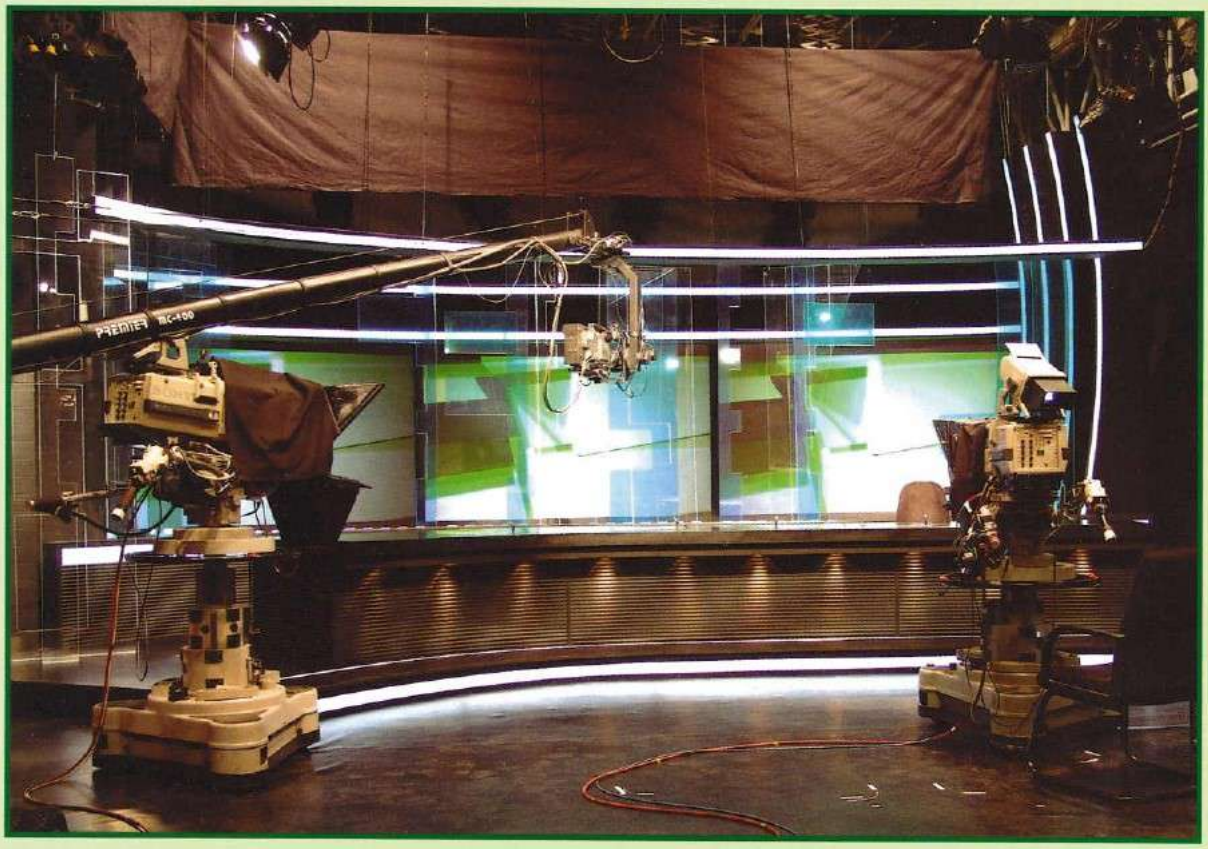
híradástechnika

1945 VOLUME LX. 2005

hírközlés ▪ informatika



Digitális műsorszórás

E-közigazgatás

Hálózatok változása, biztonsága

2005/3

A Hírközlési és Informatikai Tudományos Egyesület folyóirata
a Nemzeti Hírközlési és Informatikai Tanács együttműködésével

Tartalom

Címlap: A jó és rossz műsorok egyaránt ilyen modern stúdiókban készülnek.

Szokások rabságában

lajtha.gyorgy@ln.matav.hu

Az új eszközöket, módszereket az emberek többsége nehezen fogadja be. Ez a konzervativizmus nem kötődik sem országhoz, sem népfajokhoz, mindenütt egyaránt megtaláljuk. Az irodalomban sok esetben ez az események egyik forráspontja. Sok országban a szokások hatását közmondások is közvetítik. A német nyelvterületen általánosan használatos elítélő megfogalmazás: „Der Mensch ist ein gewohnheits Tier", vagyis az ember szokásokkal rendelkező állat. Ennél kedvezőbb az angolok idevonatkozó szóhasználata: „Works why to change it –, vagyis rögtön mentséget is adnak az embereknek, mondván, hogy a működőt minek változtatni. Végül még a rómaiaktól származó anekdota, hogy amikor Phitagoras feltalálta a róla elnevezett tételt, 50 ökröt áldozott az isteneknek és azóta fél minden ökör az újtól. Ez talán túlságosan is elítélő, de a rómaiak valószínűleg igyekeztek minden rendelkezésre álló újdonságot hasznosítani.

Ezek a gondolatok a márciusi szám összeállítása kapcsán merültek fel. Az első blokkban a digitális műsorszórás kérdéseit vizsgálja egyik szerzőnk, és ebből is kiderül, hogy az, a frekvenciagazdálkodás, minőség és adóteljesítmény szempontjából egyaránt felülmúlja az analóg megoldást. Ezt a cikket – szokásunktól eltérően – egy hírblokk követi, hogy lássuk milyen lassan halad Európa szerte az áttérés az analógról a digitálisra. Műszakilag évek óta rendelkezésre áll a megoldás, a nemzetközi testületek kidolgozták a minden ország számára elfogadható frekvencia-rasztert, mégis a rendszer lassan terjed és 5-10 éves távlatra becsülik, amikor általános lesz az új megoldás.

Akik mentegetni akarják az áttérés lassúságát, szociális kérdéseket vetnek fel. A digitális rendszerekhez új rádióvevőt és tévékészüléket kell venni. Esetleg elegendő mind a két esetben egy egyszerű adapter alkalmazása, melyek ára minden országban várhatóan a minimálbér negyede és tizede között lesz. Ezek az összegek a társadalom nagyobb része számára nem szabad, hogy gátat szabjanak az újdonság bevezetésének, hiszen a minimálbérek tízszeresét meghaladó gépkocsi vásárlásra 4-8 évenként a családok 60-70%-a tud gazdasági hátteret teremteni. Ha pedig a lakásvásárlásokra gondolunk, akkor a több millió forintos beruházásokra bankkölcsönök, vagy állami támogatások kínálnak segítséget.

Felmerül a kérdés, miért félünk akkor ettől az újtól? A kísérleti adások megindultak, de nem igyekszik senki olyan eszközöket terjeszteni és árusítani, melyekkel mind több ember véleményét megtudhatjuk a digitális műsorszórás minőségéről. Talán ez a blokk is segít a konzervatív gyártók, szolgáltatók és felhasználók nézeteinek módosításában.

Hasonló a probléma a második blokkban tárgyalt e-közigazgatással, e-kormányzattal kapcsolatban. Ez is előnyösnek látszik és kevéssé terjed. Az eszközök itt is rendelkezésre állnak. Ebben az esetben talán az is erősíti a konzervatív nézeteket, hogy kellő tudás és tapasztalat hiányában az emberek félnek, hogy a hatósággal tartott elektronikus kapcsolat számukra többletkiadást, vagy többletfáradtságot fog jelenteni és nem látják elég megbízhatónak. Az itt megjelenő két cikk egyik célja, hogy bemutassa: nincsenek különösebb veszélyek az elektronika felhasználásában, a lakosság és a hatóság közötti kapcsolatban.

Ezen a téren lapunk csak a szakmai háttérrel foglalkozik, mert ennek a propagálásában nagyon sok társunk van. A minisztériumok, a tudományos egyesületek és a különböző oktatási intézmények egyaránt megtesznek mindent annak érdekében, hogy meggyorsítsák az alkalmazást. A barátságos internet sok összefüggésben elterjedt az országban. Ennek ellenére még sokan úgy tekintenek erre az újdonságra, mint egy ellenségre...

A további két cikk is egy-egy újdonságot mutat be a távközlő hálózatok kiépítése és biztonsága területén. Az utóbbi úgy kapcsolódik az elektronikus közigazgatáshoz, hogy egyszerű eszközökkel igyekszik az adatvédelmet biztosítani.

Tudjuk, hogy egy kis példányszámban megjelenő szakmai folyóirat nem fogja a világot megváltani. Vigaszunk talán csak az lehet, hogy a több milliós példányszámban angol és spanyol nyelven megjelenő napilapoknak sem sikerült átütő eredményeket elérni egy-egy újdonság bevezetése területén, de ugyanakkor talán az is számít, hogy hányan és hányszor mondják el ugyanazt.

dr. Lajtha György

Mozaik,
avagy egy újsághír anatómiája

DR. BŐGEL GYÖRGY

KFKI Számítástechnikai Rt., CEU Business School, Debreceni Egyetem
gybogel@kfki.com

Az IBM 2004. decemberében eladta PC üzletágát a kínai Lenovónak. Ez a hír többféleképpen is értékelhető. Egyrészt érdekes állomás a személyi számítógépek iparának fejlődéstörténetében. Másrészt elemezhető a neves amerikai cég stratégiájának egy aktuális lépéseként is. Harmadrészt megvizsgálhatjuk, miként illik bele ez az esemény a nemzetközi munkamegosztásról kialakult képünkbe.

Bevezetés: a hír

2004. december 7-én az IBM bejelentette, hogy 1,75 milliárd dollárért eladja *PC üzletágát* a kínai Lenovónak. A már ezt megelőzően is óriásnak számító, hárommilliárdos forgalmat felmutató távol-keleti cég a felvásárolt részleg évi kilenc milliárdjával kiegészülve a személyi számítógép iparban a harmadik helyre kerül a Dell és a Hewlett-Packard mögött, tiszteletet parancsoló 8,6%-os piaci részesedéssel, globális jelenléttel. Az IBM a Lenovo stratégiai partnereként és 18,9%-os résztulajdonosaként pedig arra számít, hogy közelebb kerülhet a gyorsan fejlődő ázsiai ország hatalmas informatikai piacához.

A Lenovo Pekingből az amerikai Armonkba helyezi át a székhelyét, vezérigazgatónak pedig az IBM-es Stephen M. Wardot nevezi ki. Az új gazda még öt éven át használhatja az IBM logót és örök időkre megtarthatja a „Think" márkanevet.

Ez a hír önmagában is érdekes, mondhatni pikáns.

Hogy mást ne mondjunk, a kínai cég állami kontroll alatt áll, helyi vezetője, Yang Yuanquing a kommunista párt tagja. Új íróasztala az USA-ban lesz. Vajon hogyan fog viselkedni, mondjuk, egy radikális létszámcsökkentési döntés meghozatalánál? A felvásárlási ügylethez nyilván meg kellett szerezni a legfelsőbb kormányzati és pártvezetők egyetértését. Hogyan érvényesül majd az állami és pártellenőrzés a tengeren túl? A másik oldalon az IBM az amerikai kapitalizmus, a szabad piacgazdaság zászlóshajója, emblematikus képviselője, az IBM PC pedig az informatikai világban tölt be hasonló szerepet. Kínaiak az IBM-ben, IBM-esek Kínában, Kínának eladott PC üzletág – a két világ ilyen formában való közeledésének kétségtelenül van valami diszkrét bája.

Tudjuk jól, hogy a két ország kereskedelmi forgalma dinamikusan növekszik, hogy kínai vállalatok tartanak Amerikába és viszont. Az amerikai cégeket lázba hozzák az egyre jobban megnyíló kínai piac hatalmas méretei, a külföldi terjeszkedés pedig a pekingi vezetés dédelgetett vágya, grandiózus víziója. A hasonló események tengerében egy ilyen hírre mégis felkapja a fejét az ember és arra gondol: talán a következő a Coca-Cola lesz?!

Az IBM számára a kiváló helyi kapcsolatokkal rendelkező Lenovo kaput nyithat a fontos kínai kormányzati és oktatási piacok felé. Egyébként pedig, a Nagy Kék állítása szerint, a PC üzletág milliárdos veszteséget halmozott fel az utóbbi években, tehát épp ideje volt csinálni valamit, a kínai cég vásárlási hajlandósága tehát kapóra jött. 1,75 milliárd dollár sok pénz, be lehet fektetni a megmaradt üzletágakba, tőkére szomjas nagyszabású fejlesztési programokba.

Stratégiai lépésekre a Lenovónak is szüksége van. Helyi beágyazottsága ellenére a helyzete nem biztonságos, hiszen a kínai belső piacon egyre élesebb a verseny. Az év elején 27% körüli hazai piaci részesedéssel rendelkezett, ami nem kevés, de éhes és a lovagiasság szabályaival nem sokat törődő versenytársai nagyokat akarnak harapni belőle. Veszélyeztetettsége meglátszik a részvényei árfolyamán is, ami 23%-ot esett 2004-ben. Stratégiai helyzetjavító lépéseket már korábban is tett, így például megtisztította a profilját és új piaci fókuszt keresett a hazai városi lakosság körében. Az IBM-es ügylet segítségével kiemelkedhet a versenymezőnyből, hiszen, mint már jeleztük, a Dell és a HP mögött a harmadik lehet a világranglistán, ami igazán nem hangzik rosszul.

A házasság jövőjét illetően azonban nem árt óvatosnak lenni. Tapasztalatból és statisztikákból tudjuk, hogy a *felvásárlások* és *összeolvadások* fölöttébb kockázatos lépések. A siker sokszor nem a közvetlen üzleti és stratégiai logikán múlik, hanem lágyabb tényezőkön, például a kultúrák közötti különbségeken, a kulcsemberek viselkedésén. A Daimler-Chrysler egyesülés példájából is tudjuk, hogy amerikai és német vezetők sem jönnek ki mindig jól egymással. Vajon mi a helyzet egy amerikai-kínai kapcsolat esetében?

Maradjuk azonban a pénznél. Egy felvásárlás óhatatlanul felmerülő költségeit akkor lehet ellensúlyozni, ha az összekapcsolással sikerül nyereségtartalékokat mozgósítani, vagyis a költségeket csökkenteni és a bevételeket növelni. De a piaci részesedés növelése mellett hol vannak a további nagy stratégiai lehetőségek? Az olyan piacelemzők, mint például a Gartner Group, nem jósolnak nagy jövőt a PC üzletből származó bevételeknek, 2007-re például halovány 2%-os növekedést

jövendölnek. A gyártási tevékenységeket az IBM már régen Kínába és más olcsó országokba telepítette át. Talán a Lenovo racionalizálni fogja a frissen felvásárolt üzletág tevékenységét? Vagy éppen ő fog tanulni az amerikaiaktól? Vajon hány tolmács kell majd az intenzív szakmai kommunikációhoz?

Egy biztos, a két cég illetékesei nem fognak unatkozni. És nem fognak unatkozni azok sem, akik az esemény iránt nem közvetlen üzleti céllal érdeklődnek. Sok egyetemi tanszéken már nyilván hegyezik a tollukat azok, akik az ügyletről esettanulmányt akarnak írni. Az üzleti iskolák osztálytermeiben pedig kedvelt és forró téma lesz a legendás IBM PC üzletág eladása, a nagy hármas (Dell, HP, Lenovo-IBM) gigászi küzdelme a slágerlista élén.

Elemzői, újságírói vagy oktatói szemszögből az esemény fényes és szépen csillog, érdemes érte lehajolni, felvenni, alaposabban megnézni. Egy szép színű kövecske önmagában is érdekes lehet, de be lehet helyezni egy nagyobb képet adó *mozaikba* is. Hatása itt már azon is múlik, hogy milyen környezetbe kerül, milyen más kövek vannak közvetlenül mellette és tőle távolabb, mi a szerepe a teljes képben. Egy újsághír vagy egy üzleti esemény is akkor válik igazán érdekessé, ha *kontextusba* helyezzük, vagyis olyan képeket keresünk, amelyekbe beleillik, amelyekben logika van, azaz többek események egyszerű halmazánál.

Az IBM-Lenovo ügyletnek vannak távolba visszanyúló előzményei, várható hosszútávú következményei, és vannak vele párhuzamosan futó, vele összefüggő, trendeket alkotó más események. Aligha véletlen, hogy éppen most, a 21. század elején hozták tető alá. A teljesség igénye nélkül próbáljunk meg olyan mozaikokat, nagyobb képeket keresni, ahová ez a kő beilleszthető.

Mi lesz veled, PC?

Az első kép legyen horizontális, olyan, amin események egymást követő sorozatát lehet megörökíteni, valahogy úgy, mint egy képregényben. Mert regényről van szó, a személyi számítógép regényéről. Az IBM-Lenovo házasság a legfrissebb folytatás végén áll, a kép viszont nincs befejezve, szemlátomást további folytatások jönnek. Ez az esemény lezárása egy történetnek, és egyszersmind kezdete egy újnak.

Menjünk most a kép elejére. Ott láthatjuk Bill Lowe-ot, az IBM egyik, kis méretű és olcsó számítógépekkel kísérletező fejlesztési laboratóriumának vezetőjét. Éppen beszámolót tart a vezetőségnek. A falon lévő naptár 1980-at mutat. Lowe-nak két fontos mondanivalója van: 1) a kicsi és olcsó gépek piacán kedvező lehetőségek nyílnak a cég számára; 2) ezek kihasználásához ki kell lépni az IBM hagyományos kultúrájából. A vezetés zöldre állítja a lámpát, a fejlesztők pedig rövidesen megjelennek a prototípussal. Megszületik az IBM PC.

De hol itt az új kultúra? Az IBM mindezidáig vertikális piacban gondolkodott, ahol egy-egy gyártó mindent maga állít elő a chipektől kezdve a szoftverekig. Lowe emberei azonban az új gépet mások által gyártott alkatrészekből rakták össze mondván, hogy így sokkal gyorsabban lehet piacra jutni. Emellett a PC architektúrája is nyitott volt, vagyis más cégek is hozzáilleszthették a perifériáikat, futtathatták rajta a szoftvereiket. Ráadásul Lowe azt javasolta, hogy az értékesítést kiskereskedelmi boltok útján oldják meg, vagyis kerüljék ki a hagyományos IBM-imázshoz tartozó marketinges, értékesítő és szolgáltató szervezeteket.

Elképzelései ismét zöld utat kaptak. A PC-vel foglalkozó embereket az IBM önálló üzletágba szervezte, kiemelte a nehézkes cégbürokráciából és jól teletömte pénzzel. A csapat villámgyorsan kialakította a beszállítói hálózatát. Mivel a szoros határidő miatt kerülni igyekeztek a meglepetéseket, és az IBM nagygépeivel sem akartak konkurálni, egy ötéves Intel processzor mellett döntöttek. Az oprációs rendszerre a Microsoft kapott megbízást, a meghajtóra a Tandon, az áramköri lapokra az SCI, a printerekre az EPSON, az áramelláto rendszerre a Zenith. Az elosztási megbízást a ComputerLand és a Sears nyerte el.

Láthatjuk, hogy az IBM-es PC-program kezdettől fogva üzleti vállalkozás volt. Azt is érzékelhetjük, hogy az új gép eleve *tömegcikknek* készült. Tömegcikket csinálni tömegesen kapható alkatrészekből, tömegeknek, olcsón és hatékonyan – a gép további sorsát ez a filozófia határozta meg, és ennek a sorsnak szimbolikus állomása a Lenovóval kötött házasság.

Az elmúlt negyedszázadban a PC a tömegtermékek tipikus fejlődési pályáját futotta be. Rövidesen megjelentek a konkurensek, kialakult a vezetőkből, támadókból, másolókból és rés-stratégiát követőkből álló klasszikus piaci szerkezet. A mérnökök éjt nappallá téve dolgoztak, egymást követték az egyre okosabb hardver- és szoftvergenerációk. A PC a maga elemi alkalmazásaival megjelent mindenki asztalán. Használata egyre könnyebbé vált: a felhasználók hatással voltak a gépre, a gép pedig hatással volt a felhasználóira. Csekély túlzással a PC ugyanolyan szerves részévé vált a háztartásoknak, mint a hűtőszekrény vagy az autó.

A munkahelyeken lassan egy lépést sem lehet tenni nélküle. Húsz évvel ezelőtt a legtöbb vezető úgy tekintett a számítógépre, mint fejlettebb írógépekre vagy kalkulátorokra, amelyeken a titkárnőknek és könyvelőknek kell dolgozniuk. Ma egy olyan vezérigazgatói íróasztal, amin nincs legalább egy elegáns lapos monitor, meglehetősen furcsán hat. Azt az érzetet kelti, hogy a gazdája nem ura az eseményeknek, hiszen nem látja „valós időben és elektronikusan”, hogy mi történik körülötte, kimarad a kommunikációs láncból, a szervezet és a nagyvilág vérkeringéséből. Napjainkban egy ország fejlettségét egyebek között a számítógépek elterjedtségével, piaci penetrációjával mérjük; a politikusok előszeretettel dicsekednek a felfelé tartó görbékkel.

Azonban a technikai innovációk egymást követő megjelenése, a fontosság és az elterjedtség növekedése mellett a fejlődési pályának más jellemzői is vannak. Mint már jeleztük, az IBM PC tömegcikknek indult és az is maradt. Tudása és kapacitása mellett hasznosságát

a *kompatíbilitása* adja: a gépek, alkatrészeik és perifériáik szabadon cserélhetők és összeköthetők egymással. Ilyen gépeket akartak a felhasználók, ilyeneket adtak nekik a gyártók.

A kompatíbilitás, a cserélhetőség és az összekapcsolhatóság alapvető feltétele a *szabványosság*. Az IBM által a kompatíbilitás filozófiájával piacra vitt PC több okból is gyorsan szabványosodott. Először is a használatának könnyűnek kellett lennie, hiszen melyik vállalatnak van arra ideje és pénze, hogy minden új alkalmazottjának hosszadalmas képzést nyújtson a helyi gépek elemi felhasználási módjairól, és kinek van kedve minden gép- és szoftvercserénél napokig búnyi a felhasználói kézikönyvet. A technológiai piacok tipikus jelensége, hogy egy idő után már csak olyan vevőket lehet megnyerni, akik nem hajlandók vagy nem tudnak tanulni. Másodszor, tömegesen összekapcsolódni és kommunikálni csak szabványos rendszerek képesek. Harmadszor, ha tömegpiacok meghódítása a cél, a gépnek olcsónak kellett lennie, az alacsony költségekhez pedig a szabványokra épülő tömeg adja a kulcsot. Az internet megjelenése és terjedése csak erősítette ezeket a kényszereket.

A PC-t tömeges előállítása és szabványosítása tette olcsóvá. Ha konkrét számokról beszélünk, a piac alsó végén ma az 500 dolláros noteszgépnél tartunk, ami itthon sem több egyhavi minimálbérnél. A felhasználók csak nyertek: viszonylag kevés pénzért nagyon okos és hasznos eszközhöz juthatnak hozzá.

A termelőknél már nem ennyire egyértelmű a helyzet. A tömegcikkek piacán, ahol a termékeket nehéz egymástól megkülönböztetni, a legfontosabb versenytényező az ár. Tartósan árat csökkenteni az tud, aki a költségeit is le tudja szorítani. Nem véletlen, hogy a PC-piac mai, legnagyobb piaci részesedéssel bíró játékosa a Dell. Alapító-vezetője, Michael Dell szerint minden technológiai trend az olcsó szabványok felé mutat. Az elsők között ismerte fel, hogy a PC-k egymástól megkülönböztethetetlen „dobozokká” válnak. Vállalati folyamatait úgy építette fel, hogy képesek legyenek ezek gyors és olcsó előállítására és kiszállítására. Műszaki fejlesztésre jóval kevesebbet költ nagy versenytársainál.

A PC-piacon az *árak esése* mindennapos jelenség. A verseny lefelé nyomja a vállalati nyereséghányadokat, amire a tömeg növelése és további költségcsökkentés a válasz. A tömegcikkgyártás kipréseli a nyereséget az iparági ellátási lánc azon tagjaiból, akik leginkább ki vannak téve e hatásnak. A PC-piac ma a darabszámot tekintve növekszik, de az árak gyors csökkenése miatt a mennyiség legfeljebb minimális bevételnövekményt hoz. Nyertesek a fogyasztók lesznek és egyes szabadalmak birtokosai, az utóbbiak is csak addig, míg kizárólagos vagy kvázi-kizárólagos pozíciójukat meg tudják őrizni (lásd a Windows-Linux párharcot). Nem új jelenség ez, másutt is megfigyelték már.

E folyamat hatására az érett piacok *konszolidálódnak*, szereplőik olcsóbb forrásokat, olcsóbb előállítási helyeket keresnek. A konszolidáció felvásárlásokat és összeolvadásokat jelent, olcsóbb előállítási források pedig ma leginkább a Távol-Keleten találhatók. És ezzel valahol a hosszú mozaikkép jobb oldalán meg is érkeztünk a mi „kövecskénkhez”, az IBM-Lenovo ügylethez, ami szépen belesimul az itt felvázolt képbe: konszolidációs lépésről van szó, távol-keleti viszonylatban. Rengeteg hasonló történik szerte a világban, ennek különlegességét inkább az adja, hogy itt az IBM PC-ről van szó.

Arra is fel kell figyelnünk, hogy a PC (a rajta futó szoftvereket is beleértve) képességei egyre inkább meghaladják az átlagos fogyasztó igényeit. Ennek több tünete van: kapacitásai kihasználatlanok, az alkalmazásokba beépített funkciók számottevő részét a gazdáik nemhogy nem használják, de nem is ismerik. (Politikusaink, miközben a felfelé tartó elterjedtségi mutatókat elemzik, általában mélyen hallgatnak arról, hogy egy átlagos háztartásban a gépet és az internetet tulajdonképpen mire is használják.)

Születésekor a PC szakadásos innovációt jelentett a mainframe-gépek világában. Szakadásos innovációt, abban az értelemben, ahogy ezt a kifejezést a harvardos Clayton Christensen használja: olcsóbb, egyszerűbb terméket adott a piac alsó szegmense számára, – a technika az utóbbi évtizedekben gyorsabban fejlődik a felhasználóinál, és éppen ez a „túlérési” jelenség teremti meg a szakadásos innovációk lehetőségét. Ha igaz, a személyi számítógépek világában további szakadásos innovációkra számíthatunk – de ez már egy másik történet lehetne.

Felfelé a kazalban

Próbáljuk meg most egy másik mozaikképbe belehelyezni az IBM-es PC üzletág eladását. Alakját tekintve ez a kép magas legyen és egy kazlat ábrázoljon. Persze nem szénakazalra kell gondolni, hanem az informatikai termékek és szolgáltatások egymásra épülő rétegeire, amelyek együttesen kiadják egy tipikus informatikai környezet főbb elemeit.

A kazal legalján a kész hardvertermékek komponensei vannak: processzorok, tárolók, monitorok, memóriachipek, hálózati eszközök. Fölöttük találhatjuk az alapvető operációs és integrációs szoftvereket, még feljebb a különböző célokra (adminisztrációra, döntéstámogatásra, elektronikus kereskedelemre stb.) használható alkalmazásokat. A kazal legtetején szolgáltatások ülnek: informatikai tanácsadás, rendszerintegráció, kiszervezés, képzés, finanszírozás, karbantartás és ehhez hasonló dolgok.

Az előző kép ismertetésénél már elmondtuk, hogy az informatikai piac egy darabig *vertikális* szerkezetű volt: a cégek (köztük az IBM) a kazal minden elemével foglalkoztak. Egyik kazalból nem volt átjárás a másikba, mivel a termékek nem voltak kompatíbilisek egymással. A vevő fogságba esett: ha egyszer kiválasztotta a maga szállítóját, nem tudott tőle könnyen megszabadulni. Nem csoda, hogy menekülni igyekezett ebből a kiszolgáltatott pozícióból, és már csak ezért is lelkesen fogadták a minden irányba kompatíbilis PC gondolatát.

A személyi számítógép példája mutatja, hogyan vált a piac vertikálisból *horizontálissá,* hogyan vált lehetségessé, hogy egyes cégek a kazal egyes rétegeire, sőt, azon belül is egyes termékekre szakosodjanak és kihasználják a fókuszáló stratégiák előnyeit.

Az elérhető nyereség tekintetében nagy különbségek vannak a kazal egyes rétegei és elemei között *(táblázat)*. Bemutattuk, hogyan préseli össze a verseny a tömegcikkek gyártóinak és forgalmazóinak nyereséghányadát. A gyors tömegesedés leginkább a kazal alsóbb szintjein elhelyezkedő, egymástól alig megkülönböztethető, szabványosodó termékeket fenyegeti. Legkevésbé a szolgáltatások veszélyeztetettek: azokat rendszerint az ügyfél speciális helyzetéhez és igényeihez kell igazítani, nagy részük helyi és személyes jellegű, bizalomra és tudásra épül, azaz olyan tényezőkre, amiket nehéz lemásolni, szabványosítani.

Tevékenység	1995	2000	2005	Trend
Üzleti tanácsadás	10	13	17	▲
Szolgáltatás és szoftver	30	29	41	▲
Hardver: szerverek, tárolók	18	20	12	▼
Hardver: kliens gépek	13	9	6	▼
Technológia	29	29	24	▼

Tevékenységek részesedése az informatikai ipar nyereségéből (%) – Forrás: IBM, 2003.

Az informatikai ipar lendületes fejődése a kilencvenes években felgyorsította a szabványosodás és tömegcikkesedés folyamatát, a piac 2001. évi összeomlása pedig alaposan megtépázta a nyereségkimutatásokat. Nem csoda, hogy számos cég megpróbálta átpozícionálni magát a kazalban. Sokan a tetejét vették célba, mivel ott látták a legnagyobb nyereséget. A szándékokat jól mutatták a frissen készült prospektusok és honlapok, amelyek például arról igyekeztek meggyőzni a nagyközönséget, hogy az eddig hardverrel és szoftverrel foglalkozó cég mostantól „szolgáltató" és „megoldásszállító" lesz. Aki szándékosan vagy képességei miatt a kazal alján maradt, vagy kibékült csökkenő bevételével és nyereségével, a költségcsökkentés és racionalizálás állandó kínzó kényszerével, vagy olcsóbb forrásokat keresett, esetleg konszolidációba menekült.

Volt, akinek sikerült felmászni a kazal tetejére, és volt, akinek nem.

Az IBM-nek sikerült, egyebek között talán azért is, mert a többieknél korábban kezdett mászni. Jó oka volt erre: a kilencvenes évek elején a helyét sehogy se találó vállalat nagyon gyenge eredményeket produkált. Az újságok már arról cikkeztek, hogy az amúgy is kiskirályságokra bomlott céget jobb lenne szétszedni, több vállalatra bontani.

1993. áprilisában azonban Louis Gerstner vette kezébe a kormányrudat, aki némi hezitálás után úgy döntött, hogy a Nagy Kéknek egyben kell maradnia, viszont alaposan át kell alakítani a kínálatát. Az új vezető szerint az IBM nem lehet afféle ezermester, aki mindent megcsinál mindenkinek. Ha viszont választani kell, akkor a kazal csúcsát kell célba venni, és nem csak az IBM-ét, hanem másokét is, leginkább a UNIX- és Wintelpiacokét.

A legelső „véres" döntés az alkalmazás-szoftverekről való lemondás volt. Korábban az IBM alkalmazások százait készítette a legkülönbözőbb felhasználóknak. Ezek fontos szoftverek voltak fontos ügyfelek számára; a gond csak az volt, hogy a cég rengeteg pénzt veszített rajtuk. A piacot olyan cégek uralták, akik valamilyen speciális területre összpontosítottak, mint például az ügyfélkapcsolatok kezelése vagy a pénzügyi szolgáltatások. Ezek örömmel vették volna, ha az alkalmazásaikat IBM hardveren, IBM-es szolgáltatói támogatással futtathatják, de mivel a szoftverek miatt riválist láttak benne, inkább a SUN-nal vagy a HP-val kötöttek szövetséget.

A kilencvenes évek második felében Gerstner alaposan megrostálta a szoftverkínálatot, csak azokat hagyva meg, amelyekben az IBM a legeredményesebbnek bizonyult. A szakosodott alkalmazásgyártók felé így szólt az új üzenet: nektek hagyjuk ezt a piacot, riválisok helyett partner leszünk, együtt dolgozunk veletek, hogy a szoftvereitek simán fussanak a mi gépeinken, és támogatni fogunk benneteket a szolgáltatásainkkal. A vállalat vezetői két év alatt 180 partnerségi szerződést írtak alá.

A *szolgáltatások*, azaz a kazal teteje felé való mozgás fontos lépése volt 2002-ben a PriceWaterhouseCoopers tanácsadó cég megvásárlása, aminek eredményeként a cég tanácsadói-szolgáltatói állománya mintegy 30 ezer fővel gazdagodott. Könnyű dolguk mindenesetre nem volt, mivel az esemény éppen az amerikai recessziós időszakra esett. A visszaesés nem hagyta érintetlenül a tanácsadói ipart sem. Ráadásul miközben a kereslet meggyengült, a kazal tetején hirtelen nagy lett a tolongás, hiszen a szolgáltatást és a „megoldásszállítást" mások is a zászlajukra írták. Köztük vannak olyan régi motorosok is, mint az Accenture és a Hewlett-Packard, de frissek – így például egyes látványosan növekvő indiai cégek – is helyet kérnek már maguknak a boglya tetején.

Az üzlet két legfontosabb eleme, a szolgáltatás és a szoftver fejlesztése egyre inkább ehhez a koncepcióhoz kötődik. A Nagy Kék mai vezetője azzal a feladattal bízott meg egy fejlesztői csapatot, hogy dolgozzanak ki egy általános formális modellt a vállalatok stratégiája, működése és informatikai infrastruktúrája közötti kapcsolat megragadásához. A végső cél egy olyan modell felépítése, amely meg tudja mondani, hogy ha felül megváltoztatják a stratégiát, miként kell átalakítani az informatikai rendszereket odalent. Akinek ez sikerül, az megfogta az isten lábát.

