear news like "Electronic voting was held in country A" or "Residents of municipality B could vote on-line in course of the municipal elections". Different technological solutions and different experiences everywhere. There are ardent advocates and full-blooded opponents. This article sums up the principles of e-voting then recites arguments pro and contra.

Contents

THE NEAR FUTURE OF TELECOMMUNICATIONS 1

SPECIAL ISSUES OF WAVE PROPAGATION

Dr. János Csernoch
Information transfer between points with relatively high speed 2

Péter Bakki
Effects of tropospheric scintillation on satellite communications 7

UNIFICATION OF ADDRESSING TECHNIQUES

Tibor Erdélyi
Uniform telecommunications on networks with different infrastructures 13

Balázs Gódor
Let's turn to ENUM! 17

BROADBAND ACCESS AND ITS DESIGN METHODS

Dr. Árpád Dárdai
Orthogonal frequency-division multiple access 22

Gábor Kuruc, Krisztina Lója
Efficiency of routing protocols 29

Tibor Wein
Basics of the conditional access DVB CATV programme distribution 35

SECURITY AND AVAILABILITY

György Lajtha
Installation of a Xyscom system in Bárdudvarnok (Hungary) 46

Géza Godányi
Disaster Recovery and Business Continuity in information technology 47

Tamás Borovitz
Electronic voting – a long way from the end of the route 53

Book review: Information, society, history 58

László Sipos
Building future based on past experiences 59

Beatrix Havaska Nagy
Interview with dr. Gábor Prószéky, founder of MorphoLogic Co. 60

Cover: With the use of Maxwell's theory any information can be accessed at any point of the world

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

Cikkek eljuttathatók az alábbi címre is
BME Szélessávú Hírközlő Rendszerek
Budapest XI., Goldmann Gy. tér 3.
Tel.: 463-1559, Fax: 463-3289,
e-mail: zombory@mht.bme.hu

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

2004-es előfizetési díjak
Hazai közületi előfizetők részére:
1 évre bruttó 31.200 Ft
Hazai egyéni előfizetők részére:
1 évre bruttó 7.000 Ft

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

www.hte.hu
Felelős kiadó: MÁTÉ MÁRIA
Lapmenedzser: Dankó András

HU ISSN 0018-2028

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