E stratégiai lépéseknek komoly kockázata van. A profiltisztítás és a kazalban való kapaszkodás mindenesetre több éve tart már. Ebben a közegben hozták meg a döntést a PC üzletág eladásáról, ide kell behelyezni a mi mozaikkockánkat.

A korábbi vezető, Gerstner szerint az IBM tizenöt éven át alig nyert valami pénzt a PC üzletágon. A gépek

több tízmilliárd dolláros bevételt hoztak, a fejlesztők több kitüntetést is a mellükre tűzhettek, de ez nem változtatott a nyereségességen; még olyan időszakok is voltak, amikor a pénzügyesek örültek a forgalom visszaesésének, mivel így kevesebb volt a veszteség. Ráadásul az alapvető hardver- és szoftver-architektúrákat az Intel, illetve a Microsoft birtokolta. A forgalmazásban sohasem sikerült igazi vezetői pozíciót elérni és a termelési költségek is túlságosan magasak voltak.

A stratégiai logika azt kívánta, hogy a *szolgáltatói stratégia* és a nagyobb *nyereség* jegyében a gyorsan tömegcikkesedő terméktől meg kell szabadulni. A gyenge pénzügyi teljesítmény ellenére az IBM mégsem vált meg könnyen a PC-től. Az üzletág nagy bevételt hozott, a közvélemény pedig az asztalokon álló, mindenki szeme előtt lévő gépekkel azonosította a vállalatot, ahogy a mi Bábolnánkról mindenkinek a lovak jutnak az eszébe. A PC üzletágon belül azért volt mozgás, így például kiléptek a leginkább tömegcikkesedő szegmensekből és a Dell mintájára megkezdték az internetes és telefonos direkt értékesítést. A fejlesztésből és a gyártásból egyre többet adtak át másoknak.

Végül 2004. végén nyélbe ütötték a megállapodást a Lenovóval.

Változó nemzetközi munkamegosztás

Egy széles és egy magas kép után most egy minden irányban nagy kiterjedésű mozaik álljon itt harmadikként. Olyan, amire nagy ívű mozgásokat, távoli helyszíneket lehet felrajzolni. Ez legyen a legkevésbé befejezett. Valami olyasmit mutasson, ami a szemünk előtt formálódik, de még nem lehet tudni, mi is lesz belőle.

A kép egyik sarkában legyen ott a neves brit közgazdász, David Ricardo portréja. Egy másikban egy kínai mérnök egy IBM PC-vel. De hogyan kapcsoljuk össze őket és mi legyen még a képen?

Ricardo kimutatta, hogy az egymással kereskedő nemzetek akkor járnak a legjobban, ha nem abszolút, hanem a *komparatív előnyeik* alapján szakosodnak. A tétel minden valamire való közgazdaságtan tankönyvben benne van, a bor és a posztó klasszikus példájával illusztrálva. Anglia szakosodjon a posztóra, Portugália pedig a borra, még akkor is, ha Portugália egyébként mindkét terméket abszolút előnnyel állítja elő. A szakosodással mindenki jól jár, amint az matematikailag bizonyítható is.

Hosszú időn át ez az elgondolás uralta a kereskedelem elméletét. A nemzetközi munkamegosztásról, a globalizálódó gazdaságról pedig az a kép alakult ki, hogy a rutinjellegű termelési tevékenységek egyre nagyobb hányadát alacsony költségekkel dolgozó fejlődő országok veszik át, de ez nem baj, mert a fejletteknél ott maradnak a tudást igénylő tevékenységek, és azokban van az igazi haszon. Nem baj, ha a Nike vagy a Reebok sportcipőket valahol a Távol-Keleten gyártják, ha a fejlesztés, a tervezés, a design meg a marketing ott marad Nyugaton. A fejlődők gazdasága „termelésalapú”, a fejletteké pedig „tudásalapú” lesz. Az utóbbiak klubjába a „tudásgazdaság” különböző ágainak (például informatika, biotechnológia, kutatás-fejlesztés általában) fejlesztése adja a belépőt.

Ricardo egyszerű matematikai alapokon álló tétele minden bizonnyal ma is megállja a helyét. A nemzetközi munkamegosztás tekintetében azonban változni látszik a helyzet. Szándékosan beszélünk határozatlanul, mert hogy pontosan mi történik, és milyen irányba tartanak az események, még nem lehet tudni. A vészharangot mindenesetre olyan nagy emberek is megkongatták, mint a kilencvenedik életéve felé közeledő Nobeldíjas Paul A. Samuelson, aki a magyarul is több kiadásban megjelent híres közgazdaságtan tankönyvet írta.

Miről is van szó tulajdonképpen? Vegyük az IBM PC példáját. A hagyományos munkamegosztási képet egyáltalán nem zavarta, hogy az IBM gyártási tevékenységeit sorra más országokba helyezte ki. Most viszont a teljes üzletág eladásáról van szó. Erre már sokan felkapják a fejüket: hát akkor átengedjük a tudásigényes tevékenységeket is? Pont Kínának? Mi marad akkor nekünk? Mi is van akkor a „mi csináljuk a szellemi munkát, ti pedig működtetitek a gyárakat” filozófiával? Egyáltalán, hol vannak akkor a fejlett országok tartós előnyei, erősségei (a magunkfajta félig fejlettekről nem is beszélve)?

Nézzük a tényeket. Való igaz, hogy a közelmúltban figyelemre méltó változások mutatkoznak az álláshelyek nemzetközi áramlásában, tevékenységek más, olcsóbb országokba történő kihelyezésében. Az eddigi helyzetet a gyártási-fizikai tevékenységek kevésbé fejlett országokba történő vándorlása jellemezte. Ezt a mozgást a közlekedés fejlődése tette *lehetővé* és a verseny miatti állandó költségcsökkentési kényszer tette *szükségessé*. Ezek a globalizációs lépések a maguk idejében kiváltottak némi feszültséget: emlékezzünk például arra az esetre, amikor az Adidas, ez a hagyományos német családi vállalat úgy döntött, hogy a termelést elviszi a Távol-Keletre, a székhelyét átteszi Svájcba, és ráadásul egy francia vezetőt választ magának. Az effajta változásokhoz azonban szépen hozzászoktunk. Kirajzolódott a „global sourcing”, azaz globális forrásbiztosítási politikát érvényesítő vállalat, amely mindent onnan szerez be, ahol az a legolcsóbb: egyszerű kézi munkaerőt fejlődő országokból, kutatási, fejlesztési, menedzselési és egyéb igényes szellemi munkát pedig otthonról.

Ez a munkamegosztási világkép nem dőlt össze, de kétségtelenül repedések jelentek meg rajta. A lényeg: egyre több és egyre többfajta szellemi tevékenység, magas szintű tudást igénylő munkahely települ át olyan fejlődő országokba, mint például India és Kína. A legfontosabb mozgatórugó most is a verseny, ami költségeik csökkentésére, olcsóbb források igénybevételére kényszeríti a vállalatokat. A kényszer mellé az informatika és a távközlés fejődése teszi a megvalósítás lehetőségét. A modern technológiának köszönhetően a tudás szabadon áramlik szerte a világban, egy sor tevékenységnél pedig teljesen közömbössé válik végzésének földrajzi helye.

Gyakorlati példákkal tele vannak az újságok. Közismert az indiai informatikai ipar látványos felfutása és nemzetközivé, globálissá válása. Vállalataik megjelentek az amerikai tőzsdén, képviseleteik, kirendeltségeik, kereskedelmi és fejlesztő központjaik ott vannak a fejlett országok városaiban. Olyan multinacionális cégek, mint például a General Electric koncentrált szolgáltató központokat hoznak létre és olcsóbb országokba telepítik azokat. Vezető csúcstechnológiai vállalatok Kelet-Európában és Ázsiában nyitnak fejlesztő központokat. A biotechnológia térképére mások mellett Kuba is felkerült.

Említhetünk konkrétabb példákat is. A szerződéses gyártó Flextronics cég 41 ezer embert foglalkoztat Kínában. Csak Doumen városában 13 gyáruk van, ahol mobiltelefonoktól kezdve számítógépekig mindent gyártanak. A beszállítói lánc is helyi, amivel rengeteg költséget takarítanak meg. A vállalat ezrével viszi át az amerikai munkahelyeket az ázsiai országba.

Az amerikai 3Com nevű, távközlési berendezéseket gyártó cégnek 1200 mérnököt foglalkoztató közös vállalata van a kínai Huawei-jel. Új, a legfejlettebb technológiát képviselő adatkommunikációs központját nemcsak hogy Kínában gyártja, de ott is terveztette helyi mérnökökkel. Az amerikai fél szerint ez csak a kezdet. A Semiconductor Manufacturing International cég nemrég Peking mellett nyitott meg egy olyan gyárat, amelynek termékei szakértők szerint csak két generációval vannak lemaradva az Intel chipjei mögött, 2006-ig pedig még további négy gyártótelep megnyitását tervezik. Ezzel már valószínűleg olyan kritikus tömeget érnek el, amely átszívhatja a kutatás-fejlesztési kapacitások számottevő részét az Egyesült Államokból.

Mint mondtuk, harmadik, egyben utolsó mozaikképünk egyelőre befejezetlen, még az alaphangulata sem egységes. Az átalakuló nemzetközi munkamegosztás dimenzióiról és lehetséges következményeiről sokan vitatkoznak. A vészharangok kongatói a fejlett országok, leginkább az USA pozícióit féltik. A nagy tömegű, jól képzett, de egyben olcsó munkaerő megjelenése a világ szabadon kihasználható munkaerőbázisában gyengítheti a fejlett országok szakembereinek alkupozícióját, lefelé nyomhatja a bérüket, úgy, ahogy ez a kékgalléros munkakörökben is megtörténik. Egyes informatikai területeken ez a nyomás már igen határozottan érzékelhető.

A gyilkos verseny a szellemi, szakértői munkakörökben is megjelenik. Az olcsó keleti áruknak persze a fejlett országok lakosai is örülnek, de amit nyernek az árakon, elveszíthetik a béreken. Az állásukat elvesztő szakértők egyre nehezebben találnak hazájukban munkát. Egyes elemzők szerint a technológiai fejlődésnek köszönhetően értelmiségi állások milliói telepíthetők át a Föld másik oldalára, miközben Kína és India egyetemei milliószám ontják a diplomásokat. (Kínában a friss diplomások száma 2004-ben meghaladta a 2,5 millió főt.)

A nyugodtabb idegzetűek szerint azonban nem eszik olyan forrón a kását. Az elvándorlás ténye tagadhatatlan, de azért az állásokból sokan a helyükön maradnak. Elég ránéznünk a friss munkaügyi statisztikákra és láthatjuk, hogy a recesszióból ébredt amerikai gazdaság szép számmal generálja az új álláshelyeket, a szakértői és üzleti szolgáltatások szektora 2004-ben például több mint félmillióval bővült, és a bérek tekintetében sincs ok a pánikra. Különben is, a jövő tudásbázisú iparágaiban nemcsak a mozgékony tudás számít, hanem a pénz is, amiből a fejlett országoknak van több. Kína felemelkedésével hosszú távon a mostani fejlett országok is jól járnak, ahogy a japános exportőrök támadásába sem haltak bele annak idején.

Utolsó mozaikképünk üzenete, hangulata tehát többféleképpen alakulhat. Egy biztos: az IBM-Lenovo kövecske izgalmas, dinamikus környezetbe kerül.

Irodalom

[1] Ante, S.–Hof, R. (2004): Look Who's Going Offshore. Business Week, május 17., pp.84–85.
[2] Bőgel György (2004): Fehérgalléros kiszervezés – az offsore outsourcing jelensége, Competitio, december
[3] Cairncross, F. (1997): The Death of Distance. Orion Business Books, London
[4] Cairncross, F. (2002): The Company of the Future. Harvard Business School Press, Boston
[5] Carr, N. (2004): Does IT Matter? Harvard Business School Press, Boston
[6] Christensen, C. (1997): The Innovator's Dilemma. Harvard Business School Press, Boston
[7] Coase, R. (1990): The Firm, the Market, and the Law. University of Chicago Press
[8] Ewing, J. (2004): Is Siemens Still German? Business Week, május 17., pp.26–27.
[9] Halvey, J.–Melby, B. (1997): Information Technology Outsourcing Transactions. John Wiley & Sons, New York
[10] Hamm, S. (2004/a): Is Outsourcing ont the Oust? Business Week, október 4., p.39.
[11] Hamm, S. (2004/b): To the Tech Giants Go the Spoils. Business Week, november 29., p.32.
[12] Klepper, R.–Jones, W. (1998): Outsourcing Information Technology, Systems and Services. Prentice Hall, Upper Saddle River, New Jersey
[13] Lacity, M.–Hirscheim, R. (1995): Beyond the Information Systems Outsourcing Bandwagon. John Wiley & Sons, New York
[14] Malone, T. (2004): The Future of Work. Harvard Business School Press, Boston
[15] Matlack, C. et al. (2004): Job Exports: Europe's Turn. Business Week, április 19., pp.20–21.
[16] Robinson, M.–Kalakota, R. (2004): Offshore Outsourcing. Mivar Press, Inc. Alpharetta
[17] Schumpeter (1980): A gazdasági fejlődés elmélete. Közgazdasági és Jogi Könyvkiadó, Budapest
[18] The Economist (2004/a): A World of Work. November 13., pp.3–5. (melléklet)
[19] The Economist (2004/b): Out of Captivity. November 13., p.70.
[20] Zakaria, F. (2004): Rejecting the Next Bill Gates. Newsweek, november 29., p.21.

Az RRC04 elfogadott tervezési alapelvei a gyakorlatban

DR. KISSNÉ AKLI MÁRIA, BÁLINT IRÉN, DR. PADOS LÁSZLÓ

Nemzeti Hírközlési Hatóság

kissne@nhh.hu

Kulcsszavak: műsorszóró frekvenciasávok, zavarmentesítés, egyenlő hozzáférés, nemzetközi együttműködés

Az RRC04 értekezleten elfogadott tervezési elvek és módszerek hosszas előkészítő munka és nemzetközi egyeztetések eredményeképpen születtek meg, az elvek gyakorlati alkalmazása további pontosítást igényel. A tervezés sikerének fontos alapfeltétele az, hogy az igazgatások a nemzeti érdekeknek megfelelő, ám reális igényeket fogalmazzanak meg és ezeket előzetesen egyeztessék a szomszédos országokkal.

Bevezetés

A földfelszíni digitális műsorszórással (DVB-T és T-DAB) kapcsolatos cikkeket, előadásokat, híreket folyamatosan figyelemmel kísérő olvasók már ismerik a nemzetközi törekvéseket, és tisztában vannak a Nemzetközi Távközlési Egyesület (ITU) Körzeti Rádiótávközlési Értekezletének (RRC) jelentőségével [1]. A témával csak most ismerkedők számára azonban érdekes lehet egy rövid áttekintés az RRC előzményeiről és az RRC első ülésszakának (RRC04) eredményeiről *(1. fejezet)*.

A 2004-ben megrendezett RRC04 értekezlet Záródokumentuma [2] tartalmazza a digitális műsorszórás tervezésére vonatkozó műszaki feltételeket. A dokumentum néhány fejezete az alkalmazott hullámterjedési modellel, elektromágneses összeférhetőségi számítási módszerekkel és paraméterekkel foglalkozik, melyek korábbi évek elméleti kutatásaira, és mérési eredményeire támaszkodnak. A zavarmentes működést biztosító DVB-T és T-DAB hálózatok az adóállomások közötti kompatíbilitási számításokkal, a tervezési paramétereket megfelelően implementáló szoftverekkel, és kellő időráfordítással különösebb akadály nélkül megvalósíthatók *(2. fejezet)*.

A tervezés során nem csupán műszaki szempontokat kell figyelembe venni. A Tervezői Értekezlet feladata egyrészt az, hogy a DVB-T rendszerparaméterek különböző variációiból adódó akár százféle eltérő igényre készítsen egy ütközésektől mentes tervet. Másrészt biztosítania kell a spektrum hatékony kihasználását és a tervezés rugalmasságát, továbbá valamennyi ország számára a spektrumhoz való egyenlő hozzáférést *(3. fejezet)*.

Vannak-e olyan objektív szempontok vagy mérőszámok, amelyekkel pontosan meg lehet határozni a spektrumhoz való egyenlő hozzáférés teljesülését? A válasz egyértelműen nem. A kérdés csak az, hogyan fogja a 2006-ban megrendezésre kerülő RRC06 tervezői értekezlet az egyik legfontosabb célját megvalósítani, nevezetesen azt, hogy a tervezési övezeten belül elhelyezkedő összes ország a rendelkezésre álló spektrumból egyenlően részesüljön digitális műsorszórásra *(4. és 5. fejezet)*.

A tervezési alapelvek megvalósulása, és az RRC06 sikere érdekében már a két ülésszak között megkezdődik a tervezési igények összeállítása és a próbatervek elkészítése. Ezzel párhuzamosan az európai országok úgynevezett előkoordinációs csoportokat hoztak létre a beterjesztett igények egyeztetése és, szükség esetén, előkoordinációs megállapodások megkötése céljából *(6. fejezet)*.

1. RRC04/06 ITU Körzeti Rádiótávközlési Értekezletek

1.1. Előzmények

A hagyományos analóg televíziózáshoz szükséges nemzetközi frekvencia-felhasználást Európában az 1961-ben aláírt Stockholmi Terv (ST61) [3], Afrikában pedig az 1989-es Genfi Terv (GE89) [4] szabályozza. A földfelszíni TV műsorszórásra kijelölt frekvenciasávban 3-4 analóg televízió hálózat kialakítása lehetséges országonként.

Elsősorban az európai országokban ennél jóval több földfelszíni műsorra lenne igény mind szolgáltatói, mind nézői oldalról. Gondoljunk csak vissza az 1997-es magyarországi kereskedelmi televízió frekvenciák pályáztatására. A digitális rendszer gazdaságos frekvencia-felhasználása lehetővé teszi akár 6-7 országos hálózat megvalósítását is, és még több műsor sugárzását a jelenleg analóg televíziózásra használt frekvenciatartományban. Ehhez azonban előbb a digitális műsorszórás nemzetközi szabályozási feltételeit kell megteremteni.

Az Európai Postai és Távközlési Igazgatások Konferenciája (CEPT) kezdeményezésére az ITU Regionális Rádiótávközlés Értekezlete 2001- és 2002-ben döntött a digitális tervező értekezlet összehívásáról, majd 2002-ben Marrakeshben a tervezési övezet kiterjesztéséről. Ennek megfelelően nemcsak az ST61 Egyezményhez tartozó Európai Műsorszóró Övezet országai-

ra (EBA), hanem a GE89 Egyezményt aláíró Afrikai Műsorszóró Övezet országaira (ABA), a Közel-Kelet egy részére, valamint Oroszország ázsiai részének jelentős területére is készül digitális műsorszóró frekvenciaterv.

1.2. Eredmények

Az *RRC04/06* célja egy egyezmény, és a hozzá kapcsolódó földfelszíni *digitális műsorszóró* (DVB-T és T-DAB) *frekvenciaterv* (Terv) elfogadása a 174-230 MHz és a 470-862 MHz sávokban, mely az analóg televíziózás befejezését követően a „teljesen digitális jövőben" biztosítja majd minden aláíró ország számára a földfelszíni digitális műsorszórás céljára a spektrumhoz való egyenlő hozzáférést.

A 2004. május 10-28. között megrendezett *RRC04* célja a második ülésen és a két ülés között végzendő *frekvenciatervezési feladatok előkészítése* volt. Záródokumentuma egy olyan határozat (Resolution 1), melynek mellékletét képezi a Jelentés, továbbá a még szükséges tervezési paraméterek kidolgozására (COM4 határozatai), a két ülésszak közötti feladatokra (COM5 határozatai), valamint az eljárási szabályokra (Gtplen és Plen határozatok) vonatkozó határozatok. A határozatok képezik az alapját az RRC04 és RRC06 közötti időszakban az igazgatások által véleményezett próbatervezéseknek, majd a végleges digitális műsorszóró terv elkészítésének.

A Jelentés tartalmazza a földfelszíni digitális műsorszórás *frekvenciatervezéséhez szükséges műszaki alapfeltételeket és tervezési elveket,* továbbá meghatározta a tervezéshez szükséges adatok és tervezési igények beterjesztésére vonatkozó követelményeket és összeállította a 2006-ban megrendezésre kerülő második ülésszakig terjedő akciótervet. Ahhoz, hogy az RRC06-on egy ütközésektől mentes, mindenki számára előnyös frekvenciaterv kerüljön elfogadásra, a Jelentés javaslatot tartalmaz arra, hogy az igazgatások folytassanak előkoordinációs tevékenységet és szükség esetén előkoordinációs külön-megállapodásokat kössenek a szomszédos országokkal, amelyeket a végleges nemzetközi terv összeállításakor figyelembe vesznek.

Az értekezlet létrehozott egy tervezői munkacsoportot (IPG) az RRC04 és RRC06 közötti időszakban szükséges tervezés előkészítési tevékenység és próbatervezést végző tervező csoport munkájának figyelemmel kisérésére. Az IPG tanulmányozza a próbatervek eredményeit, ha szükséges módosításokat javasol. Az IPG jelentést készít, mely tartalmazza a próbatervek eredményeit, valamint javaslatokat az igazgatások számára a beterjesztett igények esetleges módosítására. Módosíthatja az RRC04-en elfogadott időtervet, ha az nem érinti az igazgatások adatszolgáltatásra vonatkozó, elfogadott határidőit.

A *teljesen digitális jövőre készített frekvenciatervet* a 2006-os *RRC06* tervezői értekezlet véglegesíti. A teljesen digitális televíziózásra történő átállás a gazdasági helyzettől, médiapolitikai döntéstől stb. függően országonként eltérő időpontban fog bekövetkezni. Ezt átmeneti időszak előzi meg, amikor egyidőben analóg és digitális televízióadók is működnek. A Megállapodás biztosítja, hogy az átmeneti időszakban, a jelenleg hatályos ST61 és GE89 Megállapodás, és az ezekhez kapcsolódó frekvenciatervek alapján üzemelő analóg adók zavartalanul működhessenek. Az európai országok legkésőbb 2015-re javasolják az analóg televíziózás megszüntetését, de az EU országok többségében már 2007-2010 között teljesen átállnak a digitális sugárzásra.

2. Tervezési paraméterek

AZ RRC04 Jelentés 1. fejezete a földfelszíni digitális műsorszórással és tervezésével kapcsolatos fogalmak definíciója. A 2. fejezet az RRC04-en a tervezéshez elfogadott ITU-R P.1546-1 Ajánlásban foglalt hullámterjedési modell leírását, alkalmazásának feltételeit tartalmazza. A 3. fejezet a digitális műsorszórásra felhasználható frekvenciasávokat, a különböző vételi módokat és a tervezési paramétereket rögzíti az ellátottság meghatározásához. Megtalálhatók a DVB-T és T-DAB tervezésnél figyelembe vehető referencia tervezési konfigurációk, valamint a referencia hálózatok. A 4. fejezetben ismerhetjük meg az üzemeltetés feltételeit a nem műsorszóró szolgálatokkal való közös sávban. Ezen a területen még sok munka van, ugyanis a meglehetősen hiányos védelmi értékek meghatározását 2006. májusáig kell kidolgozni.

Az ITU a lefektetett tervezési módszer és tervezési kritériumok alapján az EBU (Európai Műsorszóró Egyesület) közreműködésével fejleszti a tervezést támogató szoftvert. Az igazgatások többsége szintén lépéseket tesz tervezőeszközeik alkalmassá tételére, vagy újak beszerzésére a próbatervek kiértékelésére, illetve az élőkoordináció lehetővé tétele érdekében az RRC04-en elfogadott technikai peremfeltételekkel.

3. Tervezési alapelvek

A tervezési alapelvek első olvasásra egyértelműnek tűnnek, és mindenki számára elfogadható célokat fogalmaznak meg. Érdemes azonban elgondolkozni azon, hogy ezek az elvek a gyakorlatban hogyan valósíthatók meg, és nincsenek-e ellentmondásban egymással. Továbbá kérdés, hogy ha valamely ország az alapelvekben megfogalmazott lehetőségekkel él, milyen módon befolyásolja, vagy befolyásolhatja mások lehetőségeit. Előtte azonban ismerkedjünk meg a legfontosabb tervezési alapelvekkel.

3.1. A spektrumhoz való egyenlő hozzáférés

Az ITU Alapszabályzat 44. Cikkelyének 196-os pontja értelmében *minden országnak egyenlő hozzáférést kell biztosítani a spektrumhoz*, a 174-230 MHz és 470-862 MHz közti sávok felhasználásához. A gyakorlati alkalmazásakor a benyújtott digitális műsorszórási igények mellett figyelembe kell venni az analóg televízió-

zásra és a nem műsorszóró egyéb szolgálatok számára lefoglalt frekvenciákat is. Azok az országok, amelyek nemcsak műsorszórásra fogják felhasználni a műsorszóró sávot a teljesen digitális jövőben, azoknak csökkenteniük kell a digitális műsorszórási igényeiket, azaz arányosan kevesebb multiplexre tarthatnak igényt.

A Jelentés megjegyzi, hogy ez a pont még további pontosításra, finomításra szorul.

3.2. Rugalmas tervezés

Az első értekezleten elfogadott tervezési elvek és paraméterek alapján rugalmas tervezésre nyílik lehetőség. Így például az igazgatások saját elhatározásától függ, hogy milyen igényeket nyújtanak be a frekvenciatervre vonatkozóan az alternatív lehetőségek figyelembe vételével.

Ennek megfelelően másoktól „függetlenül" dönthetik el például a vételi módot (fix, hordozható, mobil), a saját körülményeket és feltételeket figyelembe vevő hálózati struktúrát (egyfrekvenciás, több frekvenciás, vagy ezek kombinációja) [6], vagy a DVB-T rendszerjellemzőket [5] és hely ellátottsági százalékot, azaz a rendszerkonfigurációt. Nincs megkötés a III. TV sávban a digitális rádió vagy televízió célú felhasználás arányára, vagy a sáv kettéosztására a két szolgálat között.

A tervnek előrelátónak, és rugalmasnak kell lennie, hogy a jövő technológiai fejlődésével lépést tudjon tartani. A kép- és hangtovábbításon túl, a földfelszíni digitális műsorszórásnak adatátviteli platformot kell biztosítania az innovatív távközlési – mint például e-gyógyítás, e-kormányzás, vagy e-tanulás – szolgáltatásoknak is annak érdekében, hogy segítsen áthidalni a „digitális szakadékot", különösen a fejlődő országok számára.

A terv rugalmasságát az úgynevezett „maszk módszer" biztosítja, mellyel lényegében meghatározzák a tervezési igényként benyújtott digitális rendszerek (T-DAB és DVB-T) által okozott zavaró hatást, illetve az általuk megkövetelt védelmi igényt. Ennek alapján a későbbiekben bármilyen digitális rendszer használható, feltéve, ha nem lépi túl a tervezés során használt digitális tervezési paraméterek által okozott zavarszintet és nem kér nagyobb védelmet, mint a tervezés során igényelt védelem.

Az analóg televíziózást meghatározó ST61 tervet több mint negyven évig sikeresen alkalmazták és az egyezményben foglalt módosítási eljárásoknak köszönhetően nyitott volt a későbbi módosításokra. Az új digitális tervnek legalább ilyen flexibilisnek kell lennie ahhoz, hogy lehetővé váljon a későbbi új digitális technológiák fokozatos bevezetése, így például DVB-H vagy HDTV technológia alkalmazása.

3.3. A spektrum hatékony felhasználása

Mindent meg kell tenni a sáv minél hatékonyabb felhasználása érdekében, – figyelembe véve a technikai és gazdasági akadályokat is –, azaz a lehető legkevesebb csatorna felhasználásával kell biztosítani a Tervben az országok igényeinek megvalósítását.

A spektrumhatékonyságra vonatkozóan az alábbi általános megállapítások tehetők:

- Fix vételi mód frekvenciaigénye kisebb a hordozható vagy mobil vételénél;
- A hordozható és mobil vétel spektrumigénye csökkenthető:
  – kisebb helyszázalék-követelmény választással,
  – kisebb „pixel"-ellátottság érték választással,
  – SFN (Single Freq. Network) hálózat választással;
- Az MFN (Multi Freq. Network) spektrumigénye a kiskiterjedésű (50 km) SFN-ével összemérhető;
- Nagykiterjedésű SFN gazdaságosabban használja ki a spektrumot, mint a kiskiterjedésű SFN;
- A 64QAM és a 16 QAM spektrumigénye hasonló, ha az összes multiplex összegzett kapacitására vetítjük.

3.4. Tervezési módszer

Minden ország maga dönti el, hogy az új Terv mennyire legyen kompatíbilis saját analóg és jelenlegi digitális tervével. Ezért az igazgatásoknak jelezniük kell, mely állomásokat kívánják védeni a Tervben, majd az átmeneti időszakban. Annak érdekében, hogy a próbatervek elkészítése reális időráfordítással elvégezhető legyen, a kisteljesítményű digitális adók, illetve kisméretű kiosztási körzetek tervezésére nem kerül sor. Amint az RRC06-on elkészített Tervet elfogadják, az igazgatások azonnal megkezdhetik a kisteljesítményű digitális adók és a kis kiosztási körzetek egyeztetését az érintett országokkal az értekezleten elfogadott tervmódosítási eljárás lefolytatásával.

A két- és többoldalú tárgyalások hatékonyan segíthetik a tervezést. Ezért az igazgatásoknak mindent meg kell tenniük annak érdekében, hogy a digitális műsorszórási igényeik kompatíbilisek legyenek egymással.

Egyik tervezési módszer szerint a kompatíbilitást úgy biztosítják az új Terv és a meglévő állomások között, hogy további egyeztetésre ne legyen szükség. Ennek a módszernek az a hátránya, hogy nem spektrumhatékony, vagyis kevesebb frekvencia jut országonként a várható digitális igények kielégítésére.

Egy másik módszer a spektrum hatékony használatára, ha a tervezéskor a meglévő állomásokat nem veszik egyáltalán figyelembe (clean sheet módszer), az átmeneti időszakra vonatkozó kompatíbilitást pedig külön eljárással biztosítják. E módszer hátránya, hogy az új Tervben szereplő digitális adók korlátozás nélkül valószínűleg nem helyezhetők üzembe.

A gyakorlatban várhatóan a két módszer kombinációja valósul meg. Így az új Terv kiosztási körzeteinek és/vagy kijelöléseinek többsége kompatíbilis lesz a jelenlegi analóg és digitális állomásokkal, így kis rész lesz az, amit csak korlátozásokkal lehet üzembe helyezni.

3.5. Az országok igényeinek figyelembe vétele

A próbatervezések során a lehető legkevesebbre kell csökkenteni az inkompatíbilis esetek számát. Ha a próbatervezések alapján a terv nem valósítható meg ilyen inkompatíbilitások nélkül, akkor ezeket a szomszédos országok közötti két- és többoldalú egyeztetések útján, külön-megállapodásokkal kell megoldani, lehetőleg még az RRC06 előtt. Ezt tehetik önállóan az igazgatások, vagy az ITU közbenjárásával. Az ITU megpróbálja majd az igazgatásokat a javasolt igények technikai jellemzőinek módosítására kérni az inkompatíbilitások feloldása érdekében. A két- és többoldalú megállapodásokat az ITU teljes mértékben figyelembe veszi.

Azon igazgatások részére, amelyek a tervezési területhez tartoznak, de nem vesznek részt az értekezleten, és nem nyújtanak be digitális igényeket, méltányos számú frekvenciakijelölést kell biztosítani.

Az RRC06 előtt az ITU közzéteszi azoknak az egyéb – nem műsorszóró – szolgálatoknak a listáját, melyeket az igazgatások külön kérésére a tervezés során figyelembe kell venni. A felmerülő inkompatíbilitásokat két- és többoldalú megállapodásokkal kell rendezni.

4. Alapvető ellentmondás az alapelvek között

A CEPT tagországok által megfogalmazott és javasolt alapelvek az értekezlet során, – a CEPT-en kívüli országok kezdeményezésére –, különböző módosításokkal kerültek a Jelentésbe. Egyik ilyen módosítás azoknak a szempontoknak a meghatározása (3.1 pont), melyekre a spektrumhoz való egyenlő hozzáférésnek teljesülnie kell.

Ezzel a kiegészítéssel azonban, – véleményünk szerint –, ellentmondás alakult ki a 3.1 és a 3.2, valamint az ezzel összefüggő 3.5 pontokban ismertetett alapelvek között. A 3.1 kritériumok gyakorlatilag azt jelentik, hogy azonos DVB-T rendszert (modulációs mód, hibajavító kódarány stb.), azonos vételi módot stb. feltételezünk mindegyik ország tekintetében. Mindez kizárja annak a lehetőségét, hogy az igazgatások sajátos igényeiknek megfelelően maguk válasszák meg a tervezési konfigurációt.

Amennyiben mégis érvényesülhet a tervezési konfiguráció szabad megválasztása, a benyújtott igényektől függően (3.2 pont) a spektrumfelhasználás hatékonysága eltérő lesz [6], azaz a 3.3 pontban megismert alapelv, a spektrum leghatékonyabb felhasználása a gyakorlati alkalmazásban csorbát szenvedhet. Az átmeneti időszak kezelésétől függően, – amire várhatóan nagyon eltérő stratégiákat fognak az igazgatások kidolgozni –, a spektrum leghatékonyabb felhasználása szintén eltérően fog érvényesülni. Felvetődik az a kérdés is, ha bizonyos országok a digitális műsorszórásra kijelölt sáv egy részét egyéb, nem műsorszóró szolgálatok részére lefoglalják, hogyan érvényesülhet a spektrumhoz való egyenlő hozzáférés a rendelkezésre álló sávszélesség tekintetében (3.1 pont).

Nyilvánvaló tehát, hogy az ellentmondások feloldása, valamint a gyakorlati alkalmazhatóság érdekében az RRC04-en elfogadott alapelvek további pontosítására és értelmezésére van szükség.

Az alábbiakban, elsősorban példákon keresztül, megpróbáljuk az alapelvek érvényesíthetőségét megvizsgálni, ahol tudunk, lehetséges megoldást felvázolni. A legtöbb esetben azonban csak a problémákat, ellentmondásokat, nehézségeket tárjuk fel, melyekre választ feltehetően csak az RRC06 után kapunk.

5. Spektrumhoz való egyenlő hozzáférés megvalósítási lehetőségei

5.1. Egyenlő hozzáférés a spektrumhoz az analóg televíziózásban

Bár analóg televízió rendszerből is többféle létezik a tervezési régió országaiban, azok száma nem összemérhető a digitális rendszerben megvalósítható változatok számával. Alapvető különbség a hangvivő-képvivő távolságában, a színes televízió rendszerben, valamint a III. TV sávban a televízió csatorna sávszélességében mutatkozik.

A különbségek ellenére a tervezési paraméterekben jelentős eltérés nincs. Az ellátási terület nagyságát elsősorban az adó sugárzási paraméterei és a terepviszonyok határozzák meg. Az országosan sugározható műsorok száma pedig a gerincállomásonként biztosított frekvenciák számával egyenlő.

Az egyenlő hozzáférési elv gyakorlati megvalósítása különösebb nehézséget nem okozott, hiszen az alkalmasan választott adótelephelyekre – melyek nagyobb átfedések, illetve ellátatlan területek nélkül biztosítják az országos ellátottságot – minden ország tekintetében lényegében azonos számú TV csatornát/műsort biztosít.

5.2. Egyenlő hozzáférés a spektrumhoz a digitális televíziózásban

A digitális technológia igen nagy szabadságot biztosít a tervezési konfiguráció megválasztására. A vételi mód, a vétel minősége, az ellátottsági kritériumok, a hálózati struktúra, vagy a DVB-T rendszerjellemzők a frekvenciasáv-elméletben ezernél is több kombinációs tervezési lehetőségre adnak módot [5].

Próbáljuk átgondolni, milyen objektív módszer (mérőszám) alkalmazásával lehetne az igazságos spektrumhasználatot lehetővé tenni az érintett országok számára.

Azonos számú országos ellátottságot biztosító multiplexszel (továbbiakban fedés), azonos számú műsorral, a VHF/UHF sávban felhasznált 8 (7) MHz-esTV csatornák azonos mennyiségével, vagy valamilyen új módszerrel, többféle paramétert is figyelembe vevő mérőszámot kellene (ha ilyen lehetséges) kidolgozni? Az elvek már megvannak, de a gyakorlati alkalmazhatóság még várat magára. A kérdés nem teljesen tisztázott voltát jelzi az is, hogy az elvek a pontosítására szólít fel az RRC04 Jelentés is.

Vizsgáljuk meg, hogy a felsorolt lehetőségek valamelyike alkalmazható-e a gyakorlatban. A teljesség igénye nélkül, csupán néhány aspektusát említjük az alapelvek érvényesítési lehetőségeinek. Megpróbáljuk felvillantani azokat a kritikus területeket, melyek várhatóan sok vitát fognak még kiváltani, és amelyekre az RRC06 végéig megoldást kell találni.

- Ha a *3.1 pontban megfogalmazott elvet és megvalósítási kritériumait* szó szerint *alkalmazzuk*, ez lényegében azt jelenti, hogy azonos tervezési konfigurációból kiindulva, minden ország számára ugyanolyan műszaki tartalmú terv készül, mely minden lényeges paraméterében megegyezik. Az *azonos fedésszám* ebben az esetben teljes mértékben *biztosítja az egyenlőséget.* Megfelelő paraméter választásával a hatékony spektrumfelhasználás is biztosítható. Az igazgatások közötti két- és többoldalú egyeztetések is egyszerűbbé válnak, hiszen többé-kevésbé „egyenszilárdságú, szimmetrikus hálózatok” között kell a számításokat végezni. Ez lényegesen megkönnyítheti a megegyezést. Problémát csak az jelenthet, ha egyéb szolgálatok számára is kell spektrumot és védelmet biztosítani. Ezt azonban később tárgyaljuk. Egyelőre azt feltételezzük, hogy csak digitális műsorszórásra használjuk a rendelkezésre álló spektrumot.

- A következőkben adjunk némi lehetőséget a rugalmas paraméter választásra is. Induljunk ki a 3.1 pontban felsorolt feltételekből: országos ellátottság, azonos vételi minőség és vételi mód, hely- és időellátottság, valamint sávszélesség. A rugalmas tervezést a *DVB-T rendszerparaméterek szabad megválasztásában* biztosítsuk. Első megközelítésben jó megoldás, ha mindegyik ország azonos számú, például 6 fedéshez elegendő frekvencialehetőséget kap. Van azonban egy jelentős különbség az analóg televízióhoz képest. Míg analóg esetben egy 8 (7) MHz-es TV csatornában mindig egy műsor továbbítható, addig digitális esetben – megfelelően jó minőséget feltételezve – a választott paraméterektől függően 1-5 műsor továbbítására nyílik lehetőség. Ennek az a következménye, hogy a szélsőséges eseteket feltételezve egyes országoknak ötször több műsor sugárzásához biztosít a Terv. Az eltérés pedig a 3.2 és 3.5 pontokban részletezett alapelvek alkalmazásából fakadhat. Nevezetesen: a tervezési konfigurációt minden ország a saját igényei szerint megválaszthatja. Aki tehát valamilyen más szempont előtérbe helyezésével például QPSK modulációs módot választ, lényegesen kevesebb műsor átvitelére alkalmas kapacitáshoz jut multiplexenként, mint aki 64QAM-re nyújt be igényt [6].
  Az RRC04 nem fogalmazta meg konkrétan, hogy a spektrumhoz való egyenlő hozzáférésnek az *egyenlő átviteli kapacitás* (műsorok száma) terén is teljesülnie kell.

- Hogyan változik a helyzet, ha a *vételi mód* is szabadon választható? Összehasonlításunkat fix és mobil vételre végezzük. Mobil vételnél egy műsor átviteléhez lényegesen nagyobb átviteli kapacitás szükséges, mint fix vételnél, tehát minden másban azonosságot feltételezve, mobil vételnél kevesebb műsorra nyílik lehetőség. Bár ez nem műszaki fogalom, a mobil vagy hordozható vételre azt lehet mondani, hogy „értékesebb” szolgáltatás, mint a fix vétel. Ilyen értelemben tehát, már a műsorok számának összehasonlítása sem alkalmas az egyenlőség mérésére. Hogyan lehet a több műsort, és „értéktelenebb” szolgáltatást, a kevesebb számú műsorral, de „értékesebb” szolgáltatással összevetni? Kézzel fogható megoldás ebben az esetben is a rendelkezésre álló átviteli kapacitás, és nem az átvihető műsorok száma. Vizsgáljuk meg azt is, hogy van-e hatása a spektrumfelhasználásra annak, hogy mobil vétel esetén a szükséges minimális térerősség (E_{min}) elméletben akár 92 dBµV/ m is lehet, míg fix vételnél – egyéb vételi paraméterekben hasonlóakat feltételezve – csak 53 dBµV/m. A [6] cikkre támaszkodva azt mondhatjuk, hogy mobil vétel esetén lényegesen több frekvenciára van szükség egy-egy multiplex fedés kialakításához. Összefoglalva tehát, bár a fedések száma és a kapacitás azo-

nos, az egyenlőség megkérdőjelezhető. Tovább nehezíti az összehasonlíthatóságot, ha az azonos kapacitást úgy próbáljuk elérni, hogy a modulációs módok eltérőek. Ekkor ugyanis csak bizonyos rendszerparaméter kombinációkra teljesül azonos fedésszám mellett az azonos kapacitás.
Ha tehát az azonos kapacitás biztosítását továbbra is fenn akarjuk tartani, akkor országonként eltérő multiplex számot is kell engedni. Hogyan mérhető ekkor az, hogy a spektrumot mindenki egyenlő mértékben használja-e? Tovább bonyolítja a helyzetet, ha a különböző fajtájú és méretű hálózati struktúrák is változhatnak. A választott helyellátottsági százalék szintén jelentősen befolyásolja a szükséges csatornák számát. Erre találták ki az *ekvivalens csatornaszámot* [6], mely az összehasonlítás alapjául szolgálhat.

Összegezve tehát elmondható; ha lehetővé válik a digitális műsorszórási igények szabad megválasztása, akkor 3.1-ben nevesített egyenlőség az alapvető ellentmondás miatt nem biztosítható. Lehetséges azonban a spektrum igazságos felhasználása, ha a rendelkezésre álló 8 (7) MHz-es TV csatornákból mindenki egyenlően részesül. A választott tervezési konfigurációkból elvileg meghatározhatók az ekvivalens csatornaszámok, ami alapján az országonként biztosítható fedésszámok kiszámíthatók. A vázolt módszer elvileg működik, a gyakorlatban azonban meglehetősen nehézkes. Egyrészt az ekvivalens csatornaszám meghatározására egzakt összefüggés nincs (gondoljunk például a terepadottságok befolyásoló hatására), másrészt legalább annyi esetre kellene meghatározni, ahány különböző tervezési konfigurációt nyújtanak be az országok.

5.3. Referencia tervezési konfigurációk

Bár az elméletben lehetséges több száz tervezési konfiguráció többsége gazdaságossági, műszaki vagy frekvenciagazdálkodási szempontból a gyakorlatban nem kerül alkalmazásra, így is túl sok különböző igényre lehetne számítani. Ugyanakkor zavarszámítási vizsgálatok szempontjából (például időigényesség) az a célszerű, ha csak viszonylag kevés variáció fordul elő a régióra kiterjedő tervezés során. A spektrumfelhasználás összehasonlítása is egyszerűsödhet, ha kellően kevés, de a felmerülő különféle igények figyelembe vételére mégis alkalmas eseteket kell csak figyelembe venni.

Ebből a megfontolásból kiindulva a Jelentés lehetőséget biztosít a referencia tervezési konfiguráció (RPC, Reference Planning Configuration) választásra a tervezési igények összeállítása során. A vizsgálatok szerint DVB-T esetén háromféle RPC elégséges ahhoz, hogy bármilyen tervezési igényre a megfelelő összeférhetőségi vizsgálatokat el lehessen végezni. Az RPC1 tipikusan fix vételre, az RPC2 hordozható kültéri, rosszabb minőségű hordozható beltéri, vagy mobil vételi igény esetén alkalmazható. Az RPC3 jó minőségű hordozható beltéri vételnél választható.

A DVB-T referencia tervezési konfigurációkhoz rendelt legfontosabb tervezési paraméterek a következő *táblázatban* találhatók:

RPC	RPC 1	RPC 2	RPC 3
Referencia helyszázalék	95%	95%	95%
Referencia C/N (dB)	21	19	17
Referencia $(E_{med})_{ref}$ (dB(μV/m)) 200 MHz	50	67	76
Referencia $(E_{med})_{ref}$ (dB(μV/m)) 650 MHz	56	78	88

1. táblázat DVB-T referencia tervezési konfigurációk (RPC)

T-DAB-nál kétféle referencia tervezési konfigurációt határoztak meg:

Referencia tervezési konfiguráció	RPC 4 mobil vétel	RPC 5 beltéri hordozható vétel
Helyszázalék	99%	95%
Referencia *C/N* (dB)	15	15
Referencia $(E_{med})_{ref}$ (dB(μV/m)) 200 MHz	60	66

2. táblázat T-DAB referencia tervezési konfigurációk (RPC)

A választott RPC nem jelent elkötelezettséget valamelyik vételi mód mellett. Csupán meghatározza, hogy milyen E_{min} értéket lehet védeni a kiosztási körzetet határoló tesztpontokban más országok zavaró adóival szemben.

Két szélső esetet nézve az RPC1 előnye az, hogy kisebb zavaró térerősséget enged meg, tehát zavarvédettebb lesz a hálózat. Hátránya, hogy hordozható, illetve mobil vétel kiépítése érdekében csak kisebb teljesítményű, ebből következően viszonylag sok adóra van szükség. Az RPC3 előnye, hogy kevesebb, nagyobb teljesítményű adóval is biztosítható a hordozható vagy mobil vétel. Hátránya, hogy a hálózat zavarvédettsége, és így a teljes országra kiterjedő ellátottság csak az összes szükséges adó kiépítésével biztosítható.

Eddig még nem készült elemzés arra vonatkozóan, hogy azonos fedésszám esetén az RPC választástól független-e a szükséges csatornaszám. Feltételezhető azonban, hogy nem. Ráadásul az RPC választásnál nem feltétlenül spektrumfelhasználási előnyök, vagy spektrumhoz való egyenlő hozzáférési elvek dominálnak, hanem például gazdasági, médiapolitikai megfontolások. A jelenlegi európai trendek azonban abba az irányba mutatnak, hogy az igazgatások igyekeznek kompromisszumot kötni minden tekintetben. Ez pedig végső soron az RPC2 választás irányába mutat.

Ha tehát egy adott ország környezetében mindenki él az RPC választás lehetőségével, ráadásul ugyanazt választják, akkor egyszerűen ugyanannyi fedésszámmal kell az egyenlőséget biztosítani. Természetesen abszolút egyenlőség frekvencia-felhasználás tekintetében sem lesz soha, hiszen az országok terepadottságai, a

választott ellátottsági körzetek méretei stb., ezt mindmind befolyásolják. Mégis úgy tűnik, hogy ez lesz a járható út.

5.4. Egyéb szolgálatok védelme a digitális tervben

Ebben a kérdésben az európai országok közös javaslatokat dolgoztak ki, amelyeket Magyarország is aláírt, azonban az értekezlet során új javaslatok születtek. Így például az egyéb szolgálatok védelme érdekében olyan szigorú értékeket javasoltak, amelyek egyes televízió csatornák felhasználását akár 400-1000 kilométeres körzetben is lehetetlenné tehetik. További problémát jelent az is, hogyan lehet olyan katonai berendezéseket figyelembe venni a tervezés során, amelyek adatairól eddig nem lehetett információt szerezni. Mivel a katonai szolgálatok és a műsorszóró adók együttélésére vonatkozóan jelenleg nincs megfelelő szabályozás, a szükséges egyeztetési eljárásokat a két értekezlet közötti időszakban dolgozzák ki. Döntés született arról, hogy az egyéb szolgálatokra vonatkozó védelmi igényeket és a szükséges adatokat 2005. őszéig kell beterjeszteni.

Végül az RRC úgy döntött, hogy az az ország, amelyik műsorszóró sávot foglal egyéb szolgálatokra, és azt védeni is kívánja a Tervben, annak tudomásul kell vennie, hogy kevesebb spektrumot, ebből következően kevesebb fedést használhat digitális műsorszórásra. Ha egy ország egyéb szolgálatainak védelme nagyobb mértékű korlátozáshoz vezet, mintha digitális műsorszórás lenne teljes mértékben a sávban, akkor az egyéb szolgálatokat védő ország digitális műsorszórási igényeit olyan mértékben kell csökkenteni, hogy az érintett szomszédok számára biztosítható DVB-T frekvencia-felhasználás ne csökkenjen.

5.5. Egyenlő hozzáférés biztosítása a spektrumhoz a III. TV sávban

A III. TV sáv tervezése alapvetően abban különbözik a IV-V. sávtól, hogy a földfelszíni digitális televízió mellett a földfelszíni digitális rádió is bevezetésre kerül (DVB-T és T-DAB közös felhasználás), továbbá a III. sávban különböző csatornaosztásokat (7 MHz és 8 MHz) alkalmaznak a tervezési övezet különböző országaiban, sőt még Európán belül is.

A III. TV sáv közös felhasználását tekintve három lehetőség közül választhatnak az igazgatások:

– kizárólag T-DAB vagy kizárólag DVB-T célú felhasználás,
– III. sáv felosztása a különböző szolgálatok között,
– vegyes T-DAB/DVB-T felhasználás.

A III. sáv közös T-DAB-DVB-T felhasználása az országok igényeitől függően, különbözőképpen valósulhat meg. Az RRC04 döntése értelmében bármelyik ország bármely csatornát használhatja DVB-T-re vagy T-DAB-ra egyaránt. Természetesen így még bonyolultabbá válik az összeférhetőségi feltételek kielégítése és a spektrumhoz való egyenlő hozzáférés biztosítása.

Bár a rugalmas tervezés alapelvére hivatkozva az igazgatások a későbbiekben is eldönthetik, hogy milyen szolgálatra használják a számukra kiosztott frekvenciákat, a DVB-T és a T-DAB szolgálat eltérő spektrumigénye miatt ez nem járható út. Egy DVB-T csatornában négy T-DAB csatorna helyezhető el, tehát már az igények benyújtásánál el kell dönteni, hogy mely csatornákat kívánják a III. sávban digitális rádiózásra vagy televíziózásra használni. Míg egy bizonyos területre kiosztott DVB-T csatorna későbbi T-DAB célú felhasználása négy T-DAB multiplex bevezetését teszi lehetővé az adott területen, fordított esetben egy T-DAB frekvenciablokk pozíciót a későbbiekben nem lehet már DVB-T céljára felhasználni.

Tekintettel arra, hogy bármelyik ország bármely csatornát használhatja mindkét szolgálatra, a leghatékonyabb frekvencia-felhasználás elve is sérül, hiszen az optimális frekvencia-felhasználás akkor érhető el, ha a szomszédos országok ugyanazokat a TV csatornákat használják DVB-T-re illetve T-DAB céljára.

Amennyiben az országok az előkoordináció folyamán egymás között nem egyeznek meg a III. sáv felhasználását tekintve, bármely analóg csatorna felhasználható T-DAB és DVB-T céljára is. Ez a legbonyolultabb tervezési mód, mivel a földrajzi átlapolódás mellett a spektrumátlapolódást is figyelembe kell venni és különböző csatornaosztások esetén nehéz feladatot jelent a határövezeti kiosztások egyeztetése.

Az alapelvek közötti ellentmondások fokozottan jelentkeznek különböző csatornaraszterek alkalmazása esetén. A T-DAB kiosztás a 7 MHz-es és a 8 MHz-es rendszerekkel is kompatíbilis, azonban a 8 MHz-es csatornaosztás esetén a négy T-DAB blokk nem fedi le teljesen a 8 MHz-es csatornát, 5 blokk pedig nem helyezhető el benne, tehát a frekvencia-felhasználás spektrumveszteséggel jár, kevésbé hatékony. Bár mindegyik országnak joga van az analóg televíziózásban használt csatornaszélesség megtartásához, az országok többsége felismerte a 7 MHz-es csatornaosztásra való áttérés előnyeit és a digitális tervet 7 MHz-es csatornaosztásra alapozva készíti el.

Mivel a T-DAB igények benyújtásánál (a csak mobil vételre tervezett WI95 kiosztásoknál is) az igazgatások szabadon választhatnak a két vételi mód közül, inkompatíbilitásra lehet számítani a már meglévő WI95 kiosztások tekintetében is.

Amennyiben a WI95 kiosztásoknál is a beltéri hordozható vételt választják az egyes országok, bizonyos kiosztások esetén az ellátott terület beszűkülésével kell számolni és előfordulhat, hogy nem valósul meg a teljes országos ellátottság. Másfelől a beltéri hordozható vételre tervezett T-DAB kiosztások nagyobb zavart okoznak, mint az azonos területekre vonatkozó WI95 kiosztások, ennek kapcsán tehát további vizsgálatok szükségesek.

A leghatékonyabb frekvenciatervezés akkor érhető el, ha a szomszédos országok azonos csatornaosztást alkalmaznak és ugyanazokat a csatornákat használják T-DAB illetve DVB-T céljára, továbbá az adott szolgálatokra ugyanazt a referencia tervezési konfigurációt választják.

6. Európai előkoordinációs folyamatok

Az európai országok többsége felismerte azt, hogy az RRC06-ot megelőző két ITU próbatervezés és az RRC06 öthetes időtartama kevés a mintegy száz országra kiterjedő optimális, mindenki számára elfogadható, az alapelvek érvényesülését biztosító digitális terv elkészítésére.

Ezért, az ITU és a CEPT biztatására, intenzív előkoordinációs folyamat kezdődött meg az érintett országok részvételével. Ezek célja az, hogy mindegyik ország esetén azonos számú országos fedéshez biztosítson frekvenciát. A tervezés kiosztási körzeteken alapszik és ezekhez a körzetekhez rendelik hozzá a frekvenciákat. Amennyiben kiosztási körzetre tervezünk, elméletileg 100%-os országos ellátottság biztosítható.

Az országos lefedések száma jelentős mértékben függ a kiosztási körzetek méretétől. Amennyiben az országok sok kis méretű kiosztási körzetet határoznak meg, a lehetséges országos lefedések száma csökken. Az eddigi tapasztalatok azt mutatják, hogy az igazgatások a számításokat egyszerűsítő tervezési konfigurációk megadását preferálják a konkrét rendszerparaméterek meghatározása helyett. Mivel a nemzeti adottságoknak leginkább megfelelő RPC kiválasztása is fontos döntést igényel, az előkoordinációs csoportok e tekintetben is folyamatosan egyeztetnek.

A tervezési alapelvek mellett igen fontos tényező az is, hogy az igazgatások mikorra tervezik a digitális átállás befejezését és milyen stratégiát követnek az átmeneti időszakban. Az előkoordinációs folyamatok jó alkalmat biztosítanak az igazgatások digitális stratégiájának megismerésére és az átmeneti időszakra vonatkozó elképzelések egyeztetésére.

Irodalom

[1] Kissné Akli Mária: Frekvenciák biztosítása a földfelszíni digitális televíziózáshoz, Infokommunikáció és jog, 2004/4. szám

[2] Resolutions from the First session of the Regional Radiocommunication conference for planning of the digital terrestrial broadcasting in parts of Region 1. and 3. in the frequency bands 174-230 MHz and 470-862 MHz, Geneve 10-28 May 2004.

[3] Final Acts of the European Broadcasting Conference in the VHF and UHF bands, Stockholm, 1961.

[4] Final Acts of the African Broadcasting Conference in the VHF and UHF bands, Geneve, 1989

[5] Kissné Akli Mária: Digitális rendszerjellemzők választása DVB-T adók besugárzás-tervezéséhez, Híradástechnika, 2002/8.

[6] dr. Kissné Akli Mária: MFN vagy SFN? Híradástechnika, 2004/8.

A digitális műsorszórás helyzete

— hírek közt tallózva —

Egyetlen ország sem lesz teljesen digitális 2014-ig

A Global Digital TV Forecasts (Globális digitális TV előjelzések) elnevezésű kutatás azt jósolja, hogy csak öt ország fogja elérni a 100%-os digitális szintet 2014-re: az USA, Kanada, Írország, Finnország és Norvégia. Az Egyesült Királyság 2015-ben jut el idáig, Dániával, Svédországgal, Hong-Konggal, Japánnal, Dél-Koreával és Tajvannal együtt.

A kitolódott határidő okai között szerepel a későn átálló fogyasztók körében mutatkozó ellenállás, valamint a fejlődő országokban a hálózat modernizálásánál tapasztalható finanszírozási hiány.

Az Informa rámutat még arra is, hogy a kormányok vonakodnak előírni a gyártók számára az analóg készülékek gyártásának beszüntetését, vagy megkockáztatni a népszerűtlenséget az analóg leállás kierőszakolásával. Az analóg kábel tartós népszerűsége szintén megjelenik tényezőként egyes piacokon.

A jelentés óvatos képet fest a digitális világ növekedéséről. A világ összes televízióval rendelkező otthonának mindössze 34 százaléka, azaz 370 millió rendelkezik majd digitális vétellel 2010-re, ami 12 százalékos bővülést jelent a jelenlegi szinthez képest, vagyis 2010-ben a világ televízióval rendelkező háztartásainak kétharmada még mindig analóg jelet vesz majd.

New Media Markets, No.41, 2004.

Előzetes DTT adásindítás januárban

A jövőbeni francia DTT szolgáltatás ingyen fogható csatornáinak szolgáltatói, valamint a kulturális miniszter megbeszélésén elhatározták, hogy az Eiffel-tornyon elhelyezkedő adóról 2005. január 15-én előzetes adást indítanak. Az ingyenes csatornák indításának hivatalos dátuma 2005. március 1. és az adás körülbelül a lakosság feléhez fog eljutni. Az előzetes adás Párizsban lehetővé teszi a korai csatlakozók számára, hogy kipróbálják a vételt és az antenna telepítők számára is lehetőséget ad az indulásra való felkészülésre.

www.advanded-television.com

Románia készül a digitális TV-re

Romániában 2004 vége előtt megkezdték az első digitális DTH platform sugárzását. A Media Expres szerint a Focus Sat-ot a Thor III sugározza majd a NY 1°-on, a kódolása pedig Conax CA technológiával történik. A helyi partner az Eastern Space Systems lesz. A szolgáltatás kezdetben 25 csatornát kínál és a vételt biztosító eszközök ára körülbelül 200 Euró lesz. Az előfizetés az első fél évben ingyenes, ezt követően pedig havi 4,5 és 9,7 Euró között fog váltakozni.

A Focus Sat vevőkészülékeket kezdetben kétszáz helyen árusítják majd az országban, a szolgáltatásnak pedig 2008-ra várhatóan 200 ezer előfizetője lesz. Romániában még legalább négy DTH platform indítását tervezik.

Broadband TV News

Spanyolország (újra) felugrik a DTT vonatára

Három évvel a Quiero nevű DTT fizetős TV rendszer fiaskója után, Spanyolország arra készül, hogy 2005-ben újra elindítsa a digitális földfelszíni televíziózást.

Annak érdekében, hogy végső lökést adjon a piac fellendítésének, a szocialista kormány úgy döntött,

Digitális televízió-vétellel rendelkező háztartások várható összetétele 2010-ben (millió), Forrás: Informa Media Group

	DTT	Kábel	DTH	DSL	*Összes digitális*	*Összes TV*
Ázsia/Csendes-óceán	8,6	100,1	15,3	10,4	134,4	605,4
Európa	21,9	45,5	31,3	9,8	108,5	237,5
Latin-Amerika	1,2	7,1	4,8	0,8	13,9	106,7
Észak-Amerika	1,0	76,1	34,6	1,3	113,0	126,4
Összesen	***32,7***	***228,8***	***86,0***	***22,4***	***369,8***	***1076,0***

hogy az analóg műsorszolgáltatás leállítását 2010 elejére, a korábban tervezettnél két évvel hamarabbra, irányozza elő. A döntés egy új DTT Műszaki Terv formájában fog testet ölteni, amelyet a kormánynak ez év első felében kell jóváhagynia. Ez az új terv megalapozza a DTT piac újbóli beindítását. A DTT szolgáltatás bevezetése ősszel kezdődik egy olyan ingyenesen fogható DTT programrendszer elindításával, amely a kormány tervei szerint kezdetben maximálisan 22 csatornát fog szétosztani: 14-et országos lefedettséggel, továbbá lesz négy regionális, és négy helyi TV állomás.

A regionális DTT állomásoknak 2005. januárjától kell megkezdeniük a digitális adásokat; a helyi DTT csatornák digitális sugárzására augusztustól 2008-ig lesz lehetőség, amikorra már befejeződik ezeknek a digitálisra való átállítása. 2005-ben a regionális hatóságok nyilvános versenytárgyalásokat írnak ki a helyi DTT engedélyek odaítélése céljából. Az új országos DTT csatornák valószínűleg a nyáron kezdik meg a digitális adásokat, amikor a Quiero frekvenciáit – három és fél multiplex összesen 14 csatornát képes továbbítani – már újra kiosztották az összes meglévő TV társaság között.

A kormánynak a DTT piac fejlődésének elősegítésére tett ezen intézkedései három törvény moódosítását fogják megkövetelni: a magán TV csatornákra vonatkozó törvényét, a helyi csatornákra vonatkozó szabályozását, és a távközlési törvényét. Ami a magán csatornákra vonatkozó törvényt illeti, a kormány a digitális műsorszórásra való átállási időszakban engedélyezni fogja háromnál több országos lefedettségű TV csatorna megmaradását, és két csatorna (analóg és digitális) egyidejű tulajdonjogát az átállási időszak alatt. A helyi tévékre vonatkozó törvény is módosul annyiban, hogy lehetővé teszik egynél több, helyi közszolgálati TV állomás fennmaradását, és a megbízást ötről tíz évre terjesztik ki. Végül a kábeltévé piac más üzemeltetők részére is megnyílik, és ezzel a piac a vártnál négy évvel korábban liberalizálódik.

A DTT piac feltámasztására irányuló ezen kormányintézkedéseket a magán TV állomások, vagyis az Antena3 és a Tele5 is üdvözölte. A hálózatok közös tévés reklámkampányt indítottak a DTT népszerűsítésére, és ezzel egyidejűleg próbálják meggyőzni a kormányt a DTT piac fellendítésére vonatkozó végső lökés szükségességéről.

Az Antena3 és a Tele5 egyaránt azt állítják, hogy készen állnak öt DTT csatorna rövid időn belüli beindítására azzal a feltétellel, hogy a kormány megnyitja a lehetőséget a piac fejlesztése előtt. Az említett két csatorna úgy véli, hogy 2007-re Spanyolország fele képes lesz hozzáférni a DTT szolgáltatáshoz. Az Antena3 több program létrehozásán is dolgozik, többek között egy élelmiszerekkel és táplálkozással, illetve egy túrizmussal foglalkozó csatorna beindítását tervezi, miközben a Tele5 egy ifjúsági csatornát szeretne létrehozni.

Digital News, No.41, 2005.

Olaszország megerősíti a 2005. évi csökkentett szintű DTT támogatásokat

Olaszország egyike azoknak az országoknak, akik agresszívan törekednek a digitális technológiára való átállásra, 2006-ot tűzve ki a befejezés határidejének. 2004 elejétől a kormány 150 Eurós támogatást ajánlott az első 700 ezer digitális set-top-box vásárlóinak, amelyeknek az ára jellemzően 200 Euró körül mozog. A támogatásra való jogosultsághoz a digitális dekódernek tartalmaznia kell egy smart card leolvasót, valamint egy beépített modemet is. Maurizio Gasparri hírközlési miniszter megerősítette, hogy a digitális dekóderek állami támogatása 2005-ben is érvényben marad, habár alacsonyabb, 120 Eurós szinten. Az árengedmény csökkentését a dekóderek csökkenő árának tulajdonítják. Gasparri azt mondta, hogy „a nyilvános információs szolgáltatások TV-távirányítóval való elérésének" távlati tervei állnak a digitális tévé további szubvencionálásáról szóló döntés mögött. Azt is bejelentette, hogy a digitális tévére történő végső átállásra az ország egyes területein már a 2006. évi határidő előtt sor kerülhet.

Digital News, No.40, 2004.

DTT hírek a Cseh Köztársaságból

A Cseh Műsorszóró Tanács (RRTV) hivatalosan versenytárgyalást hirdetett két kereskedelmi DTT multiplexre. A végső győztes 12 éves televíziós – vagy 8 éves rádiós – műsorszórási licencet kap. A két, „B" és „C" néven ismert multiplex egy harmadik („A") multiplex mellett fog működni, amelyet közszolgálati TV és rádió szolgáltatásnak tartanak fenn, és amely az ország 77 százalékát lefedi.

Az RRTV lépését a kereskedelmi TV-szektor részéről érkező nyomásgyakorlással szembeni ellenállásként lehet értékelni. A PPF Csoport, a TV Nova tulajdonosa reméli, hogy a Cseh Köztársaság vezető állomását akár 318,5 millió Eurós árat is elkérve tudja értékesíteni a Bertelsmann-nak, és attól tart, hogy a DTT bevezetése aláásható a televíziós reklámpiacot.

A Parlamenti Média Bizottság időközben azt reméli, hogy az RRTC vár a tenderrel egy új Elektronikus Hírközlési Törvény elfogadásáig. A létező műsorszórási jogszabályok változtatásait szintén el kell végezni, mielőtt a DTT megkezdhetné működését.

Többen azonban a DTT indításának reményében már tervezik digitális csatornák bevezetését. Ezek közé tartozik a Cseh Televízió és a J&T szlovák befektetői csoport, a Sazka lottójáték csoporttal és a Febio filmgyártó társasággal együtt.

DTT fellendülés az európai közszolgálati műsorszóróknál

A spanyol (RTVE), az olasz (RAI), az egyesült királyságbeli (BBC), a német (ARD és ZDF), valamint a francia (France Television) közszolgálati televíziós csoportok ígéretet tettek, hogy egész Európában kifejlesztik a digitális földfelszíni televíziós (DTT) műsorszórást.

Egy Madridban tartott megbeszélés alkalmával az említett csoportok felsőszintű vezetői kifejezték nyilvános támogatásukat a DTT iránt, és kötelezettséget vállaltak, hogy erőteljesen szorgalmazzák e rendszer nagyarányú piaci bevezetését. Igéretet tettek arra is, hogy minden állampolgár hozzáférhet a digitális rendszerekhez. Madridi találkozójukkal az európai közszolgálati műsorszórók nyilvános támogatást is akartak nyújtani az RTVE-nek egy olyan időszakban, amikor új közszolgálati televíziós modellt dolgoz ki egy kormány által kijelölt szakértői csoport, amelynek a következtetései a következő hetek során kerülnek napvilágra.

http://www.advanced-television.com/2005/news_archive_2005/Jan24_28.htm#euro

Bejelentették az Egyesült Királyság átállási menetrendjét

Az Ofcom végre hivatalossá tette az Egyesült Királyság digitális műsorszórásra való átállásának menetrendjét. A javaslatok részleteket adnak meg arra vonatkozóan, hogy a korábbi ITV koncessziós térkép alapján a 15 régió mindegyike mikor áll át kizárólagosan digitális műsorszórásra a 2008 és 2012 közötti fokozatos átállás során. A kiadvány jelenleg még mindig csak tervezet formájában létezik, és a kormány jóváhagyására vár. Erre a jóváhagyásra azonban feltehetően csak az általános választás után kerülhet sor. A kereskedelmi műsorszórók 2012. december 31-ig kötelesek átállni a digitális adásra, a Digitális Átállási Engedélyek kiadását követően. A digitális televíziós szolgáltatások jelenleg az Egyesült Királyság területének mintegy 73%-ára terjednek ki, de a lefedettség jelentős növelésére mindaddig nincs lehetőség, amíg a meglévő analóg szolgáltatásokat le nem állítják.

Macedónia DTT próbaadást indít

Macedónia megkezdte a kísérleti DVB-T adásokat egy, az IMP (Szlovénia) által szállított 100 W-os adó, valamint a Tandberg-től származó kódolók és multiplex alkalmazásával. A főváros, Szkopje, és a fővárost körbefogó terület lefedésével az MRT közszolgálati műsorszórótól két országos földfelszíni program, az MRT műholdas csatornája, és egy meg nem nevezett műholdas sugárzású szolgáltatás szerepel a nézőknek nyújtott kínálatban a 39-es UHF csatornán.

Az adó tulajdonosa a Public Enterprise Macedonian Broadcasting, amely korábban az MRT része volt, jelenleg pedig műsorszóró hálózat felügyeletéért felelős. Bár Macedóniának még ki kell dolgoznia a DVB-T-re vonatkozó stratégiát, annak potenciális előnye, azaz hogy két vagy több audió sávot lehet egy videó jelen továbbítani egy olyan országban, ahol a lakosság 25 százaléka a többségétől eltérő anyanyelvet beszél, erőteljesen egy ilyen stratégia mellett esik a latba.

Elindul a DAB?

A digitális rádiók európai eladásai biztató jeleket mutatnak, mivel az Egyesült Királyságban 2004 végén a háztartásokban 1,2 millió ilyen készülék volt. A World DAB fórum állítása szerint az egyesült királyságbeli eladások 2003/2004-ben 178%-os növekedést mutattak. Összehasonlításképpen, Dániában a növekedés 350% volt, Belgiumban pedig 500% ugyanebben az időszakban.

Az érdeklődés más országokban is növekszik; Norvégia azt jelentette, hogy az eladások száma decemberben éppen meghaladta a 4000 készüléket. 70%-os lefedettség mellett (a növekedés két éven belül 80%-ra nőtt) és egyes népszerű FM szolgáltatások kizárólag DAB-ra való átállításának terveivel a DAB piac várhatóan fellendül 2005-ben.

http://www.advanced-television.com

Digitális TV-adóberendezések rádiófrekvenciás fokozatai

DR. FALUS LÁSZLÓ
l.falus@chello.hu

Kulcsszavak: DVB-T adó, tranzisztoros teljesítményerősítő, lineáris és nemlineáris torzítások, digitális előtorzító

A rendszeres földfelszíni digitális műsorsugárzás Európa kilenc országában működik és további ötben ez évben indítják meg. A tapasztalatok alapján kialakultak a jellemzők követelményei, a mérési módszerek és a berendezések felépítése. Az adó részei a kódoló mellett a rádiófrekvenciás modulátor, a teljesítményerősítő és a szűrőegységek. Fontos, hogy ezek a fokozatok kis mértékben torzítsák a továbbított jeleket és megfeleljenek a spektrum-követelményeknek. Az általuk befolyásolt jellemzőkkel, felépítésükkel és a torzítások korrekciójával foglalkozik a cikk.

A földfelszíni digitális TV műsorszórást, a DVB-T-t Európában a 170-230 MHz-es III., illetve a 470-862 MHz-es IV/V. sávban valósítják meg. Magyarországon nincs szabad csatorna a III. sávban, így az adók az utóbbi tartományban fognak működni. Az átmeneti időszakban a jelenlegi analóg adók és az új, digitális adók párhuzamosan sugároznak majd, ami megkívánja az összeférhetőség biztosítását.

Az analóg adóberendezések kimenő-teljesítménye általában legfeljebb 20 kW, ritkán 40 kW. A digitális adóké ennek törtrésze, legfeljebb 6 kW. A hatásos kisugárzott teljesítmény (Effektive Radiated Power, ERP) az antennarendszer nyereségének következtében az adóteljesítmény többszöröse. A berendezéseknek úgy a digitális jelkialakító, kódoló, mint a rádiófrekvenciás részekben új áramköri és méréstechnikai követelményeket kell teljesíteniük. A jeltorzítások többsége a rádiófrekvenciás fokozatokban keletkezik, így ennek elemzése és a csökkentésüket eredményező előtorzítás a digitális adástechnika fontos kérdése.

A DVB-T adó felépítése

Az adó főbb részei a meghajtófokozat, a teljesítményerősítő és a kimeneti szűrő. Ezen kívül lényeges feladatokat teljesít még az automatika, a tápegység és a hűtőrendszer. A főbb részek feladatai a következők:

Meghajtófokozat

A fokozat a külső forrásból, a multiplexerből érkező kódolt és egyesített, MPEG-2 szabványú adatfolyamot fogadja. Feladata a jeleknek a DVB-T szabvány [1] szerinti kialakítása és illesztése a földfelszíni csatorna átviteli jellemzőihez. A jel hibavédelméhez elvégzi a külső és a belső kódolást és átszövést, a leképezést, az ortogonális frekvenciaosztásos multiplexelést, más szóval az OFDM jel kialakítását [6], továbbá a védelmi időköz beiktatását és a nagyfrekvenciás vivő modulálását. A jelek a kódolást követően fázisban lévő (I) és kvadratúra (Q) összetevőkként csatlakoznak a digitális előtorzító egységhez. Az előtorzító feladata fontos a rádiófrekvenciás jellemzők szempontjából. Az előtorzító után megtörténik az I és a Q jelek digitális-analóg átalakítása, majd a moduláció. Ennek eredménye a meghajtó fokozat kimenetén az előtorzított, kisteljesítményű nagyfrekvenciás meghajtójel. Az előtorzítót az I/Q modulátor követi. Ez az első rádiófrekvenciás fokozat, mivel kimenetén már vivőfrekvenciás RF jel van.

Teljesítményerősítő

A fokozat a kisteljesítményű meghajtójelet erősíti az adóberendezés kimenő-teljesítményének szintjére. A DVB-T adókban ma már szinte kizárólag tranzisztoros erősítőket alkalmaznak, bár bizonyos esetben igyekeznek induktív kimenetű adócsöveket (IOT) alkalmazni, mert azok egyes adóüzemeltetőknél az analóg adókhoz raktáron vannak. A félvezetős fokozat a kimenőteljesítménytől függően egy, vagy több fiókos egységből áll, amelyeket paralleljáratú egységek kapcsolnak össze. A fokozatok és ezzel az egész berendezés hűtésére újabban folyadékhűtést alkalmaznak.

Kimeneti szűrő

A hírközlési hatóságok a nemzetközileg egyeztetett szabványok alapján előírják és ellenőrzik a berendezések káros jelkibocsátását. Ebből a szempontból a DVB-T adóknál elsősorban a sokvivős átvitellel összefüggő, csatornán kívüli spektrumot kötik meg. Ennek a szabványnak a kielégítése az esetek túlnyomó többségében csak a kimeneten beiktatott sávszűrővel lehetséges.

Rádiófrekvenciás fokozatok

Teljesítményerősítő

Az adóberendezések nagyteljesítményű tranzisztorai első megjelenésük óta nagy változáson mentek át. A bipoláris, majd a MOS után ma az LDMOS tranzisztorokat alkalmazzák a korszerű erősítőkben.

Az LDMOS tranzisztoroknak a bipolárisokhoz viszonyított előnyei, hogy tűrik a terhelésről visszaverődött teljesítményt, a túlvezérlést és a digitális jeleknél előforduló nagy csúcsteljesítményt, továbbá erősítésük is nagyobb. Erősítési görbéjük lineárisabb, így a sokvivős, a DVB-T jelek esetén kisebb az intermodulációs torzítás. Az alkalmazott gyártási módszer és a tokozási megoldás megbízhatóbb működést, hosszabb élettartamot eredményez.

Több cég is gyárt TV adók számára LDMOS tranzisztorokat. A Philips BLF861A típusa 860 MHz-en, AB osztályú beállításban analóg TV jelek esetén tipikusan 170 W kimenő-teljesítményre képes 14 dB erősítés mellett, a DVB-T teljesítményt a gyártó nem közli. A tokban két, ellenütemű működésre tervezett térvezérlésű tranzisztor van, amelyek source-át közvetlenül csatlakoztatják a fém alaplemezhez (flange). Az erősítő áramköre a be- és a kimeneti szimmetrizálókból és illesztő szakaszokból áll *(1. ábra)*.

Az erősítő áramkörének elsődleges feladata a be- és a kimenet szimmetrizálása, továbbá a tranzisztor szélessávú illesztése. Az aszimmetrikus ki- és bemenet és az ellenütemű tranzisztor közötti szimmetrizálást koaxiális kábelből kialakított tápvonalak valósítják meg. Az illesztő áramkörök feladata, hogy a mintegy 400 MHz szélességű sávban illessze a tranzisztort az erősítő 50 Ohmos be- és kimenetéhez. A BLF861A típusú tranzisztor bemenő impedanciája a sávban 1 és 8 + j 3 és 11 Ohm közötti értékű. Az optimális terhelés 8 és 5 – j 3 és 2,5 Ohm közötti. Ezeket, a fokozat 50 Ohmos csatlakozó impedanciájának tört részét jelentő komplex impedanciákat kell széles sávban illeszteni a be- és a kimeneten. Az első illesztő szakaszok a tranzisztor belsejében vannak, a továbbiakat szalagvonalas tápvonal szakaszokkal valósítják meg.

A teljes, 470-860 MHz közötti sávra megvalósított egyenletes frekvenciamenet eredményeként a 8 MHz széles DVB-T csatornában a lineáris torzítás, az amplitúdó és a csoportkésleltetés (group delay) ingadozása elhanyagolható. A teljesítményerősítők megbízható működésének alapfeltétele a kifogástalan hűtés. A tranzisztorban fellépő hő útjának első szakasza a réteg és a tok közötti belső, majd a tok és a hűtőtömb közötti külső átmenet. A belső szakaszt a tranzisztor technológiája, a külsőt a tok és az erősítő konstrukciója határozza meg. Az egy-egy tranzisztort tartalmazó modulokból kialakított meghajtó- és végerősítőt közös felületre, a hűtőtömbre szerelik. A hőt erről korábban áramló levegővel, ma a tömbben áramoltatott folyadékkal szállítják el.

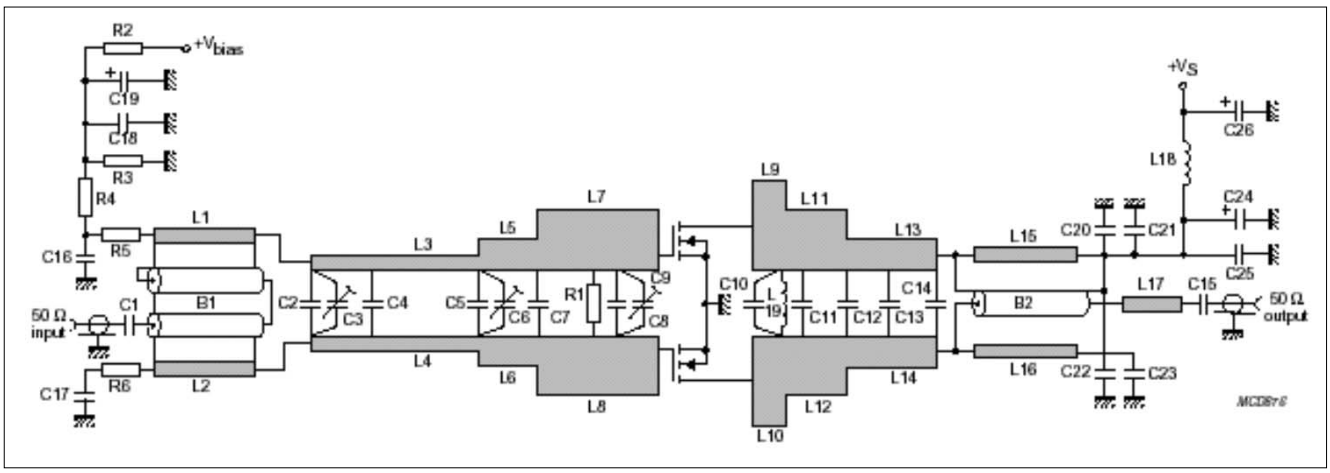
A modulokat szélessávú teljesítmény-elosztók és összegezők kapcsolják össze, amelyek egyenlő arányban szétosztják a bemenő teljesítményt és összegezik a kimenő teljesítményeket. Ezek általában a Wilkinson-csatoló elve szerint épülnek fel és alkalmasak a nyomtatott, szalagvonalas megvalósításra. Alapegységeik a kettes és a hármas csatolók, amelyből négyes, hatos, nyolcas stb. csatolók építhetők fel. A teljesítmény-elosztók és -összegezők fontos jellemzője, hogy az összekapcsolt erősítők közül egy, vagy több hibája, kiesése esetén is biztosítják az erősítőfokozat működését csökkent teljesítménnyel. Az egy fiókos egységben kialakított erősítő DVB-T kimenő teljesítménye kb. 0,5 kW, ennél nagyobb teljesítményű adónál több, párhuzamosan működtetett egységet alkalmaznak.

Kimeneti szűrő

A teljesítményerősítő nemlineáris torzítása miatt a hasznos sávon kívüli nemkívánt összetevők jelennek meg, ami a spektrum elnyúlását, az úgynevezett szoknya kialakulását eredményezi. A 8 MHz-es, közel nyolcezer vivős, 8k rendszernél a hasznos spektrum szélessége a közepes vivőhöz viszonyítva ±3,805 MHz. Az intermodulációs termékek a szomszédos csatornákban jelennek meg és zavarhatják az ott sugárzott adást.

A DVB-T adók elektromágneses összeférhetőségre vonatkozó harmonizált szabvány [2] kétféle tűrésábrát ír elő a hasznos sávon kívüli spektrum csillapítására. Az egyik a normál, vagy nem-kritikus, a másik a kritikus esetre vonatkozik. Az előbbinél a szomszédos csatornában analóg, a másiknál pedig kisteljesítményű adás folyik. A tűrésábrából két jellegzetes pont emelhető ki, amelyek a közepes vivőtől ±4,3 MHz és ±6 MHz távolságban vannak. Az előbbi a hasznos csatorna végétől,

1. ábra Teljesítményerősítő fokozat LDMOS tranzisztorral



a szélső vivőtől 0,5 MHz távolságra van. A DVB-T adók műszaki adatai között szereplő válltávolságot, a hasznos spektrumhoz viszonyított mellékhullám szintet is ebben a pontban kell mérni.

A nem-kritikus esetre, a hasznos spektrumhoz viszonyítva előírt csillapítás ±4,2 MHz-en 40 dB, és ±6 MHz-en 52 dB. A kritikus esetre a szabvány 10 dB-lel szigorúbb értéket ír elő. Az adó teljesítményerősítőjének kimenetén a válltávolság a teljesítményerősítő kivezérlésétől, torzításától és az előtorzítás hatékonyságától függ és általában szükségessé teszi kimenőszűrő alkalmazását. A kimeneti szűrő csillapítás különbsége legalább 4 dB kell legyen. A kimenőszűrő 6-8 körös sávszűrő.

Torzítások elemzése

A DVB-T jelet általában az I és Q koordinátájú konstellációs diagramban ábrázolják és torzításának mértékét a modulációs hibaaránnyal (Modulation Error Ratio, MER) jellemzik. A konstellációs diagram a modulációs módtól függő számú, 4, 16 vagy 64 vektor végpontját és döntési területét ábrázolja. A MER a vektorok végpontjának az ideálistól való eltérését fejezi ki. A torzítások, zavarójelek és a zaj hatására a konstellációs diagram különböző változásokat mutat, amelyeket az irodalomban részletesen tárgyalnak [3].

Az adóban a torzítások elsősorban az előtorzító utáni fokozatokban lépnek fel. A főbb torzítások a következők:

a) *Amplitúdó egyenetlenség, vagy I/Q amplitúdó-hiba.* Az I és a Q jelek amplitúdója közötti eltérést a két modulátor beállításának pontatlansága okozhatja. Hatására a konstellációs diagramban a pontok távolsága vízszintes, vagy függőleges irányban összenyomódik.

b) *Kvadratúra hiba, vagy I/Q fázishiba.* Ez az I és a Q jelek közötti, a 90°-hoz viszonyított eltérés. Ezt a két modulátort tápláló oszcillátor jele közötti pontatlan fázistolás okozhatja. Hatására a konstellációs diagramban a pontok helyzete elferdül.

c) *Vivőszivárgás.* Ebben az esetben a fellépő zavaró jel és az OFDM jel középső vivőjének frekvenciája azonos. Hatására a konstellációs diagramban a pontok a hasznos- és a zavaró-jel közötti fázisszögtől függően I, vagy Q irányban eltolódnak.

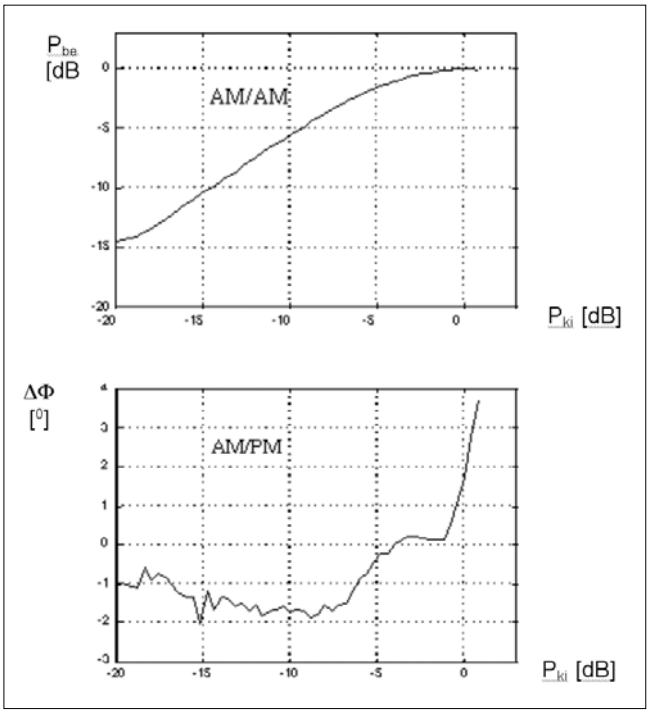
d) *Zavarójel bejutása.* A kisfrekvenciás zavarójel a hasznos vektorokkal összegeződik és a konstellációs diagramban pontok helyett körök láthatók.

e) *Zaj hozzáadódása.* A Gauss-i eloszlású zaj hozzáadódása esetén a konstellációs diagramban felhőszerű elmosódott végpont adódik. Fontos megjegyezni, hogy ilyen hatása van különböző zavaró jeleknek, mint például az intermodulációs termékeknek is.

A rádiófrekvenciás fokozatokban fellépő torzításokkal a következő szakaszokban részletesebben foglalkozunk, mivel azok részei az adó fő jellemzőinek.

A teljesítményerősítő nemlineáris torzításai

A teljesítményerősítőt alapvetően jellemzi a kis nemlineáris torzítás, a jó hatásfok és a nagy kivezérelhetőség. A nemlineáris torzítás hatása úgy a csatornán kívül, mint azon belül jelentkezik. A csatornán kívüli zavar a közeli frekvenciájú spektrumösszetevők vállcsillapítással jellemzett növekedésében és a harmonikusok megjelenésében mutatkozik. A csatornán belül hatása zajjellegű ami rontja az átviteli minőséget, a konstellációs diagramban pedig elkeni a modulációs vektorok végpontját. A nemlinearitás okozói az erősítés és a fázis szintfüggősége *(2. ábra)*.



2. ábra Erősítő AM/AM és AM/PM görbéi

Az előbbit AM-AM, az utóbbit AM-PM konverziónak is nevezik. Az AM/AM konverzió oka az tranzisztor erősítésének, az AM-PM konverzióé pedig kimenet és bemenet közötti kapacitás feszültségfüggése.

A jó hatásfok elérése érdekében az ellenütemű tranzisztorokat AB osztályú beállításban működtetik. A kivezérelhetőség azért fontos, mert a sok vivőhullámból összetett DVB-T jel esetén nagy csúcsfeszültség alakul ki. E hatás jellemzésére szolgál a csúcstényező, a Crest Factor, ami a csúcsfeszültség és az effektív feszültség arányának logaritmusa. Az elméletileg kialakuló csúcstényező a berendezésekben maximum 13 dB. A kivezérelhetőség és egyéb szempontok miatt ugyanazt az LDMOS tranzisztoros erősítőt analóg adóban 2 kW szinkroncsúcs kimenő-teljesítményre és DVB-T jelek esetén 440 W effektív teljesítményre veszik igénybe.

A kimenőszűrő lineáris torzításai

A kimenőszűrőnek a csatornán kívüli spektrum előírt tűrésábra-megvalósításához specifikálni kell a csillapítást. A csatornán belüli amplitúdó-ingadozás a körök számától, a vivőfrekvenciától és attól függ, hogy kritikus,

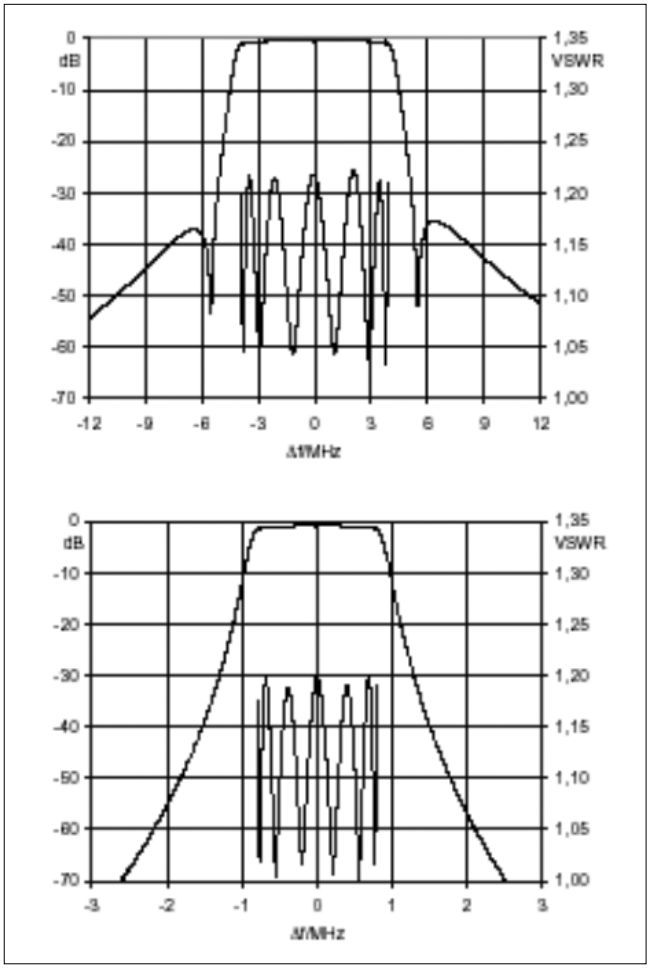
vagy nem-kritikus esethez alkalmazzák. Kritikus esetben a két sávhatáron a csillapítás 1 és 3 dB közötti, a csoportkésleltetés általában ±350 ns-nél, az állóhullámarány pedig 1,2-nél kisebb.

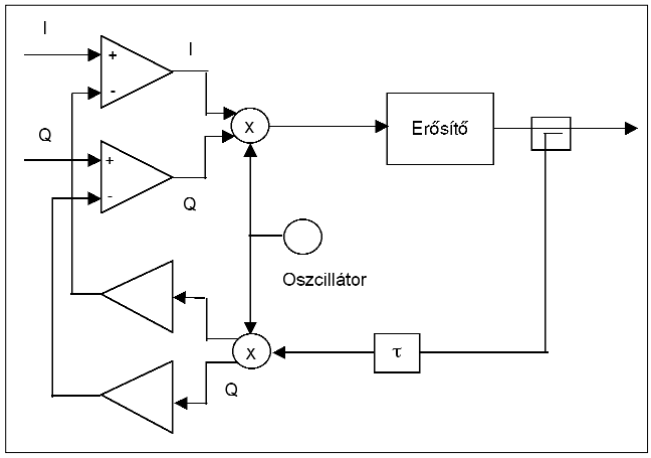
A torzítások korrekciója

A TV adóberendezéseknek a kezdeti idők óta fontos része a nagyteljesítményű fokozatok nemlineáris torzításainak kompenzálása az előtorzítással. Az analóg adókban ezt az 1960-as évektől a középfrekvenciás (KF) fokozatban valósították meg. A KF linearitás-, vagy intermodulációs-korrektor a kimenőjel torzítását csökkentette, ami a jobb jellemzők elérése mellett lehetővé tette a nagyobb kimenő-teljesítményt és hatásfokot.

Az 1969-ben üzembe helyezett hazai fejlesztésű IV. sávi, közös kép-hang erősítésű TV adóba beépített klisztronra a gyártó cég korrektor nélkül 2 kW-ot ajánlott. A szabadalmazott KF korrektorral lehetséges volt a 4 kW elérése. Közös kép-hang erősítés esetén a vizsgálójel három összetevőt, a képvivőt, az oldalsávjelet és a hangvivőt tartalmazta. A korrektort ezzel a mérőjellel kellett beállítani és az intermodulációs termék szintjét az előírt érték alá csökkenteni. A korrektor az utána következő fokozatok és első sorban a végfokozat nemli-

3. ábra IV/V. sávi 8 körös sávszűrő jelleggörbéi: nem-kritikus esetben (fent) és kritikus esetben (lent)





4. ábra Derékszögű visszacsatolás

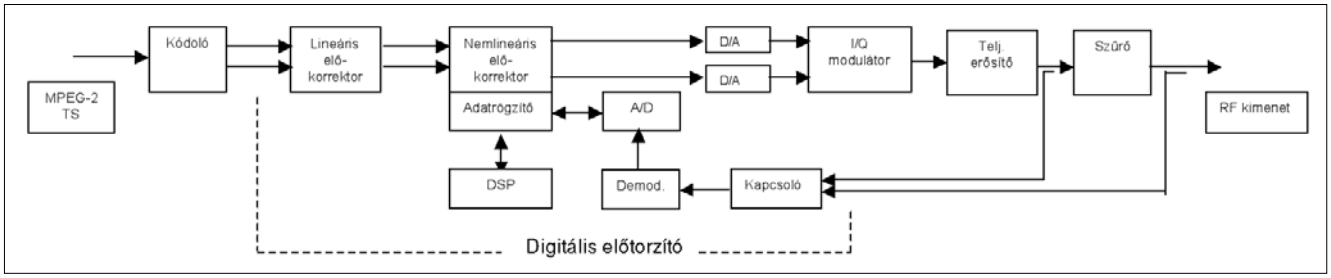
neáris karakterisztikájának inverzét valósította meg, ami a frekvenciasíkon azt jelentette, hogy azonos frekvenciájú, de ellenfázisú jeleket állított elő.

Az előtorzítókra vonatkozó, sokvivős rendszerekkel kapcsolatos kutatások több megoldást eredményeztek. A DVB-T adókban a derékszögű visszacsatolást (Cartesian Feedback) alkalmazzák *(4. ábra)*. A kimenetről kicsatolt RF jel demodulátorát és a modulátort azonos oszcillátor táplálja. Az I és a Q alapsávi bemenőjeleket a demodulátorról érkezőkkel a két műveleti erősítőben előtorzítják. Ezzel az erősítőnek mind az amplitúdó- (AM/AM), mind a fázistorzítását (AM/PM) korrigálják.

A derékszögű visszacsatolás digitális megvalósítását alkalmazza a Rohde und Schwarz cég adaptív és automatikus előtorzítójában [4,5]. A digitális megoldás az előtorzítás stabilitását eredményezi, továbbá a kezelés, a beállítás és az adatgyűjtés terén is számos előnnyel jár. A készülék alkalmas mind a félvezetős, mind pedig más, például IOT végerősítős adókhoz, így beépítik a cég tranzisztoros DVB-T adóiba. A korrektort a meghajtófokozat kódolója utáni digitális szakaszban helyezik el *(5. ábra)*.

A fejlesztők abból indultak ki, hogy a szélessávú teljesítményerősítők csak nemlineáris torzítást, a kimenőszűrők pedig csak lineáris torzítást okoznak, így célszerű volt a rendszert kettéválasztani. A nemlineáris torzítás korrektora az erősítő kimenetéről, a lineárisé a szűrő utáni mérőpontról kapja a jelet. Az erősítő kimenetéről származó jel spektruma a csatorna szélességénél szélesebb sávú és ennek eredményeként javítja a csatornán kívüli spektrumot, növeli a vállcsillapítást. A két mérőponttól érkező és az átkapcsoló által továbbított jel az előtorzító bemenő jele. A jelet demodulálják – a demodulátort ugyanarról az oszcillátorról táplálják, mint az I/Q modulátort –, majd ezután A/D átalakítóval digitalizálják és a torzítatlan bemenőjellel együtt betöltik a memóriába.

A digitális jelfeldolgozó egység (DSP) kiolvassa a memóriából a kimeneti mérőpontokról és az előtorzító bemenetéről érkezett jeleket és összehasonlítja azokat. Ennek alapján körülbelül 10 és 200 másodperc közötti kiszámítja az új korrekciós görbéket, amelyeket tárol az előtorzító memóriájában. A lineáris és a nem-line-



5. ábra Digitális előtorzító

áris előtorzítás folyamatai egymást követik. A jelek ezután a D/A átalakítókon keresztül az I/Q modulátorba kerülnek, aminek a kimenetéről a DVB-T jel a teljesítményerősítőt hajtja meg.

A korrektor a lineáris torzítások csoportjában az amplitúdó frekvenciamenet ±2 dB szélességű tartományát ±0,25 dB, a csoportkésleltetés ingadozását 500 ns-ig ±10 ns ingadozásra tudja kiegyenlíteni. A nemlineáris torzítások esetén az amplitúdó-torzítás (AM/AM) 3 dB-es és a fázistorzítás (AM/PM) 45°-os tartományát tudja korrigálni. A lineáris torzításokat a szűrő saját jellemzői mellett a külső egységek, valamint a több adót összegező szűrő és az antennarendszer együttesen határozzák meg. A lineáris előtorzítás így a külső egységek hatását is kiegyenlíti.

A korrektort kézi (manuális) üzemmódban az előlapról, vagy számítógépről vezérelhetik. Automatikus üzemmódban a számítás és a korrekciós görbe beállítása nyomógombbal indítható. Adaptív üzemmódban a működés folyamatos. A torzítások tűréshatárai beállíthatók, ezek túllépésekor az előtorzító új korrekciót állít be. A jelátvitel, tehát az adó működése mindhárom esetben megszakítás nélküli. A tranzisztoros teljesítményerősítők nemlineáris torzítása az időben állandó, ezért az előtorzítás mértéke nem változik. Más a helyzet az adócsövek, az IOT esetén, ami szükségessé teszi az előtorzítás rendszeres, vagy folyamatos beállítását, az automatikus, vagy az adaptív üzemmódot. Ugyanígy változhat a hőmérséklet ingadozásakor a szűrő által okozott lineáris torzítás is.

Irodalom

[1] MSZ EN 300 744: Digitális videoműsorszórás (DVB). A digitális földi televízió keretszerkezete, csatornakódolása és modulációja.
[2] ETSI EN 302 296: Electromagnetic compatibility and Radio spectrum Matters (ERM); Transmitting equipment for digital television broadcasting service, Terrestrial (DVB-T).
[3] Dr. Bozóki Sándor, Gelencsér István, Krémer Szabolcs: Modulációs mérések a budapesti AM-mikro rendszer digitális csatornáján, Híradástechnika, 2002/5.
[4] Reinhardt Scheide: Adaptive Digital Equalization – www.wabe.ca/papers/digital_eq.pdf
[5] Peter Mühlbacher, Cornelius Heinemann: Automatic and adaptive precorrection of digital TV transmitters – News from Rohde&Schwarz, Nr.178.
[6] DVB-T Transmission Primer www.advent.com.sg/files/white_paper.pdf

Hírek

A **HP és a Cisco Systems** a HP BladeSystem architektúrájába integrálják a Cisco kapcsolótechnológiáját, lehetővé téve a hálózat és a blade rendszer teljesítményének és megbízhatóságának optimalizálását. A Gigabit Ethernet kapcsolómodullal kibővített HP BladeSystem csökkenti az adatközponti infrastruktúra költségeit is. A rendszert hozzáigazították a Cisco Business Ready Data Center hálózati architektúrájához, így egységes hálózati szolgáltatási környezetet biztosít garantált szolgáltatásminőséggel és egyszerű felügyelettel, továbbá alacsonyabb induló kiadással jár, mint a vállalat hagyományos rackbe szerelt rendszerei, miközben az éves üzemeltetési költsége is csökken.

A **Cisco** Self-Defending Network (Önvédő Hálózat) elnevezésű biztonsági stratégiájának célja, hogy a vállalatok és intézmények hatékonyabban védhessék a hálózatba kapcsolt eszközeiket és alkalmazásaikat. Az „adaptív védelem” (Adaptive Threat Defense, ATD) stratégia többrétegű dinamikus védelmet valósít meg. Emellett egyszerűbb architektúrát és olcsóbb üzemeltetést is jelent. A Cisco stratégiájában az első fázis az IP alapú és a biztonsági technológiák ötvözése integrált védelemmé. A második fázis a Network Admission Control, amely hatékonyabban képes felismerni és megakadályozni a veszélyforrásokat és alkalmazkodni hozzájuk. Az ATD fő összetevői: a veszélyforrások elleni összehangoltabb védelmet biztosító Anti-X védelem, az alkalmazásbiztonság, valamint a hálózatvezérlés és -elszigetelés.

„Sok munka és szorgalom minden sikeres eredmény alapja”

– vallja Ladányi-Turóczy Béla a Grante Rt. vezérigazgatója

NAGY BEATRIX HAVASKA

nbh@mailbox.hu

Már több mint 20 éve kialakult Ladányi-Turóczy Béla körül egy antennatervező iskola, amely az elméleti alapokból kiindulva a gyakorlati tervezésen keresztül, egészen a gyártásig minden fázisban kiemelkedő volt. A Budavox széles távközlési palettáján egyedül képviselték a minden rádiós ajánlat elengedhetetlen részét képező antennákat és tápvonalakat. Keze alatt számos fiatal mérnök tanulta meg a szakmát és lett nemzetközileg elismert tervező. Az elmúlt 20 év a kutatások, a fejlesztések és az ipar területén óriási változásokat hozott. Kevesen mondhatják el, hogy ezt az időszakot nagyobb váltások nélkül áthidalták és ugyanazon a területen, ahol elindultak, ma is sikeresek. Érdemes utána nézni, miként sikerült ezt elérni...

Amikor látszott, hogy az állami vállalatok megszűnnek és a BUDAVOX ipari háttere is megingott, mi volt az első lépése az önállósodás felé?

Nem egyedüli érdemem, hogy az önállósodást választottuk. Az FMV-ben 1975-től egy jól képzett, szakmai tapasztalattal rendelkező csapat működött, ahol egy antennafejlesztő és mikrohullámú eszközöket fejlesztő labor is rendelkezésre állt. Az FMV 4. számú gyára volt ez a terület, ahol most vagyunk. Itt kialakult egy szakembergárda, amelyik képes volt elkészíteni azokat az eszközöket, amelyeket a labor ki fejlesztett.

A történet akkor kezdődött, amikor a Finommechanikai Vállalat átvett egy licenszet az olaszoktól, mivel addig Magyarországon professzionális antennagyártás nem létezett. A Távközlési Kutató Intézetben voltak kezdeti próbálkozások egy megbízható, nagy sorozatban gyártható antenna család kialakítására, de végül az akkori vezetők úgy döntöttek, hogy a Budavox-szal közösen az olasz GTS-től licencet vesznek. Ehhez olyan szakemberekre volt szükség, akik beindítják és biztosítják a sorozatgyártást, és akik értenek az alumíniummal kapcsolatos technológiai eljárásokhoz. Eredetileg ezen a területen repülőgép gyár működött, amelyet az idősebbik Rubik Ernő vezetett.

Az 1977-78-as években már Indiába és a volt Szovjetunióba évente több száz nagyméretű antennát szállított a gyár és elkezdődött az új mikrohullámú antennák és passzív eszközök fejlesztése. Ezzel egy időben egy troposzférikus átviteli rendszer teljes mikrohullámú részének honosítását is elvégeztük.

A vállalatnál kialakult egy olyan antenna- és tápvonal fejlesztő csapat, amelyben a kezdő mérnökök legalább 2-3 évet eltöltöttek és megtanulták a szakma tervezési- és méréstechnikai alapjait. Abban az időben a fizetések elég alacsonyak voltak mindenhol, ezért a fiatalok a szép szakmai munka lehetőségei ellenére igyekeztek más területen is szerencsét próbálni. Ennek következtében 3 évente új csapatot kellett szervezni. Természetesen mind Budapesten mind Esztergomban volt néhány szakember, akik kezdettől fogva együtt dolgoztak és több szakmailag kiemelkedő eredményt értek el.

1989-ben, az FMV az antenna termékeken kívül nem rendelkezett olyan saját gyártmánnyal, amely a világpiacon eladható lett volna. Ekkor bomlott fel a Varsói Szerződés és a KGST, aminek következtében az FMV polgári- és katonai gyártmányai eladhatatlanná váltak. Milliárdok álltak késztermékekben, amiket nem lehetett értékesíteni. Az antennatechnikában viszont több mint tízéves tapasztalat gyűlt össze mind a saját fejlesztés, mind a sorozatgyártás területén, így képesek voltunk megjelenni a piacon és ezzel lehetőségünk nyílt egy saját cég alapítására. Egyik kollegámnak – aki ennek a cégnek előttem vezérigazgatója volt – több éves, az ÁPV Rt-vel és az FMV vezetésével folytatott kemény küzdelemben sikerült elérni, hogy a gyáregység önállóvá váljék.

A kitartás, a szerencse, az ismeretségek és szakmai kapcsolatok révén mindjárt a Grante Rt. megalakulása után sikerült bekerülni a Westel 450 Rt. beszállítói közé. Kezdetben a megmaradt műszerpark segítségével 15 GHz-ig jutottunk, jelenleg már 40 GHz-nél tartunk. A gyártmányválasztékot folyamatosan és rendkívül gyorsan bővíteni kellett. Ma elmondhatom, hogy termékeink 90%-a öt évnél fiatalabb. A tudás és a szerencse párosult –, ez a siker titka.

Soha nem érezte, hogy egy mérnök, aki nagyvállalati keretek között nevelkedett és biztos háttérrel dolgozhatott ki új módszereket és tervezhetett önállóan antennákat, annak kockázatos üzleti területen kísérletezni?

1968-ban, amikor az egyetem elvégzése után az Elektromechanikai Vállalathoz kerültem, a cég fő tevékenysége az volt, hogy egy országos URH és televíziós hálózatot valamint a Jászberényi Rövidhullámú Rádióállomást a Magyar Posta részére kiépítse. Fiatal mérnökként feladatom a tervezés, a konstrukció kialakítása, a szerkesztők segítése volt, majd az antennák gyártatásában, bemérésében, a telepítésben és az átadásban is dolgoztam. Tehát a nullától egészen a befejezésig részt vettem a folyamatban. Így megszoktam, hogy mindent magunknak kellett elkészíteni.

1975-ig dolgoztam ott, 1971-től laborvezetőként. Az EMV-ben eltöltött hét év alatt kitűnő szakemberekkel dolgozhattam együtt, akiktől megtanultam a fejlesztési munkákkal együtt járó kudarcok elviselését, a munkatársak között elkerülhetetlenül fellépő konfliktusok kezelését, a szakmai célok elérésének útjait és a felelősségérzetet. Mindazt, amit a munkatársakkal szemben egy vezetőnek ki kell fejleszteni magában.

Az FMV-nél más volt a helyzet, ott a telepítésekkel nem kellett foglalkoznunk. Egy ekkora vállalat fejlesztési intézetében dolgozni azzal az előnnyel járt, hogy sokkal több idő jutott az elmélet kérdéseiben való elmélyülésre, de az új fejlesztések elé a vállalat vezetése állandóan korlátokat állított. Ez azt jelentette, hogy bizonyos elképzeléseket csak hosszú idő alatt tudtunk megvalósítani, és az energia egy részét a vállalat vezetőivel folytatott küzdelem emésztette fel.

A rendszerváltozáskor lehetőség volt arra, hogy elmenjek egy nagy multinacionális céghez, de az megint azzal a hátránnyal járt volna, hogy olyan főnökeim lesznek, akik nem értenek az adott szakterülethez. A másik hátrány az, hogy egy nagyvállalat hihetetlenül nehézkes. Nagyon sok a döntési lépcső, bizonyos irányvonal működik és egyedi igényekkel nem foglalkoznak. Magyarországon és máshol is a kis cégeknek az a nagy előnye, hogy rugalmasak és olyan igényekre is mozdulnak, amiket ezek a nagy cégek nem elégítenek ki. Ezt a stratégiát mi is sikeresen alkalmazzuk.

A vezetése alatt jelenleg egy több mint százfős vállalat tervezi és gyártja a legkorszerűbb antennákat. Mikor határozta el, hogy önállósítja magát és telepedik le Esztergomban?

Nagy variációs lehetőség nem volt, azt kellett eldönteni, hogy más területre megyek, vagy maradok ennél a csapatnál. Miután ez a szakembergárda már 15 éven keresztül bizonyított, és ezek az emberek úgy döntöttek, hogy maradnak. Akiknek a változás nem tetszett, azok elmentek más cégekhez, de a szakmai munka folytatása nem okozott gondot.

Azért vagyunk Esztergomban, mert szakembereink nagyobb része a környéken lakik és rendelkezünk egy mikrohullámú antennák mérésére alkalmas teleppel. Itt minden olyan feltétel megvan a professzionális munkához, fejlesztéshez. Nincs értelme, hogy a cég bármely részét elköltöztessük, mert akkor bizonyos feltételek hiányoznának. Az itteni antenna mérőszakasz kitűnő lehetőséget biztosít a zavartatásmentes mérések elvégzéséhez. Ezt a területet elődeink két év alatt választották ki, és itt még ma is ideálisak a feltételek.

Az állami vállalat keretei között híres volt arról, hogy környezetében olyan fiatalok nevelkednek, akik kreatívak és ötleteiket együttes erővel keresztül is viszik. Folytatódik-e ez a nevelő munka, és vannak-e tudományos ambíciójú mérnökök a környezetében?

Mint már említettem, 2-3 évente cserélődött az ifjú szakemberek egy része, akik beletanultak a szakmába, majd más vállalkozásokhoz mentek át, mivel egy kisvállalat nem tudja azokat az anyagi feltételeket biztosítani, mint a multinacionális cégek. A régi munkatársakkal a jó kapcsolat természetesen megmaradt. Amikor elmegyek bármely távközlési céghez, akkor középvezetői vagy felsővezetői pozícióban találok olyan szakembereket, akikkel valamikor együtt dolgoztam, vagy szakmérnöki tanulmányaik közben tanítottam őket. Jelenleg is van egy végzős hallgató, aki együttműködik az idősebb mérnökökkel, akik a fejlesztési munkákat és beméréseket végzik, így a szakma igazi mélységeit is megtanulja, és nemcsak számítógépes programokon keresztül ismeri meg a mikrohullámú antennák csodálatos világát.

Nálunk az alapkoncepció, hogy minden információt megosztunk egymás között. Az igény beérkezése után azt közösen értékeljük, megbeszéljük, előzetes számításokat végzünk. Amikor a konstrukció közelébe érünk, akkor a fejlesztő szakemberek és az előzetes munkákat végző munkatársak közösen teszik meg a befejezéshez szükséges utolsó lépéseket. A munkamódszer itt más, mint egy nagyvállalatnál. Állandó az információcsere, az ötleteket megbeszéljük még akkor is, ha azok rosszak, mert még egy rossz ötlet is tartalmazhat olyan hasznos részletet, amit később fel lehet használni.

Természetesen a fejlesztések nem mindegyikéből lesz piacképes termék. Azt mondják, hogy ha tízből egy sikeres lesz, az már jó eredmény. Nálunk véleményem szerint ennél sokkal jobb az arány. Ehhez nagy segítséget nyújt a szakirodalom, amit folyamatosan olvasni kell, az Internet, és a mostani és régi kollegákkal folytatott szakmai beszélgetések is sokat jelenthetnek. Mindenre szükségünk van ahhoz ahhoz, hogy olyan termékekkel jelenjünk meg, amelyek versenyképesek lehetnek a világpiacon.

Kevés vállalkozás tudja a kutatást, fejlesztést, gyártást és értékesítést sikeresen összhangba hozni. Az első kettő elhagyása néhány év alatt rendkívül nehézzé teszi a termékek értékesítését. A Grante éppen az újdonságokkal tudja folyamatosan növelni sikerét. Kifejezhető az, hogy a négy feladat közül melyikre mennyi időt, energiát, szakembert fordít?

Ez egy kulcskérdés. Vannak időszakok, amikor a piac igénye csekély. Az elmúlt néhány évben a távközlés fejlődése lelassult, így lehetőségünk nyílt arra, hogy az új termékek fejlesztésére jobban koncentráljunk. Ennek következtében hatékonyabban és gyorsabban tudtunk új konstrukciókat kidolgozni. 2004 eleje óta azonban a piaci igények újra nőnek, így az elmúlt időszakban a fejlesztés kissé háttérbe szorult. Vannak új ötletek, de kevesebb idő jut azok realizálására. Az időbeosztás is megváltozott, sokszor háromféle feladatot kell végezni egyszerre, mindegyikkel folyamatosan kell foglalkozni: a fejlesztéssel, a marketinggel, és figyelni, hogy a világ merrefelé halad. De mindig máson van a hangsúly. Magam is besegítek a konstrukció kialakításába, nemcsak az elméleti háttérrel foglalkozom, amikor pedig tendert kell írni, akkor annak koordinálása a fő feladatom.

Folyamatosan figyelni kell a távközlés fejlődésének tendenciáit. Az IEEE anyagait, a külföldi szakmai folyóiratokat folyamatosan olvassuk, az Internetről is sok hasznos információt szerzünk. Kialakítottunk egy adatbázist, amelyben az összes, szakterületünket érintő és hozzáférhető magyar- és külföldi szakmai publikáció, újdonság megtalálható, így ha valamilyen információra szükségem van, pillanatokon belül meg tudom keresni az ide vonatkozó adatokat. A keresési idő minimalizálásához az anyagok rendszerezve, katalogizálva vannak. Munkatársaim egy része az adatbázis bővítésével és kezelésével foglalkozik.

Vállalati struktúra, szakmai tudás, a világ szakirodalmának figyelése – mind hozzájárul a cég fejlődéséhez. Van-e ezek közül valamelyiknek kiemelt szerepe a vállalatnál?

A vállalati struktúra az elmúlt pár évben kialakult. Örököltük az FMV-től azt a szakember gárdát, amely részvénytársaságunk gerincét képezi, és sikerült fiatalokat is integrálni a szervezetbe. A munkatársak egy része nem tudta felvenni azt a ritmust, amit a dinamikus gyártmányfejlesztés és a naponta változó piaci igények megkívánnak, ezért át kellett alakítani a cég szervezeti felépítését, másrészt a piaci igények időszakos beszűkülése miatt csökkenteni kellett a létszámot.

Az elmúlt három évben a távközlésben bekövetkezett piaci változások hatására a mikrohullámú antennák ára csökkenni kezdett. A gazdasági gondokat részben további létszámcsökkentéssel, döntően pedig új, piacképes gyártmányok (például Wireless Internet antennák, kompakt tartalékolt rendszerek stb.) kifejlesztésével oldottuk meg. A vállalati struktúrát folyamatosan hozzá kell igazítani a piac igényeihez.

Műszaki igazgatónk irányítja a termelést, koordinálja a szállításokat, az anyagbeszerzést és felügyeli a szerkesztést. Gazdasági igazgatónk feladata a cég pénzügyi stabilitásának biztosítása, humánpolitikai igazgatónk foglalkozik a dolgozók személyes gondjaival és a Grante Rt. szállodájának és éttermének irányításával. A fejlesztési munkákat magam tartom kézben, én határozom meg a stratégiai irányokat és ápolom az üzleti kapcsolatokat.

Az új termékek gyors kifejlesztésére kényszerít bennünket, hogy a hazai piacon is a világ vezető antennagyártó cégeivel kell megküzdenünk.

Egy vállalat főnökének, szakmai vezetőjének elegendő-e a napi 24 óra feladatai teljesítéséhez?

Attól függ, hogy mit veszünk munkának. Természetesen a 24 órának elegendőnek kell lennie. Megválogatom, hogy mire fordítom az időmet. Napi 6-7 óra alvás, minden nap egy kis mozgás, ami részben kompenzálja az irodai munka statikusságát. Domináns a munkahelyen eltöltött idő, és a gondolkodás. Este elolvasom az újságokat és néha még szépirodalomra is marad idő, melyet alkalmasint komolyzenehallgatás egészíti ki.

Nyaralásra, hosszabb szabadságra nincs lehetőség. Kis cég vezetőjeként nem hagyhatom magára munkatársaimat hosszabb időre. Az ünnepek környékén és nyáron azért pár napot szakítok a kikapcsolódásra, de a mobiltelefon természetesen mindig kéznél van. Sok munka és szorgalom minden siker alapja.

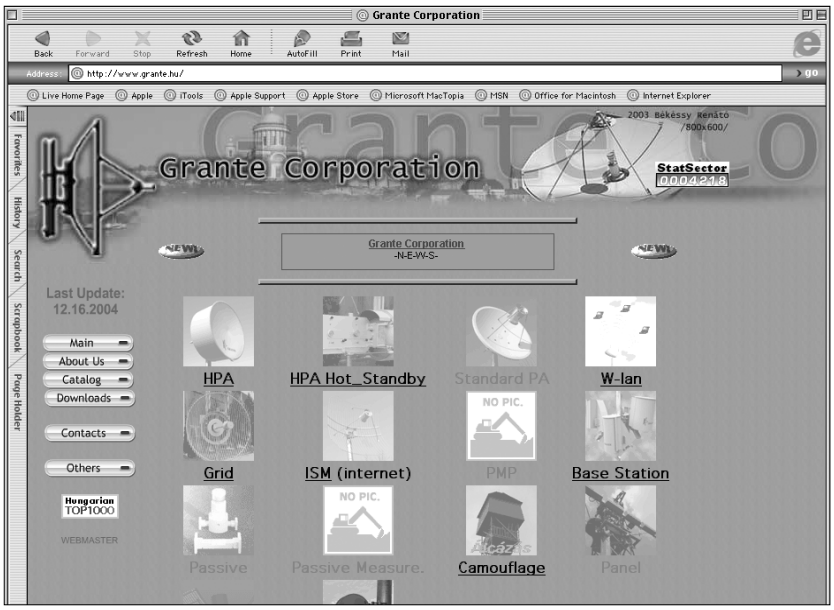
A kérdésekből talán látszik, hogy igyekeztünk valami nagy titoknak a megszerzésére és közreadására. Valószínűleg az igazi titkot ezekből a kérdésekből nem tudjuk meg. Ezért utoljára azt szeretném kérdezni, hogy mi a tudomány és az üzlet összehangolásának, a változások kezelésének, – összefoglalóan Ladányi-Turóczy Béla nagy titka?

Nagyon fontos a lehetőségek maximális kihasználása, a tapasztalatok gyűjtése, a fejlesztési eredmények és kudarcok precíz dokumentálása. Minden véleményt meg kell hallgatni, a szakemberek természetes kíváncsiságát ki kell használni, el kell ismerni a különleges tudást, érzékeltetni a munkatársakkal, hogy véleményük és tapasztalatuk rendkívül fontos. Gyorsan és határozottan kell dönteni.

A vezeték nélküli távközlés aranykorát éli, oda kell figyelni minden apró jelre, információra, újdonságra. Figyelni kell a világra, be kell kapcsolódni a körforgásba és napra késznek kell lenni.

Részvénytársaságunk valódi értéke nem az infrastruktúrában, a rendelkezésre álló gépekben és műszerekben, hanem a munkatársak fejében, kezében, az évtizedek alatt felhalmozott tapasztalatokban, szakmai és emberi kapcsolatokban van. Ezekkel kell minél hatékonyabban gazdálkodnunk, mert ez teszi lehetővé hogy hosszú távon is sikeresen szerepeljünk a rendkívül gyorsan változó világban.

A Grante Rt. honlapja



Az m-kormányzat biztonsági kérdései és lehetőségei

FAIGL, ZOLTÁN, IMRE SÁNDOR
BME Híradástechnikai Tanszék, imre@hit.hit.bme.hu
BUDAI BALÁZS
BKAE Közigazgatás-szervezési és Urbanisztikai Tanszék, E-government kutatócsoport
balazs.budai@e-government.hu

Kulcsszavak: adatvédelem, mobil tranzakciók, elektronikus aláírás, hitelesítés

A közigazgatás modernizálásának egyik kiemelkedő feladata az informatika bevonása, melynek fejlesztő hatásai megkérdőjelezhetetlenek, azonban ezekért az innovatív eredményekért nem áldozhatunk fel két alapvető dolgot, nevezetesen az adatbiztonságot és az adatvédelmet. A cikk áttekintést ad a mobil adminisztráció bevezetésének lehetőségeiről, technikai és törvényi szempontból is érzékelteti az ezzel járó kihívásokat. A lehetséges alkalmazási területek között részletesebben szerepel a mobil tranzakciók használata a közigazgatási ügyekben. Hangsúlyt kaptak azok a felhasználó-hitelesítési és elektronikus aláírás képzési sémák, amelyeket a mobil adminisztrációban alkalmazni lehet. Végül a szerzők nyitott tervezési kérdésekre, nevezetesen a megfelelő biztonságpolitikák és tanúsítványfajták kialakítására hívják fel a figyelmet.

Számos motiváló tényezője van a mobil kormányzat bevezetésének. Ma még hazánkban az 1957. évi Államigazgatási Eljárásról szóló törvény fogalmazza meg a közigazgatási eljárások formai követelményeit. Kidolgozás alatt áll a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló törvény (KET) tervezete, ami lehetővé teszi majd az elektronikus út, így a mobil csatorna használatát is közigazgatási eljárásokban.

Az m-governement és m-commerce fejlődési folyamatában fontos motiváló tényezőként hatnak azok az EU-s direktívák és ajánlások, amelyek elektronikus ügyintézés lehetőségének bevezetését szorgalmazzák hatósági eljárásokban. Kiemelkedően fontos ezek között az elektronikus aláírás elfogadásáról és bevezetéséről szóló EU direktíva [1], valamint az eEurope akciótervek visszatérő eleme, a „Common List of Basic Public Services" (CLBPS) című dokumentum [2].

A cikk első részében bemutatjuk, miért és milyen feladatra célszerű mobiltelefont használni, a második részben összefoglaljuk, milyen esetekben indokolt a mobil csatorna alkalmazása a KET és CLBPS alapján a közigazgatásban és különböző hivatalos szerveknél. A harmadik részben leírjuk azokat a lehetséges módokat, ahogy a mobil csatorna beilleszkedhet egy ügymenetbe. A negyedik részben kitekintést adunk technológiai kérdéseken túlmutató rendszertervezési elvekre, amelyeket figyelembe kell venni, amikor elektronikus közigazgatási vagy más, széleskörűen elérhető, bizalmas jelleggel bíró elektronikus tranzakciókat vezetünk be.

1. A mobil technológia indokoltsága

A Nemzeti Hírközlési Hatóság 2004. májusi gyorsjelentése 8 145 298 aktív SIM kártyáról ad számot [3]. A legalacsonyabb kategóriájú készülékek is rendelkeznek SMS küldésen túl WAP képességgel. A technológia kellőképpen érett olyan újszerű szolgáltatások bevezetésére, ahol fontos a felek egyértelmű hitelesítése és a bizalmas kapcsolat megteremtése.

E szolgáltatások a WPKI (Wireless Public Key Infrastructure) technológián alapulnak, amely megfelel az internetes PKI infrastruktúrának, azzal a különbséggel, hogy a tanúsítványok formátumát és a tanúsítványszerzés menetét a kis sávszélességű, és a kis tárolási, számítási kapacitású mobil technikára adaptálták [19].

A mobiltelefon és hálózat két módon illeszkedhet be egy elektronikus üzleti modellbe:

– csatornát szolgáltat biztonságos partnerhitelesítéshez, felhasználó-azonosításhoz,
– megvalósíthatja a felhasználó-oldali digitális aláírást, az elektronikus aláírásról szóló törvénynek megfelelően.

Ez alatt a következőt értjük:

A felhasználó-azonosítás célja, hogy a rendszer ellenőrizni tudja egy adott személy jogosultságait, ez az első lépés egy bizalmas tranzakció lebonyolítása során. A digitális aláírás alatt a hosszú távon letagadhatatlan aláírást értjük. Számtalan esetben alkalmazhatunk elektronikus aláírást. A körülményektől függ, hogy mennyi idő múlva, mennyi ideig kell érvényesnek maradnia (szélsőséges példa erre a végrendelet), vagy milyen ügymenetben, milyen szereppel alkalmazzák (állampolgár, vállalatvezető, közjegyző, cégpecsét). Minden eset más és más követelményeket támaszt az aláírás hitelességét, letagadhatatlanságát, érvényességi idejét illetően.

A mobil elektronikus aláírásnak és felhasználó-azonosításnak széles felvevő piaca létezik, ezek közül az egyik az m-kormányzat, ahol a hatóságok kapcsolatba lépnek az állampolgárral. Ha GSM, vagy a közeljövőben elterjedő UMTS rendszeren keresztül végezzük az előfizetők azonosítását és a hozzáférés-engedélyezését, a rendszer kellőképpen biztonságosnak tekinthető. A biztonsági funkciót megtestesítő SIM kártyák kiosztása és felügyelete megfelelő keretek között zajlik. Az előfizetők személyes adatai – más néven identitás

információk [5] – a szükséges mértékben védettek. Következésképpen, a megbízható elektronikus tranzakciókhoz érdemes GSM/UMTS vagy más cellás rendszereket igénybe venni. A felhasználó-azonosításhoz és a digitális aláírás képzéséhez tipikusan kis sávszélességre van szükség, ezért elég a GSM adatátviteli sebessége.

A mobilszolgáltatók számára az új kihívást – amelyet a versenyképesség fenntartása, és a felhasználók kényelmesebb kiszolgálása diktál – a személyes adatok (identitás információk) és egyéb bizalmas információk elektronikus úton való közlése jelenti. Idegen mobil hálózatban a felhasználó azonosítása és hitelesítése úgynevezett identitás-roaminggal fog történni [7].

Számos nemzetközi szakmai szervezet alakult a 90-es évek végétől, amely a megbízható elektronikus tranzakciók kidolgozásán, az identitás információk biztonságos átvitelén dolgozik. Tagjaik általában mobilszolgáltatók, pénzügyi intézmények, kutató-, fejlesztő és szabványosítási szervezetek és fórumok. Tevékenységükről az *1. táblázatban* található összefoglalás.

2. Elektronikus ügymenetmozzanatok mobil csatornán keresztül

A mobil csatornán történő tranzakciókat sok területen fel lehet használni, banki szolgáltatások esetén beszélünk m-bankingról, adminisztratív jellegű feladatok végzésénél m-adminisztrációról, közigazgatásban zajló ügymenetek felváltásánál m-kormányzatról, és még sorolhatnánk. Ebben a fejezetben, a közigazgatásban bevezethető mobil szolgáltatásokat szemléltetjük.

Az első számú kérdés, hogy a közigazgatási eljárások mely mozzanatai válthatók ki mobiltelefonos tranzakció segítségével. A hazai jogszabályok és EU direktívák melyek használatát teszik lehetővé? M-kormányzat szintjén a közeljövőben bevezetendő „Közigazgatási hatósági eljárás és szolgáltatás általános szabályairól szóló törvény” (KET). Ez és a hozzá kapcsolódó kormányrendeletek határozzák meg a közigazgatási eljárások formai követelményeit – például milyen adatokat kell tartalmaznia egy kérelemnek – illetve garanciális szabályokat fogalmaz meg az ügymenetek sértetlenségére, bizalmasságára, és az állampolgár jogaira vonatkozóan. A KET műszaki szempontból kiindulópontot jelent az elektronikus ügymenetek biztonságpolitikájának kidolgozásához (lásd 4. fejezet).

A KET tervezete szerint a *2. táblázatban* felsorolt eljárási mozzanatokban lehetséges az elektronikus kapcsolattartás. A felsoroltak közül a mobil technológia alkalmazása elsősorban a kérelem, tájékoztatás, az értesítés, idézés és a felhívás területén lehetséges.

1. táblázat Megbízható mobil elektronikus tranzakciókat specifikáló szervezetek

Név	Alapítás	Tagok	Célja
Radicchio (T^2R) [8]	2002 március	GSMA, Liberty Alliance, ETSI	Globális identitás-menedzsment platform kidolgozása.
Liberty Alliance [9]	2001 szept.	VeriSign, Nokia, Sun, RSA, Vodafone, American Express, Novell	Identitás alapú webes szolgáltatások kialakítása, ún. *federated identity management* specifikálása.
GSMA [10]	1987	GSM szolgáltatók	Nemzetközi szintű kapcsolatok kiépítése pénzügyi szervezetek és GSM szolgáltatók között.
ETSI (M-COMM) [11]	2000 április	M-COMM Working Group	Elektronikus úton történő aláírást és fizetést végrehajtó rendszerek követelményeinek kidolgozása.
MPSA (SimPay) [12]	2003 március	Vodafone, T-Mobile, Orange, Telefónica Móviles	Globális micropayment rendszer kialakítása.
Mobey Forum [13]	2000 május	VISA, ABN-Amro Bank, Nokia, Deutsche Bank	Mobil fizetési rendszer kialakítása, m-payment, m-brokeraging, m-banking szolgáltatások.
MeT [14]	2000 április	NEC, Nokia, Panasonic, SonyEricsson	WAP-os szolgáltatások kialakítása, mobil tranzakciók kidolgozása.
PayCircle [15]	2002 február	HP, Siemens	M-payment szolgáltatás kialakítása.
Mobile Payment Forum (MPF) [17]	2001 november	American Express, JBC Co. Ltd., MasterCard International, Visa International	M-payment szolgáltatás kialakítása.
Open Mobile Alliance (OMA) [16]	2002 június	Vodafone, Ericsson, WAP Forum, IT vállalatok	Műszaki előírásokat fogalmaz meg a mobil kommunikáció területén használt alkalmazásokra és szolgáltatásokra vonatkozólag.

2. táblázat Az állampolgár és a hatóság kapcsolatfelvételével járó eljárási mozzanatok a közigazgatásban

a) kérelem, fellebbezési kérelem, újrafelvételi kérelem, méltányossági kérelem és a jogszabályban előírt mellékleteik benyújtása,
b) jogsegély iránti kérelem és annak teljesítése,
c) hiánypótlási felhívás és a hiánypótlás,
d) az eljárás irataiba való betekintés,
e) idézés,
f) igazolási kérelem előterjesztése,
g) ügyfél nyilatkozata, bejelentése, a hatósághoz intézett beadványa,
h) bizonyítékok ügyfél elé tárásának határnapját tartalmazó felhívás,
i) felügyeleti szerv eljárásához szükséges iratok felterjesztésére szóló felhívás,
j) az ügyfél tájékoztatására, értesítésére és felhívására vonatkozó egyéb hatósági közléseknek az ügyfél tudomására hozása,
k) a döntés közlése

A mobiltelefon minden olyan területen használható, ahol az adott szerv az elektronikus út használatát lehetővé teszi. Az eEurope akcióterv fontos dokumentuma – a „Common List of Basic Public Services (CLBPS)” – 20 ilyen elemet foglal össze: tizenkettőt az állampolgárnak és négyet az üzleti szférának szántak közül.

A *3. táblázatban* a kiemelt elemek egészben a többi eljárás csak részben tartalmazza a felhívás, kérelem, tájékoztatás, idézés vagy értesítés mozzanatot. Látható, hogy a közigazgatási eljárásoknál bevált, kormány-rendelkezésben megfogalmazott elektronikus ügymenet az üzleti szférában, vagy más hivatalos szerveknél is jól hasznosítható.

3. A mobil csatorna alkalmazási módozatai

Ebben a fejezetben bemutatjuk a mobil csatorna alkalmazási lehetőségeit az elektronikus eljárásokban. Az itt leírt tranzakciók csak ügymenetmozzanatok, általában az eljárás fennmaradó része Interneten keresztül, vagy hagyományos ügyintézéssel zajlik.

3.1. Felhasználó-hitelesítési módozatok

A felhasználó-hitelesítési lehetőségeket önkényesen, az azonosításhoz szükséges tényezők száma alapján csoportosítottuk.

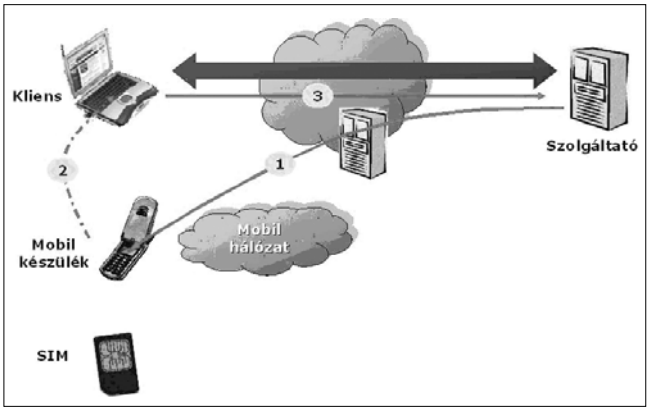
Személyes információ alapján történő hitelesítésnél

egyetlen tényező, a jelszó (például PIN kód) ismerete szükséges csak ahhoz, hogy a felhasználó azonosítsa magát. Statikus jelszavak használata köztudottan sebezhetővé teszi a felhasználó-azonosítást, mivel a jelszó nyilvánossá válásának valószínűsége folyamatosan növekszik az idő múlásával. Ebből fakadt az ötlet, hogy jobb lenne minden jelszót csak egyszer használni, majd használat után eldobni.

Az *egyszer használatos jelszavak (One-Time-Password, OTP)*, kiosztását és változását valamilyen módszerrel szinkronizálni kell a szolgáltató és a felhasználó között. Ha nem elég biztonságos az átviteli csatorna, nyilvánvaló, hogy a két oldal nem küldheti el egymásnak az új jelszót. Ilyen esetben chipkártyára, vagy más intelligens eszközre ültetett, megbízható számlálóval vagy időzítővel szokták megoldani a jelszavak változásának összehangolását.

A GSM, UMTS és más mobil hálózatok kellő biztonságot nyújtanak ahhoz, hogy egyszer használatos jelszót küldjünk a felhasználó mobil telefonjára. Az *1. ábrán* látható esetben a szolgáltató titkosítás nélkül küldi át a jelszót. A felhasználó elolvassa a kijelzőn, és begépeli a számítógépén a jelszót, hogy azonosítsa magát a szolgáltató portálján.

E megoldás biztonsága a mobil hálózat (GSM, UMTS) titkosításán és hitelesítésén alapszik. A statikus jelszavas módszereknél megbízhatóbban hitelesíti a felhasználót. A jelszó például SMS formájában érkezik az előzetesen regisztrált SIM kártyára. A mobil telefonszám egyértelműen azonosítja a SIM kártyát. A jelszó csak a SIM kártyát tartalmazó készülék képernyőjén olvasható, így illetéktelen kezekbe csak úgy kerülhet, ha a SIM kártyát, vagy a SIM-et tartalmazó készüléket elveszítik/eltulajdonítják, és a tulajdonos nem tiltatja azt le.



1. ábra Egyszer használatos jelszó (OTP) kiosztása nyíltan

Kis és közepes jelentőségű tranzakcióknál (például banki szolgáltatások) érdemes bevezetni e megoldást. Előnye, hogy minimális költséggel megvalósítható, a SIM kártya pedig nem igényel változtatást.

Kulcs és személyes információ alapján történő azonosításnál és hitelesítésnél

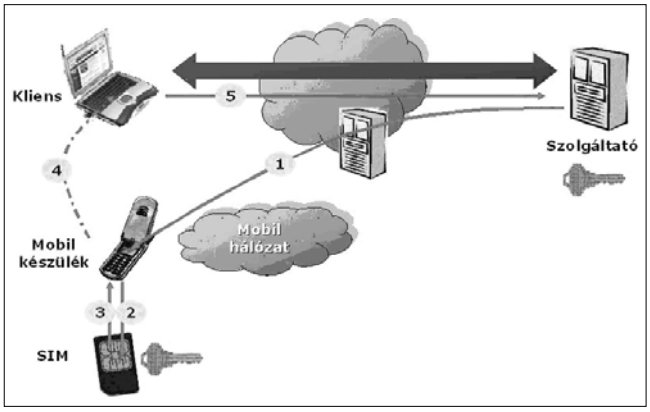
két tényező együttes megléte szükséges: birtokolni kell egy kulcsot (nem egyezik a GSM titkos kulcscsal), és ismerni kell egy PIN kódot (eltér a GSM PIN kódtól). A háttérben jelen van a mobil hálózat által nyújtott előfizető-hitelesítés és titkosítás a rádiós csatornán.

A *titkosított OTP kiosztás* mechanizmusa megegyezik az előző esettel, de megsokszorozza a felhasználó-hitelességének erejét azzal, hogy feltételezi, hogy a SIM kártyáján jelen van a titkos kulcs, amely hatását csak a megfelelő PIN kód ismeretében képes aktiválni a felhasználó. A szolgáltató oldalán tárolni kell a titkos kulcsot. Az egyszer használatos titkosított jelszó kiosztást a *2. ábra* szemlélteti (a következő oldalon).

A második lépés során a SIM kártya bekéri a PIN kódot a felhasználótól, és ha az megfelelő, akkor a harmadik lépésben megjeleníti a kijelzőn a jelszót. A PIN ismerete nélkül a jelszó nem válik olvashatóvá. A módszer biztonságát a PIN ismerete adja, jóval biztonságosabb nyílt OTP kiosztásnál. Ha a mobil készülék támadó kezébe kerül, nem tudja megszemélyesíteni a felhasználót, amíg nem ismeri a PIN kódot. A titkosított OTP kiosztáson alapuló felhasználó-hitelesítés már komolyabb elektronikus tranzakciók hozzáférés-engedélyezési részét is képezheti. A második lépésben sebezhető a módszer, ha a PIN

AZ ÁLLAMPOLGÁROK SZÁMÁRA NYÚJTOTT SZOLGÁLTATÁSOK	AZ ÜZLETI SZFÉRÁNAK NYÚJTOTT SZOLGÁLTATÁSOK
1. Jövedelemadó: adóbevallás megtétele, értesítés a kivetett adóról	13. Munkavállalók után befizetett hozzájárulások
2. Álláskeresés: munkaügyi hivatalok	**14. Társasági adó**
3. Társadalombiztosítási kifizetések (legalább három az alábbi négy lehetőség közül) - munkanélküliek járadékai - gyermekek után járó pótlékok - gyógyászati költségek - tanulói ösztöndíjak	**15. Általános forgalmi adó**
4. Személyi dokumentumok: útlevél, gépjárművezetői jogosítvány	**16. Új társaság bejegyzése**
5. Gépkocsik nyilvántartásba vétele: új, használt, importált autók	**17. Adatközlés a statisztikai hivatalnak**
6. Építési engedély kérelem	18. Vámnyilatkozat
7. A rendőrségnek tett bejelentések: pl. lopás esetében	19. Környezetvédelemmel összefüggő engedélyek
8. Közkönyvtárak: katalógusokhoz, keresési lehetőségekhez való hozzáférés	20. Közbeszerzés
9. Születési és házassági bizonyítványok: kérelmezésük és kiadásuk	
10. Felsőbb oktatásba történő jelentkezés (ide értve az egyetemeket is)	
11. Költözés bejelentése: lakcímváltozás	
12. Egészséggüggyel összefüggő szolgáltatások: pl. interaktív tanácskérési lehetőség a különböző kórházi szolgáltatások elérhetőségéről, kórházi bejelentkezések	

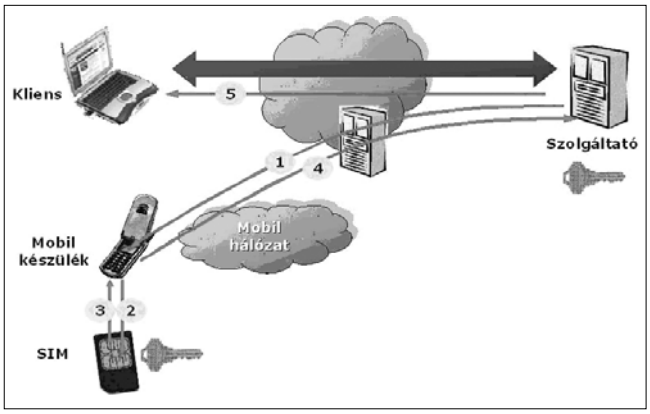
3. táblázat Common List of Basic Public Services (CLBPS)



2. ábra Egyszer használatos jelszó kiosztása titkosítva

kódot leolvassák, és a SIM kártyát (vagy a telefont) eltulajdonítják. A megoldás bevezetéséhez a SIM kártyát alkalmassá kell tenni a fenti műveletek elvégzéséhez (ki kell cserélni/át kell programozni). Az új SIM kártyára fel kell tölteni az azonosításra használt kulcsot és algoritmust. A kulcsok kezelése, érvényességük ellenőrzése extra komponenseket kíván a szerver oldalon is.

Kihívás-válasz mechanizmus alkalmazása esetében a szolgáltató egy kihívást generál, amelyre megfelelően kell válaszolnia a felhasználónak. Csak a megfelelő kulcs birtokában adhat jó választ a felhasználó. A válasz képzése történhet titkosítással, vagy bármilyen más kulcs alapú eljárással, például aláírás képzéssel. A *3. ábra* szemlélteti ezt a lehetőséget.

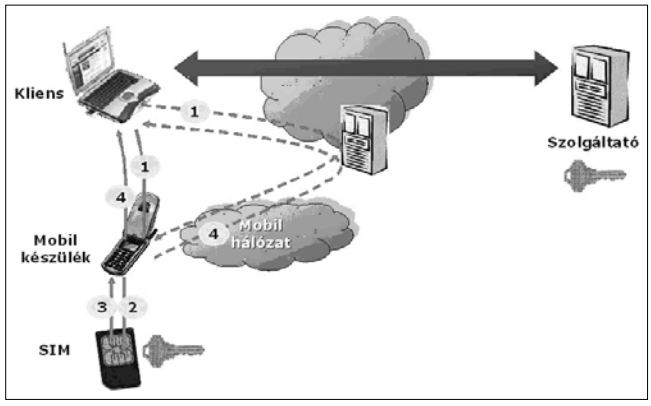


3. ábra Hitelesítés kihívás-válasz algoritmussal

Az eddig leírt felhasználó-hitelesítési lehetőségek közül ez a legbiztonságosabb. A hitelesítés erőssége persze függ a kulcshossztól, a kihívás-válasz algoritmus megválasztásától. Nagy biztonsági szintű, hosszútávon letagadhatatlan felhasználó-azonosítást eredményez, ha az üzeneteket megfelelően naplózzák és tárolják mind a hálózatban, mind a mobiltelefonon. A megoldás bevezetéséhez le kell cserélni/át kell programozni a SIM kártyákat és meg kell teremteni a kulcsok kezeléséhez szükséges infrastruktúrát.

Egycsatornás hitelesítés, kihívás-válasz alkalmazásával

Az előző esetekben a szolgáltató vette fel a kapcsolatot a felhasználó mobil készülékével és számítógépével is, ezáltal kétcsatornás megoldásról beszélhettünk. Elképzelhetőek olyan módszerek is, ahol a felhasználó számítógépe épít ki kapcsolatot a mobil készülékkel, mintegy smartkártya olvasóként használja. A szolgáltatónak ilyen esetekben csak a számítógéppel kell kapcsolatba lépnie, vagyis a felhasználó-hitelesítés egycsatornás [6] *(4. ábra)*.



4. ábra Egycsatornás, kihívás-válasz alapú hitelesítés

A kliens gépnek el kell érni a mobil telefont akár személyi hálózaton (PAN, pl. Bluetooth), akár Interneten és GSM/UMTS hálózaton keresztül. Ha az utóbbit használjuk, meg kell bíznunk a háttérben meghúzódó hálózat biztonságában. Bluetooth-on keresztüli elérés hátránya a kapcsolat felépítésének lassúsága, és nem kidolgozott biztonsági szolgáltatása.

A SIM kártyán tárolt rejtett kulcs megbízható hitelesítést nyújt a szolgáltató felé. Az egycsatornás hitelesítésnél viszont nagyobbak az elvárásaink a kliens oldalon, ezért az korlátozhatja a szolgáltatás mobilitását, skálázhatóságát, illetve veszélyeztetheti a felhasználó kulcsainak biztonságát.

A módszer előnye, hogy a felhasználó hitelesíthető bármilyen Interneten használt, régóta bevált protokollal (például SSL) úgy, hogy a felhasználó rejtett kulcsa a SIM kártyáján marad. Ez magas biztonsági foknak felel meg. A mobil csatorna kimaradásaira és késleltetésére a hagyományos hitelesítő protokollok azonban igen érzékenyek lehetnek, ezért az architektúra tervezése során körültekintően kell eljárni.

3.2. Aláírás mobil készülékkel

A következőkben a digitális aláírás-képzés lehetőségeit soroljuk fel. Az aláírás letagadhatatlanságát úgy lehet biztosítani, hogy semleges résztvevőket nevezünk ki, amelyek naplózzák az aláírás tranzakciók üzenetváltásait, és tárolják az aláírásokat.

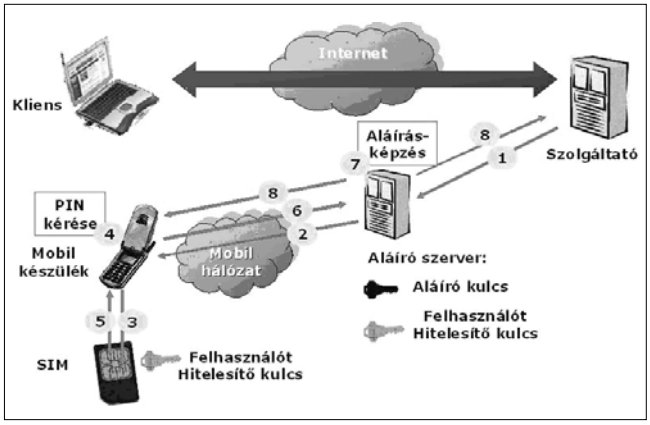
Szerver oldali aláírás, mobil készülék ad utasítást

A legegyszerűbben megvalósítható lehetőség az, ha aláíró szervert hozunk létre, amely tárolja a felhasználó aláíró kulcsát és az aláíró algoritmust. A mobiltelefon szerepe felhatalmazást adni az aláíró szervernek az aláírás létrehozására/végrehajtására. A felhasználó aláíró szerver általi hitelesítése elképzelhető bármelyik

előzőekben tárgyalt felhasználó-hitelesítési módozattal, és ettől függően különböző biztonsági szintű aláírások születhetnek. Fontos, hogy az eljárás során az aláíró szervert is hitelesítse a felhasználó. A módszer előnye, hogy nem kell az alacsony számítási kapacitással rendelkező SIM kártyának aláírnia, nem kell az aláíró kulcsot és algoritmust is tárolnia, és a szerveren hosszabb kulccsal biztonságosabb aláírás is képezhető. Emiatt bevezethetőségének nehézsége megegyezik a kulcs alapú felhasználó-azonosítással. Az aláírás hitelességének szűk keresztmetszete a felhasználó és az aláíró szerver közti kapcsolat biztonsági szintje.

A szolgáltató aláírást szeretne kérni a felhasználótól egy dokumentumra. Elküldi a dokumentumot az aláíró szervernek és esetleg a felhasználó mobil telefonjának. Ha csak az aláíró szerver kapta meg, akkor továbbküldi a dokumentumot – vagy annak egy kivonatát – a mobil telefonra, és kéri a felhasználót az aláírási szándékának megerősítésére. A felhasználó ezután hozzájárul az aláíráshoz egy PIN kód megadásával. A szerver oldali aláírás menetét az *5. ábra* mutatja.

Gyakorlatilag a dokumentum kézhez vétele az egyik legsebezhetőbb pontja a megoldásnak. Olyan módszert kell kidolgozni a dokumentumcserére, amely letagadhatatlan módon tükrözi a felhasználó szándékát. Ha a megerősítés megérkezett, a szerver elkészíti a felhasználó aláírását és visszaküldi mind a szolgáltatónak, mind a felhasználónak, akik azt tárolják.



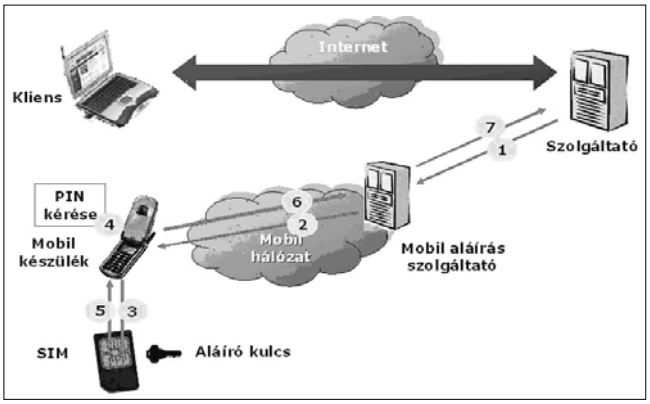
5. ábra Szerver oldali aláírás

A megoldás hátránya, hogy kiemelt hitelességet igénylő aláírás készítésére a megoldás alkalmatlan. A módszer nem felel meg az elektronikus aláírási törvényben leírtaknak, biztonsága a kulcs alapú azonosításnál is maximum közepesnek mondható.

Mobil oldali aláírás (ETSI M-COMM)

Magasabb fokú biztonság a felhasználó kezében lévő chipkártyával, vagyis felhasználó oldali aláírással érhető el. Az ETSI M-COMM Workgroup erre előírásokat dolgozott ki, meghatározta a rendszer komponensek követelményeit és definiált néhány interfészt [4].

Ebben az esetben a szolgáltatók egy speciális hozzáférési szervernek, a mobil aláírás szolgáltatónak (Mobile Signature Server) küldik az aláírandó dokumentumot. A mobil aláírás szolgáltató továbbküldi ezt a mobil csatornán a felhasználó mobil telefonjára. A telefonban lévő chipkártya létrehozza az aláírást. Ehhez a SIM kártyának tartalmaznia kell az aláíró kulcsot és algoritmust. A mobil készülék visszaküldi az aláírást a mobil aláírás szolgáltatónak, aki továbbküldi a szolgáltatónak *(6. ábra)*.



6. ábra Mobil aláírás folyamat

A megoldás biztonságát itt is nagyban befolyásolja a mobil csatornán választott technológiai megoldás biztonsága (WAP, SMS). Bevezetéséhez ebben az esetben le kell cserélni a SIM kártyát, és implementálni kell a mobil aláírás szolgáltatást (mobil aláírás szolgáltató és kapcsolódó funkciói).

Az M-COMM szabványok részletesen leírják a résztvevők feladatait, meghatározzák, hogy milyen interfésszel kell rendelkeznie mobil aláírás szolgáltatónak a szolgáltató felé. A mobil aláírás szolgáltató és a mobil készülék közötti interfészeket viszont nem definiálja. Elképzelhető adatkapcsolt vagy csomagkapcsolt (GPRS), WAP vagy SMS átviteli technológiai megoldás.

Egycsatornás mobil oldali aláírás

A felhasználó-azonosítási módszerekhez hasonlóan, az aláírási folyamat is megvalósítható egycsatornás módszerrel *(4. ábra)*. A szolgáltató elküldi a kliensnek az aláírandó dokumentumot, a kliens gép továbbítja ezt – vagy egy kivonatát – a mobil készülékre. A SIM kártya létrehozza az aláírást, és visszaküldi a kliens gépnek. Ezután a kliens visszaküldi az aláírást a szervernek. A SIM kártyának kell tárolnia az aláíró kulcsot és algoritmust. Nagy biztonságú megoldást jelent, de feltételezi, hogy a felhasználó számítógépe kapcsolatba tud lépni a mobil telefonnal. Bevezethetősége nehézkes, mivel a mobil készülék és a kliens gép közötti kapcsolatnak speciális követelményeket kell kielégítenie (például mindkettő támogassa a Bluetooth technológiát, vagy a felhasználó rendelkezzen adatkábellel).

4. Szempontok a rendszertervezéshez

Az előzőek alapján meg van minden lehetőség arra, hogy olyan eljárások kerüljenek kidolgozásra, amelyek részben vagy egészben tartalmaznak elektronikus ele-

meket, és ezen belül részben vagy teljes egészében a mobil csatornán zajlik. A KET tartalmazza, hogy senki nem kényszeríthető elektronikus ügyintézési út használatára, illetve az eljárás alatt az állampolgár szabadon válthat az elektronikus és hagyományos ügyintézési út között.

Adottak jól működő, szabványosított technológiák és olyan specifikációk, amelyek meghatározzák az elektronikus ügyintézés biztonsági követelményeit. Azonban, hogy minőségileg is megfelelő, sikeres szolgáltatásokat teremtsünk, fontos, hogy a műszaki követelményeknél és a technikai interfészeknél a jelen törvényeket tükröző biztonsági politika kerüljön érvényre. Például meg kell határozni, hogy adott körülmények között milyen adatokat tartalmazzon egy tanúsítvány, mire kell felhívni az állampolgár figyelmét, hogy ne sérülhessenek a jogai, milyen elágazások legyenek az ügyintézésben, így a megvalósító szoftverben.

Vegyük példaként a mobiltelefonnal végzett elektronikus aláírást. Az aláírási politika meghatározza, hogy adott ügymenetben milyen szereplők aláírását várjuk, mire szóljon az aláírásuk, hosszú- vagy rövid távú letagadhatatlanságot nyújtson stb. [18]. Az aláírás többféle szereppel bírhat: felhasználó azonosítása, névvel való ellátás, szervezet pecsétje, delegált személy aláírása, szerződés legális vonzatainak vállalása, tanú, közjegyzői aláírás stb. Fontos, hogy az aláírás megtételénél eleget tegyünk az adott eljárásra érvényes rendelkezéseknek, és az Elektronikus aláírási törvény által megkövetelt biztonsági szintnek.

A biztonsági politikának minél inkább automatizáltan kell működnie, de úgy, hogy a felhasználó egyértelműen kinyilváníthassa szándékát. Az emberi tényező okozhatja a legtöbb hibát, félreértést a mobil aláírórendszer használata során. Fontos, hogy amikor részletekig menően kigondolják a biztonsági politikát, azt is vizsgálják, hogy mi az, ami automatizálható, és mi az, amihez kérni kell az aláíró személy megerősítését. A felhasználó semmiképpen ne mondhassa azt utólag, hogy nem állt rendelkezésére egy szándékát tükröző opció, vagy hogy félrenyomott egy menüpontot.

A biztonságpolitika létrehozása tehát nemcsak mérnöki feladat, hanem egy igen hosszadalmas munka, amelyben mérnököknek és jogászoknak kell együtt dolgozniuk. Az ETSI M-COMM szabványok megfelelő iránymutatást adnak a mobil aláírás tranzakciók és felhasználó-hitelesítés technikai megteremtéséhez, azonban ez még korántsem elég egy használható rendszer megvalósításához.

5. Összegzés

A cikkben bemutattuk, hogy miként használható a mobil csatorna, és hogy ez milyen biztonsági jellemzőket von maga után. Láthattuk, hogy van helye a mobil technológiának egyes közigazgatási és hivatalos eljárások bizonyos mozzanatainak felváltásában, azonban bármilyen rendszert is szeretnénk kialakítani, előtte körültekintően számba kell venni és harmonizálni az esedékes törvényeket, rendeleteket, hogy jogi szempontból is megfelelő biztonságpolitika érvényesüljön. A technológiai feltételek adottak.

A cikk alapját képezi az IKTA 00046/2003 számú pályázat („Elektronikus aláírás mobil telefonnal”) keretében készült tanulmány, illetve az IBM Magyarország Kft. által az Informatikai és Hírközlési Minisztérium részére „Részletes követelményspecifikáció kidolgozása elektronikus aláírás és intelligens kártya használatához a közigazgatás informatikai biztonságának érdekében” című közbeszerzés keretében átadott vonatkozó dokumentumok, melyeket az E-Group Magyarország Rt. készített jelen cikk szerzőinek közreműködésével.

Irodalom

[1] “Directive 1999/93/EC of the European Parliament and of the Council of 13 Decembre on Community framework for electronic signatures”, Official Journal L 013, 19/01/2000, pp.12–20.
[2] “Common List of Basic Public Services”, www.innovazione.gov.it/eng/intervento/e_europe/010501_basicpublicservices_eng.pdf
[3] „Digitális Mobil Gyorsjelentés, 2004. május”, NHH, www.nhh.hu/menu3/m3_2/mobil/2004/majus.pdf
[4] ETSI TR 102 203: “Mobile Commerce (M-COMM); Mobile Signatures; Business and Functional Requirements”.
[5] Liberty Alliance Project: “Introduction to the Liberty Alliance Identity Architecture Revision 1.0”, 03/2003
[6] S. Lannerstrom: ”White Paper Mobile Authentication”, MPM 02:0041, SmartTrust, August 2002
[7] Radicchio Best Practice Working Group: “A universally recognized and accepted identity scheme that leverages the mobile infrastructure.” Working Document, 26th September 2002
[8] Radicchio – http://www.radicchio.org
[9] Liberty Alliance – http://www.projectliberty.org
[10] GSM Association – http://www.gsmworld.com
[11] ETSI – http://www.etsi.org/m-comm/summary.asp
[12] SimPay – http://www.simpay.com
[13] Mobey Forum – http://www.mobeyforum.org/
[14] MeT Ltd. – http://www.mobiletransaction.org
[15] PayCircle – http://www.paycircle.org
[16] Open Mobile Alliance – http://www.openmobilealliance.com
[17] Mobile Payment Forum – http://www.mobilepaymentforum.com/
[18] ETSI TR 102 045: “Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model”, V1.1.1 (2003-03)
[19] WAP Forum: ”Wireless Application Protocol, Public Key Infrastructure Definition”, WAP-217-WPKI, Version 24-Apr-2001
[20] WAP Forum: “Wireless Application Protocol, WAP Certificate and CRL Profiles Specification”, WAP-211-WAPCert, 22-May-2001

E-kormányzás:
lehetőség, kényszer és valóság

DR. DEDINSZKY FERENC[1], FRIGYESI VERONIKA[2], FUKKER GABRIELLA[3], MÉREI EMIL

[1]*Elektronikus Kormányzat Központ, ferenc.dedinszky@ekk.gov.hu*

[2]*verfri@qwertynet.hu*

[3]*Informatikai és Hírközlési Minisztérium, gabriella.fukker@ihm.gov.hu*

Kulcsszavak: összekapcsolt (joined-up) kormányzás, folyamatszervezés, víziók, k-kormányzás

Az e-kormányzás lehetőségét a „műszaki-technológiai" infrastruktúra kialakulása, az információs és kommunikációs technológia fejlődése teremtette meg, mely minden korábbi technológiánál gyorsabban épült be a gazdaságba és társadalomba. A kormányzati szektor „elektronizálása" új piac lehet az info-kommunikációs technológiai szektor számára.

A XIV. Információtechnológiai Világkongresszuson (WCIT – Athén, 2004. május 19-21.) az alábbiak fogalmazódtak meg: *„A multinacionális info-kommunikációs fejlesztő cégek felismerték annak jelentőségét, hogy számukra az e-kormányzati szolgáltatások széleskörű igénybevétele jelenti növekedésük egyik fő területét, ezért készek a szolgáltatásokhoz szükséges infrastruktúra és alkalmazásfejlesztések kialakításában támogatni a kormányokat."*

(Forrás: MeH, Elektronikus Kormányzat Központ)

A vállalkozói szféra az információs társadalom fejlesztésének nagy hányadát képes megvalósítani, a „maradék" a kormány feladata [7]. Természetszerű feszültség tapasztalható a piac-vezérelte érdekek és a gyakran váratlan irányokban haladó gyors műszaki-technológiai fejlődés, valamint a közösségi érdekek védelme és az intézményi/szervezeti feltételek biztosítása között. A kormányok hatása ebben az erőtérben óriási, hiszen különböző szerepeket töltenek be. Tulajdonosként rendelkeznek a frekvenciaelosztásról. Szabályozó szervezetként meghatározzák a vállalatok működésének feltételeit. Hatóságként ellenőrzési feladatokat látnak el. Felhasználóként, megrendelőként maguk is piaci szereplők. Az adókedvezményeken, alapítványokon keresztül egyben „finanszírozó testületként" is működnek. A közösségi érdekek védelme csak a politika intézményesült keretei között valósulhat meg.

A vállalati és kormányzati szféra infokommunikációs fejlettsége között nagy az eltérés, ami nem tartható fenn. A műszaki-technológiai-menedzsmentnek azt a fejlődését, amely a vállalati szférában megvalósult, a kormányzati szektornak is követnie kell. A technológiai lehetőségek és nyomás mellett a megváltozott környezet is cselekvésre ösztönzi a kormányokat. Az erősebb nemzetközi verseny következtében a hatékony, gyors együttműködés a helyi (nemzeti, regionális, helyi) kormányzattal – mint versenyképességi tényező – felértékelődik a vállalati szektorban [4]. (Így az online szolgáltatások gyorsabb pályázati és elbírálási eljárásokat tesznek lehetővé, ami közvetlenül befolyásolhatja a vállatok jövedelmének alakulását stb.)

A lakossági elvárások szintén szigorodnak. Az igények korosztályok szerint is változnak. Egy jelenleg iskolás korú állampolgárt néhány év múlva nem lehet már többé meggyőzni arról, hogy várnia kell a hivatal nyitvatartási idejére és sok esetben hosszú sorokban kell várakoznia valamilyen igazolvány igénylése céljából, amikor számára teljesen természetes, hogy vásárlásait vagy bankügyeit interneten keresztül bonyolítja [3,8].

Tervek és víziók

Az információs és kommunikációs technológiák bevezetése a kormányok számára is lehetőséget biztosít a hatékonyság növelésére, valamint az állampolgároknak és vállalatoknak kínált szolgáltatások minőségének javítására. Az állam modernizálására vonatkozó elképzelések szerint ezen technológiák alkalmazása együtt jár a kormányzati filozófia gyökeres megváltozásával. Az új futurisztikus forgatókönyv szerint a kormányzat eszményképe egy szolgáltató szervezet, melynek részvényese az adófizető [1,8].

Az e-kormányzati víziók szerint a teljes társadalmi-politikai rendszer átalakul. Megváltoznak a kormányzati (nemzetek feletti, nemzeti, regionális, helyi) szintek és funkciók, valamint ezek aránya. Az intézményi szereplők közötti hatalmi kötelezettségek, szövetségek és függési viszonyok új struktúrája jön létre. Ezt a folyamatot a globalizáció és decentralizáció kettős trendje, valamint a hagyományos politikai demokrácia intézményeinek szerepváltozása vezérli. A helyi és regionális kormányzatok szerepe nő. A hagyományos hierarchiák gyengülnek. A kormányzás rendszere a hálózatok irányába mozdul el, melyek nem egyszerűen technológiai alapú, hanem társadalmi és intézményi infrastruktúrák is. Ebből eredően a személyes kapcsolatok, a szerepek, hatáskörök, együttműködések, valamint technológiai konfliktuskezelő minták új szerkezete alakul ki (szervezetek határát átlépő együttműködések stb.) [1,3].

A vertikális integráció (a nemzeti, regionális, helyi szintek részvételével) és a horizontális integráció (a különböző kormányzati szervezetek és hatóságok, valamint magánpartnerek részvételével az adott régióban)

kombinációja az úgynevezett *összekapcsolt (joined-up) kormányzás*. Az összekapcsolt kormányzás koncepciója nem feltétlenül jelent központosított, hierarchikusan irányított szervezetet. Az integráció és együttműködés centralizált és decentralizált hálózati modell keretében is megvalósítható [1]. Az e-kormányzás az állam virtualizálásaként is értelmezhető [8].

Az e-kormányzással kapcsolatos vitákban növekvő figyelmet szentelnek az *új kormányzati menedzsment (new public management)* koncepciónak, melynek sarokköve a hatékonyság növelése a kormányzati folyamatok menedzsmentjében. Az e-kormányzásra úgy tekintenek, mint az új kormányzati menedzsmenten alapuló paradigmára, mely a felhasználók keresletére összpontosít, kiaknázva az infocom technológiák által „biztosított" interakciós potenciált. Ennek megfelelően az e-kormányzástól az alábbiakat várják:

– a kormányzati szolgáltatások hatékonyságának, termelékenységének, minőségének javítása;
– az állampolgároknak rugalmasságot biztosító, új szolgáltatási szabványok bővítése, személyre szabott, a nap 24 órájában és a hét minden napján rendelkezésre álló megoldásokkal (ugyanolyan módon, mint a magánszektorban) [1].

A fejlődés új, elképzelt irányaként jelent meg a *K-kormányzás (tudásalapú kormányzás)* bevezetése az évtized végéig. Az állami szervezetek a legnagyobb tudásvagyon birtokosai és tudásmenedzselő szervezetek is. A kormány által létrehozott és tárolt információk menedzselésének megtanulása és jobb hasznosítása nagyon értékes javak „előállítását" eredményezheti. Az információs és távközlési technológiák fejlődése – túlmutatva az igazgatási feladatokon – lehetőséget biztosít az állam számára, hogy integrálja az általa birtokolt tudásvagyont a társadalmi és gazdasági innovációs folyamatokba. Elméletileg egy központi nemzeti adatbankot kellene létrehozni. Ennek gyakorlati megvalósítása csak a hálózati kapcsolódás komplex rendszerén keresztül lehetséges. (Az információvagyon megőrzése már napjainkban is nagy fontosságú lenne. A honlapokon megjelenő információk nagy része egy idő után törlésre kerül, nagy mennyiségű tudásanyag válik ezáltal a jövő számára elérhetetlenné.) [1,2,10].

A fent vázolt elképzeléseknél is „merészebb" a *környezeti (ambient) intelligencia* víziója: a különböző objektumba beágyazott intelligens intuitív interfészek alkalmazását célul kitűző „technológiai forgatókönyv". A környezeti intelligencia képes lesz felismerni a különböző individuumok sajátos egyéni igényeit és reagálni is arra [1]. Az e-kormányzás várható hatásairól az *1. táblázat* ad áttekintést.

általános hatások

1. a rendszer jobb átláthatósága
2. a folyamatok jobb követhetősége
3. nagyobb nyitottság
4. a kormányzat és az állampolgárok kapcsolatainak javítása
5. a kormányzat és vállalkozások kapcsolatainak javítása
6. „olcsóbb" kormányzat és takarékos állam (adófizetők pénzének hatékonyabb felhasználása)
   6.1. a kormányzat munka, az államigazgatás hatékonyságának javítása
      6.1.1. termelékenység javítása
   6.2. munkavégzés minőségének javítása
      6.2.1. gyorsul az információk áramlása
      6.2.2. gyorsul a munkavégzés
   6.3. költségek csökkenése
      6.3.1. alacsonyabb működési költségek
      6.3.2. gyors ügyintézési folyamatok
7. a versenyképesség javulása
8. a gazdaságfejlesztés esélyeinek javulása
9. nagyobb lehetőségek tudásalapú szolgáltatások nyújtására
10. a döntéselőkészítés, döntéshozatal információs bázisának bővülése
11. hozzájárulás fenntartható fejlődéshez
    11.1. környezetmegóvás
       11.1.1. az utazásból származó környezeti terhelés csökkenése
       11.1.2. a környezetkárosító eljárások észlelésének gyors bejelentése
       11.1.3. a papírhasználat csökkenése

e-szolgáltatások

1. a szolgáltatások minőségének javítása
2. időmegtakarítás
3. korlátlan hivatali „nyitvatartási idő"
4. kényelem
5. rugalmasság
6. személyre szabás (perszonalizáció)
7. korlátlan hivatali „nyitvatartási idő" (rendelkezésre állás a nap 24 órájában és a hét minden napján)
8. ügyfelek kiszolgálásának színvonala emelkedik

e-közbeszerzés

1. költségmegtakarítás
   1.1. az állam számára
      1.1.1. beszerzési folyamatok menedzselési költségeinek csökkenése
      1.1.2. a folyamatok alacsonyabb költségei
      1.1.3. az alacsonyabb beszerzési árak
      1.1.4. a folyamatok átláthatósága
      1.1.5. a folyamatok követhetősége
   1.2. vállalatok számára
      1.2.1. alacsonyabb tranzakciós költségek
2. a korrupció csökken
3. időmegtakarítás
4. kényelem
5. rugalmasság
6. kis- és középvállalkozások marginalizálódása
7. központosítás

e-demokrácia

1. az esélyegyenlőség növekedése, a lemaradók felzárkózásának elősegítése
2. bizalom erősödése
3. a demokrácia fejlődik
   3.1. a közügyekben a részvétel bővül
   3.2. a részvételi demokrácia kiteljesedik
4. partneri viszony lép az „alattvaló" állampolgár és a „hatóság" tekintélyelve helyébe

1. táblázat Az e-kormányzás lehetséges hatásai

Eredmények

A valóság még nagyon messze áll a vízióktól. A kormányok az elmúlt években elért jelentős eredmények ellenére is még csak az útkeresés szakaszában élnek. A politikai motiváció és elkötelezettség erős a kormányok szintjén, és ez jelentősen meglendítette az e-kormány-

zati fejlesztések ütemét. Az infrastruktúrára és a szolgáltatások elérhetőségére vonatkozó adatok valóban ígéretes fejlődésről tanúskodnak, de ez a fejlődés sokkal lassúbb és a felhasználók közömbösebbek mint várták. Jellemző, hogy az e-kormányzás értékelésének céljaira ma még az infrastruktúra színvonalmutatóival és az online szolgáltatások elérhetőségével „mérnek". Az e-kormányzás fő területeinek fejlettségére vonatkozó általános értékelést a *2. táblázat* mutatja be [1].

Az e-kormányzás előtt álló fontos „minőségi" feladat az igazgatási és a kormányzati folyamatok átszervezése (a vállalkozói szféra business process re-engeneeringjéhez hasonlóan). Az e-kormányzást úgy „vezették be", hogy az alapvető szervezeti struktúrák, szerep- és hatásköri megosztások változatlanok maradtak [3,8]. A kormányzati tevékenységek integrálásának ki kell terjednie:

– a szolgáltatások horizontális integrációjára (egy ablakos rendszer);
– a horizontális szolgáltatások integrációjára (személyazonossági okmányok, e-fizetés menedzselése stb.);
– a front-office-ok integrálására az összefüggő back office-okkal (a tevékenységek jellegéből eredően).

Az ENSZ 2003. évi, az összes tagállamra kiterjedő felmérésének eredményei szerint nagyon sok kormányzati portál mindössze információt tartalmaz. 2003-ban a világ országainak csak 14%-ában állt rendelkezésre az online konzultációs lehetőség és mindössze 9%-ában nyílt lehetőség bármely állampolgárnak a visszacsatolásra is a kormányzati honlapokon közzétett kormányzati politikával vagy tevékenységekkel kapcsolatban [3].

Az e-kormányzati programok kudarcai az alábbi tényezőkkel függnek össze:

a) Túl ambiciózus tervek, amelyeket a politikákat kidolgozók „visznek keresztül", majd még ambiciózusabb projekteket generálnak.

b) A közszféra speciális voltát alábecsülik. A rugalmasság hiánya, a struktúrák komplexitása, az ösztönzés hiánya a hatékonyság javítása terén (az elért megtakarítások a következő évben a költségvetés csökkentéséhez vezetnek, csökkentik a közszolgáltatásban dolgozók motivációját stb.).

c) A politikai prioritások változhatnak a projekt megvalósításának időszakában.

d) Hiányzik a megfigyelés és értékelés, ami azt eredményezte hogy nincsenek megfelelő információk a fejlesztések általános hatásaira és a hatékonysági hatásokra vonatkozóan [1].

A negatív tényezők közül egy sem „technológia- vagy piacorientált", az összes a projektek szervezeti és menedzsment feltételeivel, valamint a kormányzati környezet sajátos jellegzetességeivel „áll kapcsolatban". A fejlődés legnagyobb akadálya az „adminisztráció" gondolkodása és merevsége. Az e-kormányzás nehezebb része vár megvalósításra: a kormányzati szektor szerkezeti és szervezeti átalakítása.

Irodalom

[1] Cattaneo, G.: Building government: European Regions alternative Strategies, Databank Consulting, 2003. www.europa.eu.int/information_society
[2] eDemocracy. Seminar Report. February 12 and 13, 2004. Brussels, www.europa.eu.int/information_society
[3] E-Government at the Crossroads. World Public Sector Report 2003. United Nations Economic and Social Affairs Dep. New York, 2003
[4] Frigyesi Veronika: Globalizáció és versenyképesség, Valóság, 2000/3.
[5] Hivatalos jelentés, adatszolgáltatás (magyar nyelvű), Magyar Inform. Stratégia Monitoring Jelentések, No.30, TÁRKI – IHM, 2004. január
[6] Kanalas Imre: Az információs fejlettség területi különbségei Magyarországon, eVilág, 2003. október
[7] Rechnitzer János: Az információs társadalom térformáló szerepe. eVilág, 2003. február
[8] Stobbe, A.: E-government: large potential still to be tapped. Economics. Deutsche Bank Research. October 31, 2002.
[9] Szentgyörgyi Zsuzsa: Az információs társadalom nagy kérdőjelei. eVilág, 2003. november
[10] Ugrin Emese: Az e-közigazgatás funkcionális rendszere, eVilág, 2003. december

2. táblázat Az e-kormányzás fejlettségi szintje (Forrás: Databank Consulting, 2003.)

	fejlettségi szint	meghatározó intézményi szereplők	fő problémák
e-szolgáltatások	online rendelkezésre álló „egyszerű" szolgáltatások, melyek a horizontális integráció és a nagyobb interaktivitás irányába mozdulnak el	bottom up folyamat, melyet a helyhatóságok és helyi kormányzatok vezérelnek	kínálat és kereslet rossz illeszkedése
e-közbeszerzés	a központi rendszerek és platformok fokozatos bevezetése – a hatás még korlátozott	felülről lefelé irányuló folyamat, melyet a nemzeti vagy regionális hatóságok vezérelnek	ellenállás a helyi szereplők részéről, marginalizálódásának veszélye, a technológiai bezárkózás kockázata
e-demokrácia	pilot projektek – korai szakasz	kevert: egy részük nemzeti, egy részük helyi a politikai környezettől függően	változó kormányzati elkötelezettség, kockázat marginalizálódás a „teljesítményre" vonatkozó célok által

A vezetékes hálózatok változásának oka és következménye

HANSSON LEIF, BORDÁS CSABA

Ericsson Magyarország

leif.r.hansson@ericsson.com; csaba.bordas@ericsson.com

Kulcsszavak: fix állomások fejlődése, együttműködési kérdések és tendenciák, hálózati jövőkép

A hagyományos, vezetékes távközlésben lényegi változásokat tapasztalhatunk már ma is, viszont a hálózatok és szolgáltatások forradalmának a java még hátra van. Cikkünkben a vezetékes hálózatok jelenlegi állapotát, illetve a belátható jövő irányzatait szeretnénk felderíteni.

1. A változás oka és iránya

Lényegében jól ismert közhelyszerű okokról van szó, amelyeket mindnyájan ismerünk. Érdemes mégis – megfelelő sorrendbe téve – összegezni ezeket, kiinduló alapot teremtve a következő okfejtéshez.

1.1. Mobil előretörés

A mobil távközlés használata életforma, elsősorban erre gondolunk, amikor kommunikációról beszélünk. A kommunikáció és a mobilitás lényegében mindig szorosan összefüggtek egymással, csak a vezetékes hálózatok technológiai kötöttségei miatt voltak „fix” terminálok. Az emberek összenőnek a svájci bicska szerepét átvevő terminájukkal, amit mindenüvé magukkal visznek és beszélgetésen túl hangfelvételre, fényképezésre, Internet böngészésre, zenehallgatásra, bevásárlásra, játékra és még ki tudja mi minden másra használják, de még inkább fogják használni azokat.

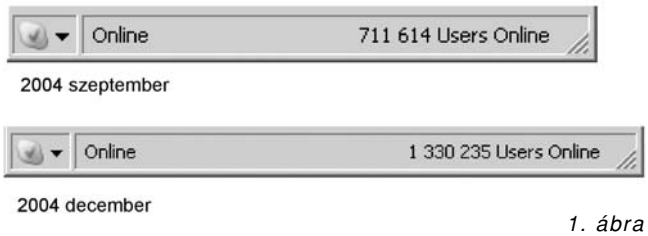
A mobiltelefonok a legnagyobb számban forgalmazott fogyasztói eszközök a világon, éves forgalmuk forgalmuk meghaladja a PC-k, televízió készülékek és DVD lejátszók együttes forgalmát.

Ezek után szükségünk van még egyáltalán vezetékes hálózatokra? Minden bizonnyal, viszont a távközlési hálózatok vezetékes és mobil hálózatok ilyen éles elkülönítésére nincsen szükségünk, ahogyan ezt később majd látni fogjuk.

1.2. Új formabontó technológiák – új üzleti modellek

Formabontó technológiának (disruptive technology) a kifelyezést magyarázó Clayton M. Christiensen szerint olyan technológiákat nevezünk, amelyek gyengébb minőségű, alacsonyabb teljesítményű, de új és olcsó termékek, szolgáltatások előállítását teszik lehetővé [1]. A sikeres formabontó technológiák a megfelelő minőségi fejlődés és piaci érés után képesek az inkumbens technológiák és az ezekhez kapcsolódó szolgáltatások kiszorítására.

Jó példa erre a formabontásra a Skype jelenség[1], amelynek az alábbi ábra tanúsága szerint ma már több, mint 1,3 millió aktív felhasználója van világszerte.



1. ábra
Aktív Skype felhasználók világszerte 2004 szeptemberében és 2004 decemberében

Számos ilyennel találkozhatunk a jelenlegi távözlési piacon, inkumbens technológiává válásuk különböző szakaszaiban. Egy rövid felsorolás ezekből a technológiákból, megoldásokból és termékekből, teljesség igénye nélkül: VoIP, Wi-Fi, WiMAX, xDSL, VoDSL, Ethernet, UM (Unified Messaging), IM (Instant Messaging), FTTx, Parlay/OSA (Open Service Access), Triple play, Skype, de ide sorolhatóak a 3G vagy ennek részeként IMS (IP Multimedia Subsystem) is.

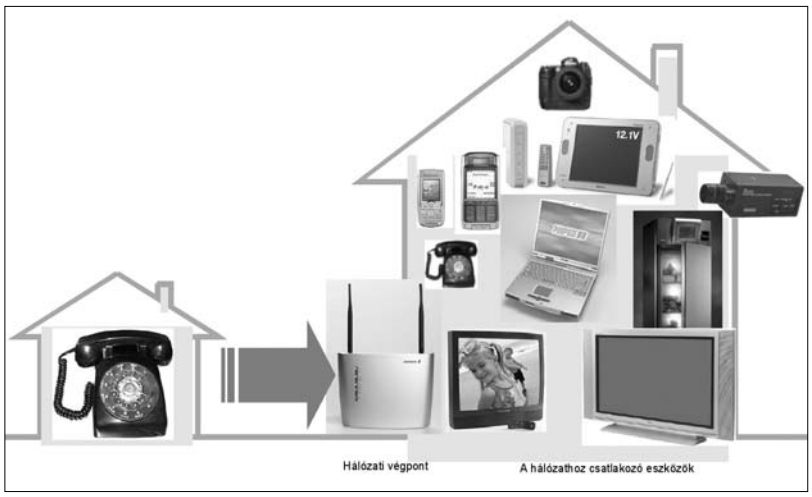
Összességében ezek az új technológiák új üzleti modellek kidolgozását is lehetővé teszik vagy elősegítik. Az előző Skype példánál maradva, Niklas Zennström, a cég alapítója szerint a hanghívások perc szerinti árazása huszadik századi csökevény. A hang – az ő szempontjából – nem egyéb, mint egy, az IP hálózatokon futó sok alkalmazás közül, tehát az üzeti modell inkább a szoftverek jogdíjazását mintsem a hívások percdíjazását kellene kövesse.

1.3. Új üzleti modellek – új formabontó technológiák

Az előző fejezetben bemutatott irány fordítva is működik, hiszen az új piaci szereplők nem követik a hagyományos üzleti modelleket, ami a fejlesztők figyelmét az új elképzeléseket támogató irányba tereli. Az elérési hálózatok terén ilyen jelenség a Wi-Fi, vagy maguk

1 A Skype az egyik legnépszerűbb és legdinamikusabban fejlődő internetes telefónia alkalmazás a világon. Sikerét elsősorban a kliens szoftver (Windows, Linux, Mac OS, Pocket PC) egyszerűségének, a kiváló hangminőségnek és annak köszönheti, hogy belső IP hálózatokon, tűzfal mögött és NAT után is működik. A Skype felhasználók egymást ingyen hívhatják, de a PSTN hálózatba is igen kedvező áron telefonálhatunk. Bővebb információ: www.skype.com

az Ethernet alapú hálózatok, amely kilépve a LAN-on környezetből továbbfejlődnek a nagy kiterjedésű elérési hálózatok irányába. Egy másik ilyen példa az IP protokoll maga ami adatátviteli protokollból nőtte ki magát – piaci igényektől sarkallva – MindenoIP (Minden over IP) jelenséggé. A hagyományos, „inkumbens" technológiák gyakran nem adnak kielégítő megoldásokat az új üzleti modellekre.



3. ábra Az előfizetői berendezések sokoldalúsága

1.4. Új szolgáltatások, új alkalmazások

Ma már senki sem épít ki dedikált hálózatot egy alkalmazáshoz vagy szolgáltatáshoz, dedikált hálózatok esetén is olyan megoldásokat alkalmaz, amelyek többcélú felhasználást tesznek lehetővé. Például ha professzionális minőségű videójel átvitelt kell megvalósítani, nem fektetünk le ezért egy fényvezető hálózatot, hanem a meglévő IP gerinchálózatot bővítjük az IP csomagokba ágyazott videójelek átvitelére.

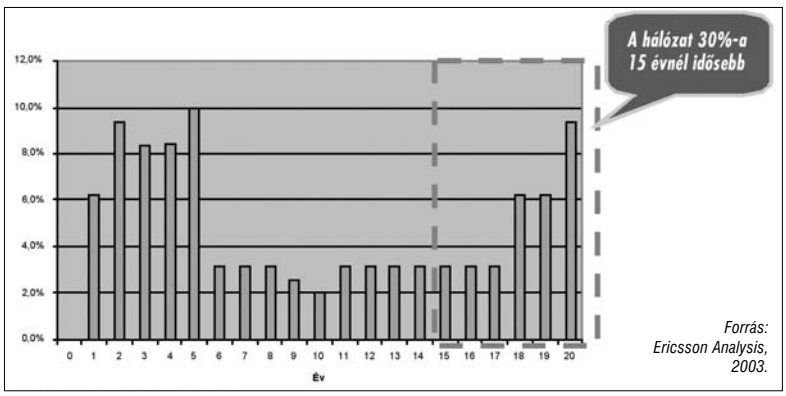
Egyes szolgáltatásokat olyan gyorsan kell piacra dobni (vagy onnan visszavonni), hogy az lehetetlenné teszi hálózatok kiépítését, de még alkalmazásplatformok beszerzését is. A meglévő hálózat és platform alkalmas kell legyen a szolgáltatások gyors be- és kivezetésére, módosítására, ami a vonalkapcsolt vagy alkalmazás specifikus hálózatokra nem jellemző.

Az is természetes – de nem ennek a cikknek a témája –, hogy a hálózatok mögött álló szervezet is a kihívásnak megfelelően rugalmas és gyors kell legyen[2].

1.5. Korosodó, amortizált hálózatok

A meglévő vonalkapcsolt hálózataink jól működnek ugyan, de ha egy pillantást vetünk a *2. ábrára*, akkor kiderül, hogy rövidesen a digitális hálózat nagy része is már olyan életkort ér el, hogy a szolgáltatónak hosszú távú döntéseket kell hoznia a hálózat konzerválásáról, modernizációjáról vagy kiváltásáról. Az alkatrészek többségét, amiből ezeket a rendszereket tervezték és gyártották, már régen nem rendelhető, gondoljunk csak a 8086-os processzorra vagy az 1 GB-os merevlemezre.

2. ábra
Tipikus nyugat-európai szolgáltató vonalkapcsolt hálózatának életkora



Új vezetékes hálózatra van tehát szükség, ezért sürgősen el kell gondolkodni a jövő hálózati stratégiáján.

A helyes stratégia megválasztása tehát nem egyszerű, mivel a formabontó technológiák többsége még nem érett meg a széleskörű alkalmazásra, aminek egyik feltétele a szabányosítás befejezése.

2. A változás következménye

A fenti okok miatt az elkövetkezendő 10-20 évben a hálózatok teljes újjászületése várható a hozzáférési, vezérlési és alkalmazási szinteken. A 21. századi hálózatban fontos szerepet játszik az előfizetői terminál, vagy az akár több eszközből is álló előfizetői állomás (CPE). A hálózati intelligencia és főleg a szolgáltatások a hálózat peremén levő terminálokba és alkalmazás szerverekbe költözik. Ezek után természetes, hogy az előfizetői terminálok is teljesen kicserélődnek majd és különös figyelmet érdemelnek.

2.1. Előfizetői berendezések, a háztartások átalakulása

A hálózatok értékének zömét mindig is a hozzáférési szakasz tette ki, ehhez adódik az új hálózati struktúrában az előfizetői berendezések jelentős része. Persze korántsem egyértelmű, hogy mi tartozik ebbe a kategóriába, vessünk csak egy pillantást a *3. ábrára!*

A szélessávú hálózatokon bármilyen információ átvihető, tehát az eszközök és a beléjük integrált szolgáltatások sokoldalúságának csak a tervezők képzelete szabhat határt.

Emiatt is nehezebb lesz a hálózat létesítmény határait meghatározni előfizetői oldalon, ami lehet DSL modem, IAD, Set-top-box, W-LAN hozzáférési pont, akár egy intelligens hűtőszekrény vagy a hagyományos telefon aljzat.

2 Ameddig egy hagyományos, hierarchikus szervezet reagál egy üzleti lehetőségre, főleg ha az beszerzési folyamattal is jár, addig egy kissebb szervezet már vagy megvalósítja a szolgáltatást, vagy már megyszűnik az üzleti lehetőség.

A terminálok egyre intelligensebbek, egyre kevesebben használják a jó öreg telefonkészüléket; a tetszőleges, jól használható terminálok hiánya a vezetékes távközlés egyik megoldandó problémája.

A terminálok lehetnek közösek a mobil hálózatéval, a vezetékes-mobil konvergencia egyik fajtáját megvalósítva, de ezt a gondolatot bővebben is kifejtjük a vezetékes-mobil konvergencia fejezetben.

2.2. Hozzáférés

A hálózat másik nagyértékű és a legnagyobb infrastruktúrát használó része a hozzáférési szakasz. Az új hozzáférési hálózatnak számos tulajdonsága és szolgáltatása lehet, amelyek közül a következőket emeljük ki:

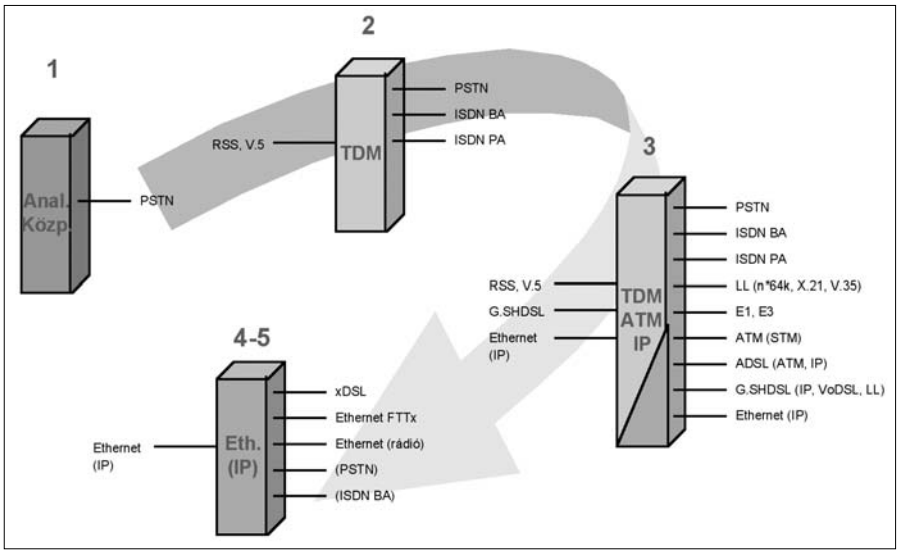
- Megfelelő sávszélességű kell legyen. Ez a gyakorlatban, a mai álláspontok szerint bővíthetőséget jelent akár 20-50 Mb/s (letöltési) sebességre. Nem érdemes tehát olyan hozzáférési hálózatokat építeni, vagy a meglévőket úgy átalakítani, hogy azok a belátható jövőben sávszélesség szűkületet jelenthessenek.
- Képes kell legyen a különböző osztályú csomagkapcsolt forgalom prioritásainak kezelésére, vagyis minőségi szolgáltatások nyújtására.
- Feleljen meg az alapvető biztonsági követelményeknek, elsősorban a különböző előfizetők és eszközök forgalmának elkülönítésére.
- Kedvező árú legyen, vagyis belátható időn belül, a technológia elavulása előtt térüljön meg.

Nagyon tömören, a hozzáférési csomópontok fejlődését (vagy dilemmáját?) a *4. ábrával* is illusztrálhatnánk.

Az analóg hozzáférési rendszerek (helyi központok) kizárólagos analóg előfizetői vonalai után a digitális előfizetői szakasz az ISDN elérést is lehetővé tette.

Az adatátviteli igények túlnőttek a TDM kapacitásokon és az előfizetői fokozatokba adatkommunikációs képességeket integráltak, amint az a *4. ábra* 3. fázisában látható. Az így keletkező IAD (Integrated Access Device) vagy IAM (Integrated Access Multiplexer) eszközök még ma is kaphatóak, viszont számos hátrányuk van:

4. ábra
A hozzáférési csomópont fejlődése és átalakulása



- A csomagkapcsolt és vonalkapcsolt vonalkártyák fizikailag integrálva vannak ugyan egy fiókba, viszont logikailag és üzemeltetés szempontjából legtöbbször teljesen külön menedzselt rendszereket képeznek.
- Külön PSTN (pl. E1), külön csomagkapcsolt (pl. ATM, STM-1, Ethernet) hálózati interfészeket igényelnek.
- Nem, vagy csak nehezen fejleszthetőek ki új interfészek (pl. SDI video).
- Korlátozottan skálázhatók, korlátozott sávszélességű hátlapjuk (pl. cellbusz) van.

Mivel IP alapú rendszerek felett gyakorlatilag bármilyen infomáció átvihető és az IP alapú rendszerek jól skálázhatóak, logikusan következik a fejlődés következő, az ábra szerinti 4. fázisa, ahol a hozzáférési csomópont egyetlen, IP alapú hálózati interfésszel rendelkezik. És mivel az IP natív, leghatékonyabb adatkapcsolati protokollja az Ethernet, ez az interfész FE vagy GE alapú.

Az Ethernet réteg csak a PSTN/ISDN esetben végződik a hozzáférési csomópontban, egyébként xDSL, optika vagy rádiós interfészen keresztül az előfizetői hálózati végpontig tart, nyilvános Ethernet hálózatot alkotva. PSTN/ISDN vonali kártyákra egyelőre szükségünk lesz az olyan előfizetők miatt, akik csak ezt a szolgáltatást igényelik, mert az ő esetükben nem lenne gazdaságos integrált előfizetői eszközt (IAD) telepíteni.

Ezzel el is jutunk a hozzáférési csomópontok fejlődésének utolsó, 5. szakaszához, amikor a csomópontok tisztán Ethernet alapúak lesznek és a szolgáltatások igény szerinti sokszínűségét (adat, hang, videó, bérelt vonal stb.) az előfizetőknél telepített IAD eszközök nyújtják, Ethernet/IP felett.

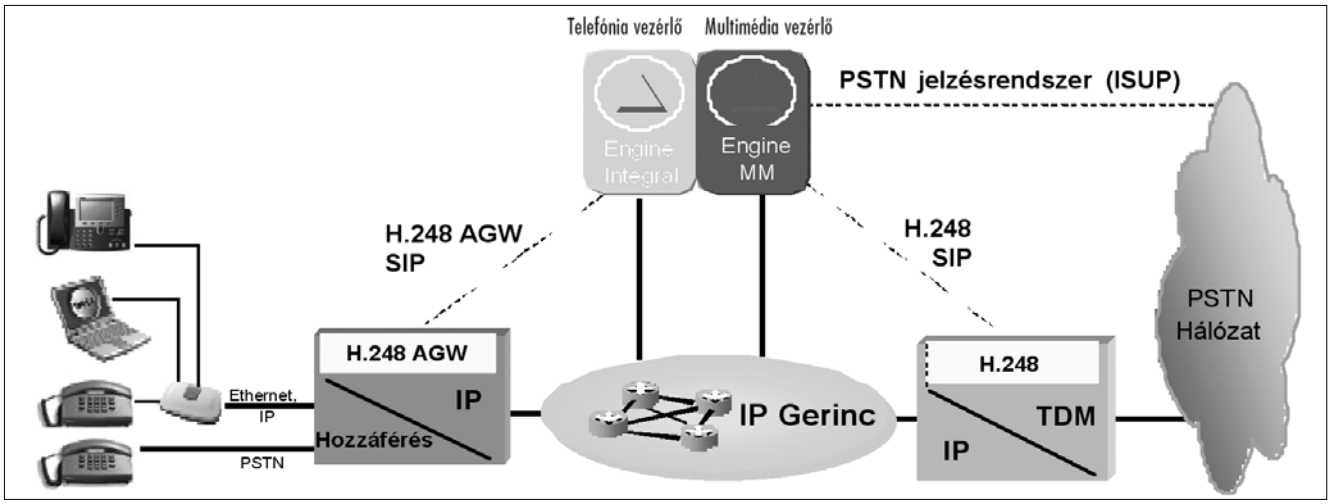
A nyilvános Ethernet hálózatok előnyeivel több kiadvány, cikk is foglalkozik [3,4], ezért ezeket itt nem kívánjuk taglalni. Mára már Magyarországon is minden vezetékes szolgáltató felismerte a nyilvános Ethernet hálózatok előnyeit és optikai (CWDM, DWDM) GE, 10GE transzport és aggregációs hálózatot építenek.

2.3. Vezérlés

Ebben a hálózati rétegben két komoly kihívással kell szembenéznünk:

– meg kell oldani a jelenleg használt szolgáltatások kontroll szintjének zökkenőmentes migrációját a többcélú hálózatokra, lehetőleg a meglévő beruházások megőrzésével,
– olyan merőben új kontroll-réteget kell kialakítsunk, amely a multimédiás kommunikációt támogatja.

A megoldásra jó példa az Ericsson Engine Integral/Engine Multimedia portfóliója, ahogyan azt korábban már a Híradástechnikában bemutattuk [5]. Az Engine Integral TPV eredetű telefónia vezérlője garantálja az összes meglévő PSTN szolgáltatás elérhetőségét, akár



5. ábra Telefónia és multimédia vezérlő a közös IP gerinc és Ethernet hozzáférési hálózaton

teljesen IP alapú elérési hálózat és előfizetői IAD esetén is, eleget téve a szolgáltatással járó törvényi kötelezettségeknek.

Az Engine Multimedia lehetővé teszi a multimédiás hívásokat és szolgáltatásokat (hang, videó, jelenlét, üzenetküldés stb.) ugyanazon az IP alapú gerinc- és hozzáférési hálózaton, mint amelyen az Engine Integral is működhet. Külön ki szeretnénk emelni, hogy bár számtalan multimédiás softswitch létezik, önmagában a VoIP átvitel vagy akár a SIP alapú híváskezelés nem jelenti a különböző rendszerek közötti kompatíbilitást, vagyis zárt szolgáltatói rendszereket eredményezhet (ilyen például a már említett Skype). Az Engine Multimedia a 3GPP és 3GPP2 IP Multimedia Subsystem (IMS) ajánlásai alapján készült, SIP alapú, szabványos, nyílt rendszer.

Mivel jelenleg az IMS az egyetlen általánosan elfogadott technológia, ezektől a rendszerektől várhatjuk el, hogy egyesíteni fogják az Internetet a mobil és a vezetékes távközléssel azáltal, hogy a minimálisan elvárt követelményeknek eleget tesznek: a garantált szolgáltatás minőség (QoS), a szolgáltatások számlázhatósága és számlázása, valamint a szolgáltatások kompatíbilitása és együttműködése által.

Az IMS működését, achitektúráját és alapvető szolgáltatásait [2] kimerítően tárgyalja.

2.4. Alkalmazások

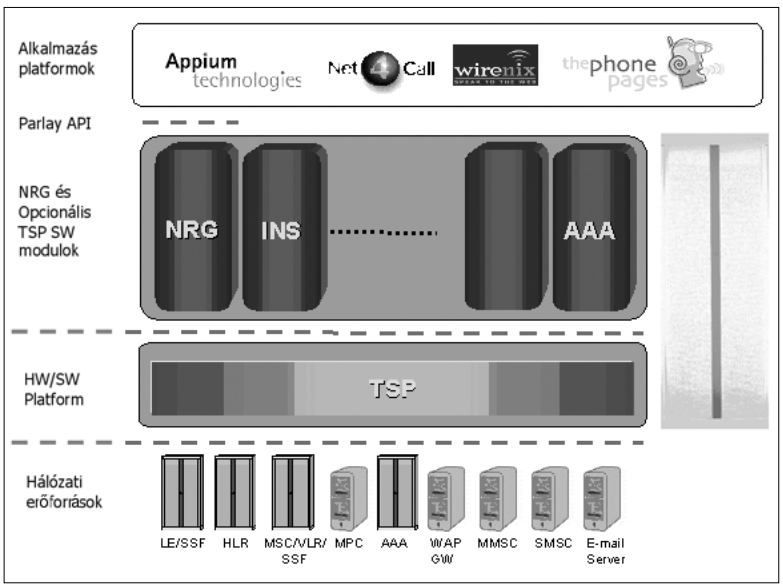
A jövő hálózataiban az alkalmazás platformok kulcsszerepet játszanak, hiszen a legalapvetőbb, szabványos szolgáltatásokon kívül minden hálózati alkalmazásért ezek felelnek. Az alkalmazás platform szolgáltatói szintű megbízhatósággal kell rendelkezzen, ugyanakkor megfelelően rugalmas kell legyen, elősegítendő a gyors alkalmazás fejlesztést és bevezetést. Ez jelenleg már csak szabványos hardver és szoftver platformokon és szabványos fejlesztőkörnyezetet használva lehetséges. Ezek garantálják egyrészt a mindig versenyképes hardvert, másrészt a programozói erőforrásokat.

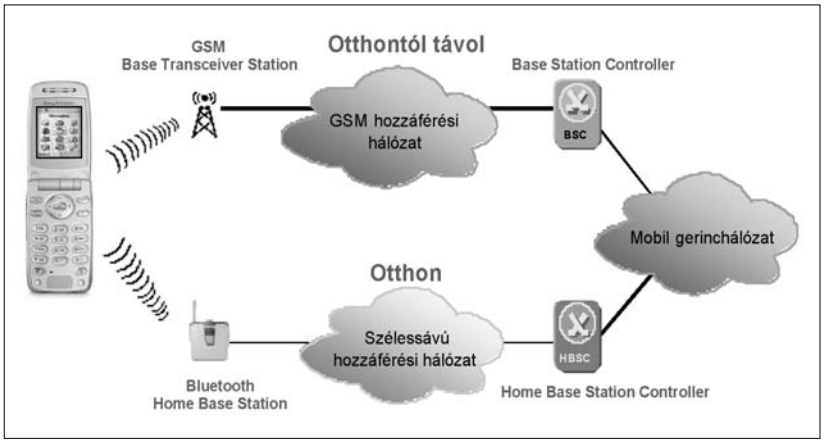
Az IMS architektúra esetén, ennek leírása tartalmazza a SIP alkalmazás szervereket is, illetve meghatározza ezek interfészeit a rendszer többi elemével (konkrétan az S-CSCF-el és a HSS-el). Ezáltal az IMS egy olyan nyitott rendszer, amely megfelel a korszerű alkalmazásfejlesztés minden követelményének.

Mit tegyünk azonban, ha már a meglévő hálózati erőforrásainkat felhasználásával szeretnénk szabványos platformon megírt alkalmazásokat fejleszteni és futtatni? Erre a kérdésre ad egy lehetséges választ az Ericsson Network Resource Gateway (NRG) megoldása. A megoldás elvi vázlata a *6. ábrán* látható.

Az NRG az Ericsson távközlési rendszerekhez kifejlesztett redundáns Telecom Server Platformján (TSP) fut. A különböző hálózati elemekkel a megfelelő protokollokat használva kommunikál, vagyis pl. a PSTN és GSM kapcsolókkal SS7 INAP, a HLR-el SS7 TCAP, míg az SMSC, WAP GW, MMSC, MPS vagy e-mail szerverekkel IP felett. Minden erőforrást elérhetővé tesz a nyitott Parlay API interfészen, ami által egyrészt lehetővé

6. ábra
A Network Resource Gateway (NRG) platform elvi vázlata





7. ábra A Mobile@Home megoldás a mobilitást ötvözi a vezetékes szélessávú hozzáféréssel

válik a különböző erőforrások egy platformon keresztüli elérése, másrészt olyan alkalmazások írását teszi lehetővé, amely több, eddig különálló erőforrást használ. Például NRG segítségével írhatunk olyan IN alkalmazást, amely e-mail vagy MMS küldést tesz lehetővé vezetékes telefonról kezdeményezett hívással. Ez esetben az alkalmazás-platformmal kiegészített NRG a vezetékes hálózat szempontjából SCP-ként viselkedik.

A megoldás nyitott szabványokon, a Parlay csoport (www.parlay.org) Parlay/OSA ajánlásain alapul. Az alkalmazások fejlesztéséhez szükséges fejlesztői csomag (SDK) szabadon letölthető az Ericsson internetes oldaláról. Számos cég sikeresen fejlesztett is NRG-re szolgáltatásokat, ilyenek a Net4Call, az Appium, a ThePonePages és a Wirenix. További információk az NRG-vel kapcsolatosan a [6] linken érhetőek el.

2.5. Fix-mobil konvergencia

A két hálózat találkozását, vagyis konvergenciáját minden gyártó vagy rendszerintegrátor másképpen közelíti meg. Próbáljuk meg rendszerezni ezeket az átfedési lehetőségeket:

1. Alkalmazási réteg szintű konvergencia: ebben az esetben ugynaz az alkalmazás szerver, ugyanazt, vagy hasonló szolgáltatást nyújt mindkét hálózatban. Ilyen lehet például egy Parlay felületű alkalmazás-platform, vitruális PBX vagy távszavazás szolgáltatást nyújtva több mobil és vezetékes hálózaton.

2. Ritkán bár, de előfordult már eddig is kontroll szintű konvergencia, vagyis amikor a hívásokat felépítő szerverek vezetékesés mobil hálózatokhoz is voltak kapcsolva. Ilyen volt, amikor egy MSC, ISDN PRA csatlakozásokon keresztül vezetékes ügyfeleket is kiszolgált. A jövőben a vonalkapcsolt-csomagkapcsolt migráció után és az IMS elterjedésével természetes lesz, hogy ez nem csak mobil vagy csak vezetékes terminálok SIP alapú kommunikációját irányítja majd. Mivel az IMS IP hálózatot használ és az IP hálózatok hozzáférés-függetlenek (GPRS, W-LAN, ADSL), valószínűleg ez lesz a vezetékes-mobil konvergencia fő csapásiránya. A 3GPP máris standard hozzáférésként emelte a W-LAN-t az IMS referencia architektúrába [2].

3. Közös transzport hálózat. Kézenfekvő (lenne) ugyanazt a csomagkapcsolt gerinchálózatot használni a vezetékes és a mobil forgalom továbbítására.

4. Hozzáférési hálózat és terminál szintű konvergencia, amikor az előfizetői eszköz több hálózatra is tud csatlakozni (pl. GSM és W-LAN, mint a Motorola MPx Wi-Fi GSM telefonja), illetve ugyanaz a szolgáltatás egy vezetékes és egy mobil hálózaton keresztül is elérhető. Erre, a más néven UMA (Unlicenced Mobile Access) alapú hozzáférésre jó példa a BT Bluephone szolgáltatásában is alkalmazott Ericsson Mobile@Home megoldás.

Ebben az esetben az előfizető az otthoni Bluetooth cellájának közelében a vezetékes szélessávú IP hálózaton keresztül éri el ugyanazokat a szolgáltatásokat (hang, SMS, MMS, WAP, WEB stb.), mint amelyeket lakhelyétől távol a GSM/GPRS/EDGE/UMTS hálózaton keresztül ér el. A szolgáltatás elméletileg minden olyan GSM telefonon keresztül igénybe vehető, amelyik támogatja a Bluetooth szabványt és telepítették bele a megfelelő Mobile@Home Bluetooth profilt és szoftvermodult. A rádiós hozzáférés váltásakor a hívások nem szakadnak meg, tehát ha az előfizető beszélgetés közben kisétál az UMA területről, akkor a GSM/UMTS hálózat átveszi a hívást.

3. Összegzés

A vezetékes és a mobil hálózatok jövőjét együttesen érdemes vizsgálni. A szélessávú hálózatok elterjedésével és az előfizetői igények változásával olyan megoldások kerülnek előtérbe, amelyek nyitott szabványokon alapulnak és kihasználják a vezetékes Ethernet /IP hálózatok lehetőségeit. Az új üzleti modellek kiaknázása és a gyors alkalmazásfejlesztés elengedhetetlen feltételei az üzleti sikernek.

Irodalom

[1] Wikipedia, the Free Encyclopedia
http://en.wikipedia.org
[2] Gonzalo Camarillo, Miguel A. Garcia-Martin:
The 3G IP Multimedia Subsystem,
John Wiley&Sons Ltd., England, 2004.
[3] Michael Bergley: The Public Ethernet –
The next generation broadband access network,
Ericsson Review, No.01, 2004.
www.ericsson.com/about/publications/review/2004_01
[4] Bordás Csaba: Ethernet hozzáférés
13. távközlési és informatikai hálózatok szeminárium
és kiállítás, Előadások gyűjteménye, HTE, 2002.
[5] Bordás Csaba: Távközlési hálózatok konvergenciája,
Híradástechnika, 2003/10.
[6] Parlay and Ericsson Network Resource Gateway
www.ericsson.com/mobilityworld/sub/open/technologies/
parlay/index.html

Ad hoc útvonalválasztó protokollok biztonsága

ÁCS GERGELY, BUTTYÁN LEVENTE, VAJDA ISTVÁN

Budapesti Műszaki és Gazdaságtudományi Egyetem, Híradástechnikai Tanszék, CrySyS laboratórium
{acs, buttyan, vajda}@crysys.hu

Kulcsszavak: ad hoc hálózatok, forrás alapú ad hoc útvonalválasztás, bizonyított biztonság, szimulációs paradigma

A cikkben egy olyan formális módszert mutatunk be, amellyel az ad hoc hálózatok számára javasolt, igény szerinti, forrásalapú útvonalválasztó protokollokat (on-demand source routing) lehet biztonsági szempontból elemezni. A módszer alapját a szimulációs paradigma adja, mely egy jól ismert, általános eljárás kriptográfiai protokollok biztonságának bizonyítására. Formálisan megfogalmazzuk, hogy mit értünk biztonságos útvonalválasztás alatt, melyhez felhasználjuk a statisztikai megkülönböztethetetlenség fogalmát. A gyakorlati alkalmazást egy példán keresztül szemléltetjük, melyben ismertetjük az endairA útvonalválasztó protokoll működését, és bebizonyítjuk, hogy a protokoll biztonságos az általunk definiált modellben.

1. Bevezetés

Az ad hoc hálózat egyenrangú csomópontokból álló, előre telepített infrastruktúrával nem rendelkező, vezeték nélküli hálózat, melyben a csomópontok terminál- és hálózati funkciókat egyaránt ellátnak. A csomópontok gyakran korlátozott energia ellátással (elemmel, akkumulátorral) rendelkeznek. Ezért, és a rádió kapcsolatok miatt fellépő interferencia csökkentése érdekében, az ad hoc hálózat csomópontjai multihop kommunikációt használnak. Infrastruktúra hiányában, a multihop kapcsolathoz szükséges útvonalválasztó és -karbantartó feladatokat maguk a csomópontok végzik.

Az útvonalválasztásnak alapvetően két formáját lehet megkülönböztetni: a pro-aktív és a reaktív (vagy igény szerinti) eljárásokat. Jelen cikkben az utóbbi típussal foglalkozunk. Reaktív útvonalválasztás során egy kapcsolatot kezdeményező csomópont csak igény esetén próbál útvonalat találni a célcsomópont felé. Ekkor a kezdeményező csomópont egy útvonalkéréssel (route request – *rreq*) árasztja el a hálózatot. A kérést minden csomópont megkapja, majd ahhoz saját azonosítóját hozzáadva, többesküldéssel (broadcast) továbbítja. A célcsomóponthoz érkező kérésüzenetekre, a célcsomópont egy (vagy több) útvonalválasszal (route reply – *rrep*) válaszol, mely tartalmazza a kérésben rögzített csomópontazonosítók sorozatát, azaz a felfedezett útvonalat. A válasz a kérés által követett útvonal fordítottján jut vissza a kezdeményező csomóponthoz.

A biztonságos útvonalválasztás feladata ezen mechanizmus helyes működésének megvalósítása támadó jelenlétében. Ez elsődleges fontosságú, mivel az útvonalválasztó mechanizmus manipulálásával egy támadó viszonylag kevés erőforrás felhasználásával az egész hálózatot működésképtelenné teheti.

Az irodalomban számos biztonságosnak mondott útvonalválasztó protokoll jelent meg ([3] jó áttekintést ad a területről), ám ezen protokollok szerzői formálisan nem igazolták állításaikat. Tudomásunk szerint [2] az első olyan munka, melyben ad hoc útvonalválasztó protokollok elemzésére precíz matematikai modell jelent meg. [2]-ben a szerzők megmutatták két irodalomban javasolt protokollról (SRP, Ariadne), hogy azok támadhatóak, és javasoltak egy új protokollt, melyről bebizonyították, hogy az biztonságos. A [2]-ben használt módszer alapját a szimulációs paradigma adja, mely egy jól ismert eljárás a kriptográfiai protokollok biztonságának bizonyítására [4,5]. A [2]-ben definiált modell azonban csak egy korlátozott Aktív-1-1 támadót enged meg, mely egyetlen kompromittált csomópontot és egyetlen kompromittált azonosítót használhat. További megkötés, hogy a támadó egyidejűleg csak egy útvonalválasztási folyamat végrehajtását támadhatja.

Jelen cikkben a [2]-ben használt modellt általánosítjuk tetszőleges Aktív-*y*-*x* támadó esetére, megengedve párhuzamos protokollfutásokat is. Megmutatjuk továbbá, hogy a [2]-ben javasolt endairA protokoll ebben a bővített modellben is biztonságos. Itt elsősorban csak a fő gondolatokat írjuk le; a munka részletesebb leírását [1] tartalmazza.

2. A modell

2.1. A hálózat modellezése

Az útvonalválasztás vizsgálata során az ad hoc hálózatot statikusnak tekintjük és egy G(*E,V*) gráffal modellezük, ahol a csúcsoknak egyértelműen megfelelnek az egyes hálózati csomópontok, és két csúcs között akkor és csak akkor van él, ha az azoknak megfeleltetett csomópontok hallják egymás adását, vagyis szomszédosak. Feltesszük, hogy a hálózat minden csomópontja rendelkezik egy azonosítóval, amely egyértelműen azonosítja a csomópontot a hálózatban (ez lehet például egy publikus kulcs). Feltesszük, hogy az azonosítók hitelesítettek, de néhány azonosító kompromittálódott, s az ezek hitelesítéshez szükséges kulcsok a tá-

madó birtokába jutottak. A támadót is tartalmazó hálózatot röviden *konfigurációnak* hívjuk. Formálisan a konfiguráció egy ($G(E,V)$, V^*, L) hármas, ahol $G(E,V)$ a hálózatot reprezentáló gráf, a $V^* \subset V$ a támadó irányítása alatt álló csomópontok halmaza, L pedig egy olyan függvény, amely mindegyik csúcshoz hozzárendeli a hozzátartozó csomópont által birtokolt azonosítók halmazát. Megbízható csomópontok esetén ezek egy elemű halmazok, míg a támadó irányítása alatt álló minden csomóponthoz az összes kompromittált azonosítót tartalmazó halmazt rendeljük.

2.2. A támadó modellezése

A támadóról az alábbiakat feltételezzük:

- fizikailag nem lehet mindenütt jelen, ezért nincs irányítása a teljes hálózat felett;
- x csomópontot irányít és y kompromittált azonosítót birtokol (Aktív-y-x támadó, ahol $x,y \geq 1$);
- a birtokában levő kompromittált azonosítók halmaza és a megbízható csomópontok azonosítóinak halmaza diszjunkt;
- kommunikációs képességeit tekintve egy átlagos csomópont képességeivel rendelkezik, azaz a támadó csomópontok csak szomszédaiknak tudnak üzenetet küldeni és csak azok adását hallják;
- aktív, abban az értelemben, hogy nemcsak üzeneteket hallgat le, hanem képes új üzenetek megalkotására és beszúrására is, valamint képes üzeneteket módosítani, késleltetni stb.;
- nem adaptív abban az értelemben, hogy az egyes protokollfutások ellen végrehajtott támadásai egymástól függetlenek.

Az útvonalválasztást kezdeményező csomópontról és a célcsomópontról feltesszük, hogy megbízhatóak.

2.3. A plauzibilis útvonal definíciója

A biztonság fogalmának definiálása nem egyértelmű feladat. Egy kézenfekvő megoldás lehet az optimális (egyes esetekben a legrövidebb) útvonalak visszaadásának követelménye, ez viszont az eltérő csomóponti késleltetések és a szinte mindig alkalmazott optimalizációk miatt irreális [2]. Továbbá az is látható, hogy nem tudjuk megakadályozni (az útvonalválasztás szintjén), hogy a támadó az általa birtokolt azonosítók közül tetszőleges számút hozzáadjon egy lehallgatott útvonalkéréshez, és hasonlóan nem tudjuk megakadályozni a szomszédos támadó csomópontok kooperációját sem [1]. Látható tehát, hogy bizonyos támadások ellen egyáltalán nem tudunk védekezni, vagy ha tudunk, akkor a gyakorlati esetek többségében a védelem kialakítása túl költséges lenne. Ezért körültekintően kell megadni a biztonság fogalmát: ha túl szigorú definíciót adunk, akkor a fent említett elkerülhetetlen támadások miatt egyetlen protokoll sem fogja kielégíteni definíciónkat, míg ellenkező esetben olyan protokollt is biztonságosnak nyilváníthatunk, mely nemcsak az elkerülhetetlen támadások ellen védtelen.

E problémát úgy oldjuk meg, hogy a „helyes” útvonal fogalmába „beépítjük” az elkerülhetetlen támadások hatásait. A „helyes” útvonalakat *plauzibilis* útvonalaknak nevezzük és az alábbi módon definiáljuk.

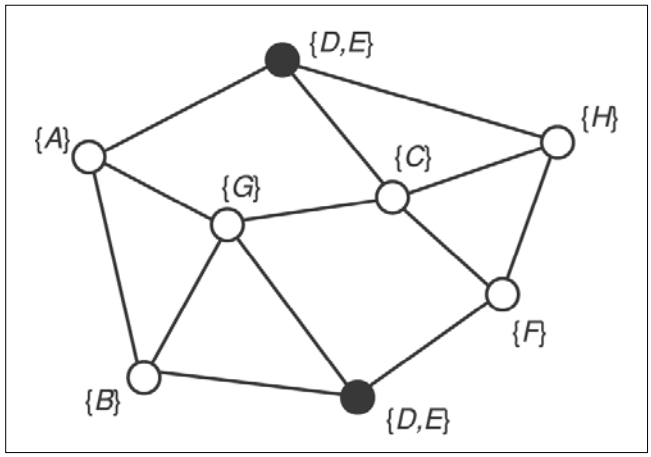
Minden konfiguráció egyértelműen redukálható egy olyan másik konfigurációra, amelynek megfeleltetett gráf nem tartalmaz szomszédos támadó csomópontokat. Más szavakkal a redukált konfigurációban összevonjuk a szomszédos támadó csomópontoknak megfeleltetett csúcsokat. A redukált konfigurációhoz tartozó redukált gráfot $\underline{G}$-vel jelöljük.

Definíció:

Egy útvonalat alkotó csomópontazonosítók sorozata akkor plauzibilis, ha

– nem tartalmaz ismétlődő azonosítókat és

– particionálható olyan részsorozatokra, amely részsorozatok egyértelműen hozzárendelhetőek olyan csúcsokhoz a redukált gráfban, hogy ezen csúcsoknak megfeleltetett csomópontok rendelkeznek a hozzájuk tartozó partíció összes azonosítójával, és ezen csúcsok egy útvonalat alkotnak a redukált gráfban.



1. ábra

A csúcsösszevonás valamint a plauzibilis útvonal definíciójának értelmét a fentebb tárgyalt elkerülhetetlen támadások adják. Az *1. ábrán* egy redukált konfiguráció látható. A telített csúcsok reprezentálják az összevont támadó csomópontokat, melyek a D és E kompromittált azonosítóval rendelkeznek. Látható, hogy ebben a konfigurációban az A,D,E,C,F útvonal plauzibilis, melynek egy helyes particionálása $A|D,E|C|F$, viszont A,B,D,E,H nem plauzibilis útvonal, hiszen az E és H azonosítónak megfeleltetett csomópontok nem szomszédosak.

2.4. A szimulációs paradigma

A modell egy sarkalatos pontja a biztonság fogalmának precíz definiálása. Erre a széleskörben használt szimulációs paradigmát [4,5] szeretnénk alkalmazni. A szimulációs paradigma alapja, hogy egy valós és egy ideális modellt definiálunk, ahol a valós modell leírja a protokoll valóságos működését, míg az ideális modell azt reprezentálja, hogy mit várunk el egy biztonságos (ideális) protokolltól. A valós modellre gondolhatunk úgy, mint a protokoll implementációjára, míg az ideális mo-

dellt tekinthetjük a feladat specifikációjának. Mindkét modellnek része egy támadó is. Az ideális modellbeli támadó reprezentálja az elkerülhetetlen támadásokat. Ezzel szemben, a valós modellbeli támadó erejét nem korlátozzuk, csak annyiban, hogy a valós támadó által végrehajtható lépések száma az alkalmazott biztonsági paraméter polinomiális függvénye kell legyen.

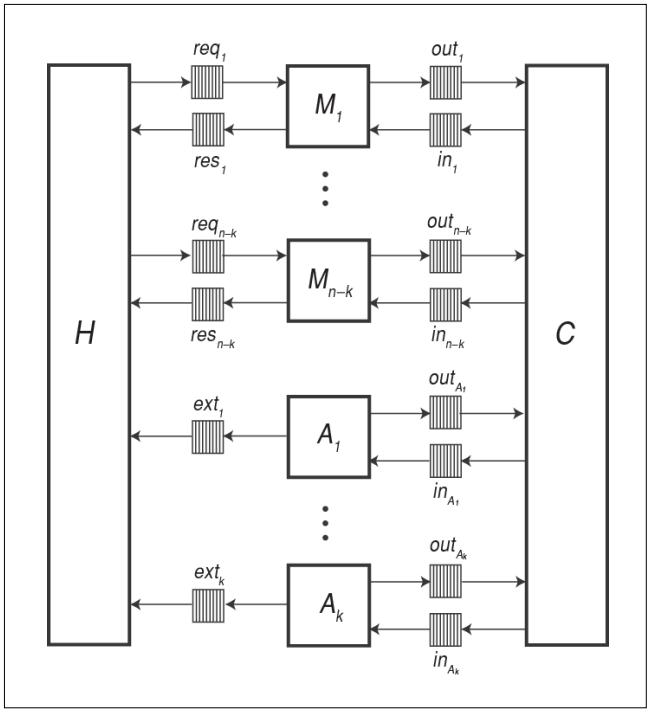
Egy protokollt ezek után akkor tekintünk biztonságosnak, ha a valós és az ideális modellek megkülönböztethetetlenek a becsületes résztvevők számára. Precízebben, egy protokoll akkor biztonságos, ha bármely valós modellbeli A támadóhoz létezik olyan ideális modellbeli A' támadó, hogy minden amit A elér a valós modellben, azt A' is eléri az ideális modellben ugyanolyan mennyiségű erőforrással. Más szavakkal bármely valós támadó tevékenységének hatását szimulálni lehet az ideális modellben. Mivel azonban az ideális modellben definíció szerint csak az elkerülhetetlen támadások lehetségesek, ezért következik, hogy ennél többet egy valós támadó sem tud elérni a valós modellben.

A szimulációs paradigmának megfelelően a következőkben definiáljuk az ad hoc útvonalválasztás valós és ideális modelljét, majd pontosan megadjuk, hogy milyen értelemben követeljük meg a kettő megkülönböztethetetlenségét.

2.5. A valós modell

A valós modellt a *2. ábra* szemlélteti. A modell interaktív és véletlenszerű Turing gépekből épül fel, melyek közös szalagok segítségével kommunikálnak. Az egyes gépek az egyes protokoll résztvevők, valamint a támadó működését és kommunikációját modellezik. $M_1,\ldots,M_{n-k}$ reprezentálja a megbízható működésű csomópontokat, melyek pontos működése az adott útvonalválasztó protokolltól függ.

2. ábra A valós modell

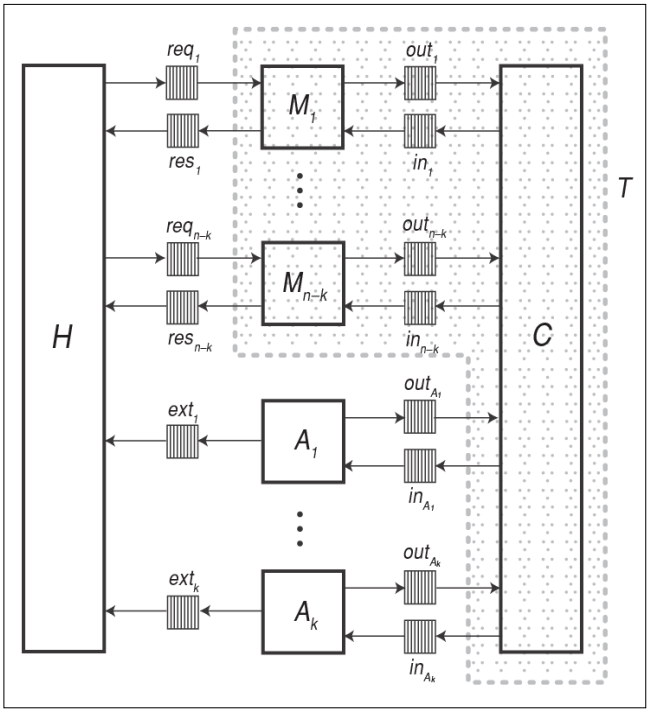


$A_1,\ldots,A_k$ a támadó csomópontokat reprezentálja, melyek tetszőleges polinom idejű gépek lehet. C gép modellezi a kommunikációs kapcsolatokat (azaz $\underline{G}$ éleit). C feladata, hogy az egyes gépek kimeneti szalagjain (out_i és out_{Aj}) megjelenő protokollüzeneteket átmozgassa a gépek ($\underline{G}$ szerinti) szomszédainak bementi szalagjára ($in_{i'}$ és $in_{Aj'}$). Végül H reprezentálja az útvonalválasztás feletti protokollrétegeket (és a becsületes felhasználókat). A modellben H kezdeményezi az útvonalválasztó protokoll futtatását a req_i szalagokra elhelyezett kérésekkel, melyekre a választ a res_i szalagokon kapja meg. Az ext_j szalagokra írt utasítások segítségével a támadó befolyásolni tudja, hogy a becsületes felhasználók mely csomópontokról indítsanak útvonalválasztást és mely csomópontok felé. Mivel azonban a támadó nem adaptív, ezeket a szalagokat csak a végrehajtás elején használhatja, s így az itt elhelyezett befolyásoló utasítások nem függnek a támadó által később megfigyelt üzenetektől.

Minden gép kezdetben inicializálódik valamilyen bemeneti adattal (például kriptográfiai kulcsokkal) és valamilyen véletlen bemeneti adattal (ami a véletlenszerű működéshez szükséges). A gépek reaktív módon működnek, azaz aktiválni kell őket ahhoz, hogy elvégezzék a feladatukat. Aktiválás során, egy gép először beolvassa a bemeneti adatokat a bemeneti szalagjairól, majd állapottranzíciók után valamilyen kimenetet generálhat a kimeneti szalagjaira. Ezután visszatér inaktív állapotba, s várja a következő aktiválást. A gépeket egy feltételezett, hipotetikus ütemező aktiválja menetekben, előre meghatározott sorrendben. A számításnak akkor van vége, amikor H eléri az elfogadó állapotát.

A valós modell kimenete a H-nak visszaadott útvonalak halmaza, amit adott *conf* konfiguráció és A támadó esetén $real\_out_{conf,A}(r)$-rel jelölünk.

3. ábra Az ideális modell



Itt $r = (r_I, r_{M1}, ..., r_{Mn-k}, r_{A1}, ..., r_{Ak}, r_C)$ az egyes gépek véletlen bemeneteit tartalmazó vektor és r_I a kriptográfiai kulcsok generálásánál használt véletlen bemenet. $real\_out_{conf,A}$ jelöli a kimenetet leíró valószínűségi változót, amikor *r*-et egyenletes eloszlás szerint választjuk.

2.6. Az ideális modell

Az ideális modellt a *3. ábra* szemlélteti. Mint látható, az ideális modell felépítése hasonlít a valós modell felépítéséhez, ezért itt csak a különbségeket említjük:

- Mielőtt *C'* egy M_i gép in_i szalagjára helyezne egy útvonalválaszt (rrep), ellenőrzi, hogy az tartalmaz-e nem-plauzibilis útvonalat. Ha igen (és csak ekkor) megjelöli korruptként az üzenetet. Egyébként *C'* úgy működik mint *C*.
- Amikor M_i' egy olyan útvonalválaszt kap, amelyhez tartozó útvonalkérést ő kezdeményezte, akkor az üzeneten először elvégzi a protokoll által megkövetelt ellenőrzéseket. Ha ezek sikeresek, akkor ellenőrzi, hogy az üzenet meg van-e jelölve korrupciós jelzővel. Ha igen, akkor M_i' eldobja az üzenetet. Egyébként M_i' úgy viselkedik mint M_i.

  Az ideális modell kimenete a *H*-nak visszaadott útvonalak halmaza. A kimenetet $ideal\_out_{conf,A}(r')$-vel jelöljük, ahol *r'* értelmezése a valós modell esetéhez hasonló. $ideal\_out_{conf,A}$ jelöli a kimenetet leíró valószínűségi változót, mikor *r'*-t egyenletes eloszlás szerint választjuk.

Mint az a leírásból látható, az ideális modellben *H* soha nem kap vissza olyan útvonalválaszt, mely nemplauzibilis útvonalat tartalmaz. Az ideális modellt pontosan ebben az értelemben értjük ideálisnak.

2.7. A biztonságos útvonalválasztás formális definíciója

Az elkerülhetetlen támadásokkal kapcsolatos megjegyzéseket figyelembe véve, egy biztonságos útvonalválasztó protokolltól azt várjuk el, hogy az csak elenyésző valószínűséggel adjon vissza nem-plauzibilis útvonalakat. Formálisan, a fent bevezetett két modell segítségével, és a szimulációs paradigma szellemében, ezt a következőképpen írhatjuk le:

Definíció:
Az útvonalválasztó protokoll akkor biztonságos, ha bármely conf konfigurációhoz és bármely A valós támadóhoz létezik egy olyan A' ideális támadó, hogy $ideal\_out_{conf,A}$ *és* $real\_out_{conf,A'}$ *eloszlások statisztikailag megkülönböztethetetlenek.*

Vegyük észre, hogy nem az eloszlások pontos egyezését követeljük meg, hiszen azt a gyakorlatban egyetlen protokoll sem tudná garantálni, mivel a támadó, bár elenyésző valószínűséggel, de mindig képes sikeres támadást végrehajtani az alkalmazott kriptográfiai primitívek ellen (például megtippel egy digitális aláírást). Megjegyezzük még, hogy a fenti definíció gyengíthető, ha statisztikai megkülönböztethetetlenség helyett számításelméleti megkülönböztethetetlenséget követelünk meg. Jelen cikkben azonban erre nem lesz szükségünk.

3. Az endairA biztonsága

Ebben a fejezetben, az eddigieket egy rövid példán keresztül szeretnénk szemléltetni. Először röviden ismertetjük az endairA protokollt [2,1], majd bebizonyítjuk, hogy az biztonságos a fenti értelemben. A protokoll működését szemléltetik a következő üzenetek, ahol sig_x jelöli az *x* azonosítójú célcsomópont digitális aláírását az üzeneten, *id* pedig egy nem predikálható véletlen tranzakció-azonosító:

Útvonalkérés:
S→* : [rreq, S, D, *id*, ()]
B→* : [rreq, S, D, *id*, (B)]
C→* : [rreq, S, D, *id*, (B, C)]
Útvonalválasz:
D→ C : [rrep, S, D, *id*, (B, C), (sig_D)]
C→ B : [rrep, S, D, *id*, (B, C), (sig_D, sig_C)]
B→ S : [rrep, S, D, *id*, (B, C), (sig_D, sig_C, sig_B)]

Kezdetben az útvonalkeresést kezdeményező **S** csomópont küld egy *rreq* útvonalkérést, ami tartalmazza saját és a **D** célcsomópont azonosítóját, egy frissen generált véletlen tranzakció-azonosítót, és egy üres azonosítólistát. Minden egyes közbenső csomópont, mely megkapja a kérést, hozzáfűzi saját azonosítóját a kérésben található azonosítólistához, majd a kérésüzenetet többesküldéssel (broadcast) továbbítja. Amikor a kérés eléri a célt, az egy *rrep* útvonalválaszt generál. A válasz tartalmazza a kezdeményező és a cél azonosítóját, valamint a kérésben talált tranzakció-azonosítót és azonosítólistát (azaz a felfedezett útvonalat). A választ a célcsomópont digitális aláírásával látja el. A válaszüzenetet minden érintett csomópont az üzenetben található útvonal fordítottján továbbítja a megfelelő szomszédos csomópontnak. Továbbítás előtt azonban minden közbenső csomópont ellenőrzi a következőket:

– szerepel-e a saját azonosítója az útvonalban;
– a saját azonosítóját követő és megelőző azonosítók valóban szomszédos csomópontokhoz tartoznak-e;
– a **D** célcsomópont aláírása helyes-e.

Ha minden ellenőrzés sikeres, akkor a közbenső csomópont aláírja a válaszüzenetet, majd továbbítja azt. Ellenkező esetben eldobja a válaszüzenetet továbbítás nélkül. Amikor a kezdeményező megkapja a válaszüzenetet, ellenőrzi, hogy

– az útvonalban szereplő első azonosító valóban egy szomszédos csomópont azonosítója;
– az útvonalban szereplő minden azonosítóhoz található aláírás az üzenetben;
– minden aláírás helyes.

Ha minden ellenőrzés sikeres, akkor a kezdeményező elfogadja a válaszüzenetben kapott útvonalat.

Az alábbi tétel az endairA protokoll biztonságára vonatkozik:

Tétel:
Az endairA útvonalválasztó protokoll statisztikailag biztonságos, ha a felhasznált digitális aláíró séma biztonságos választott nyílt szövegű támadás esetén.

Bizonyításvázlat:

Egy útvonalválasztó protokoll statisztikailag biztonságos, ha nem-plauzibilis útvonalat csak elhanyagolható valószínűséggel ad vissza bármely *conf* konfigurációra és bármely *A* támadó esetén. Pontosabban azt kell belátni, egy *rrep* üzenet az ideális rendszerben elhanyagolható valószínűséggel kerül eldobásra a korrupciós jelző miatt.

Tegyük fel, hogy a következő üzenet eldobásra kerül a korrupciós jelzője miatt az ideális rendszerben, míg a valós modellben nem:

$[\ \text{rrep}, S, D, id, (N_1, N_2, \ldots, N_p), (sig_D, sig_{Np}, \ldots, sig_{N1})\ ]$

Ekkor a következőket állapíthatjuk meg:
- nincs ismétlődő azonosító a $\pi=(S, N_1, N_2, \ldots, N_p, D)$ útvonalban;
- N_1 csomópont S szomszédja;
- minden aláírás érvényes;
- S és D megbízható csomópontok;
- minden köztes csomópont (nagy valószínűséggel) azt az útvonalat látja amit D küldött (azaz π-t), mivel D azt aláírta, és ezt mindegyik csomópont ellenőrzi;
- ennek ellenére π egy nem plauzibilis útvonal $\underline{G}$ gráfban, ahol $\underline{G}$ a redukált konfiguráció gráfja.

Bebizonyítjuk, hogy ez csak úgy lehetséges ha az A támadó hamisította legalább egy megbízható csomópont aláírását. Tudjuk, hogy a redukált konfiguráció gráfjában nincsenek szomszédos támadó csomópontoknak megfelelő szomszédos csúcsok. Így a π útvonal egyértelműen particionálható részsorozatokra a plauzibilis útvonal definíciója szerint mégpedig úgy, hogy minden megbízható csomóponthoz tartozó azonosító külön partíciót alkot, míg a szomszédos kompromittálódott azonosítók szintén külön partíciót alkotnak. Ha a π útvonal nem plauzibilis, akkor a következő állítások közül legalább egy igaz:

1. $P_j = \{N_i\}$ és $P_{j+1} = \{N_{i+1}\}$ megbízható csomópontokhoz tartozó partíciók, mely csomópontok nem szomszédosak $\underline{G}$ gráfban.
2. $P_j = \{N_i\}$ egy megbízható v csomóponthoz tartozó partíció, míg P_{j+1} egy v' támadó csomóponthoz tartozó partíció, és az N_i azonosítóhoz tartozó v csomópontnak
   a) nincs szomszédja $\underline{V}^*$ csúcshalmazban
   b) van szomszédja $\underline{V}^*$ csúcshalmazban.
3. P_j egy v' támadó csomóponthoz tartozó partíció, míg $P_{j+1} = \{N_i\}$ egy megbízható v csomóponthoz tartozó partíció, és az N_i azonosítóhoz tartozó v csomópontnak
   a) nincs szomszédja $\underline{V}^*$ csúcshalmazban
   b) van szomszédja $\underline{V}^*$ csúcshalmazban.

Az 1., 2.a, és 3.a esetekben v becsületes csomópont detektálja, hogy v' egy nem szomszédos csomópont, így nem írja alá az üzenetet. Ezért S csak úgy kaphatta ezt az üzenetet, hogy a támadó hamisította az N_i-hez tartozó aláírást. 2.b és 3.b esetben v szomszédja legyen q, ahol q támadó csomópont, melynek azonosítója legyen v' azonosítója. q és v' nem lehetnek szomszédosak, ezért q csak úgy járhat sikerrel, ha egy új üzenetet konstruál és így meghamisítja D aláírását.

Ezért arra jutottunk, hogyha az ideális modellben nem-elenyésző valószínűséggel fordul elő egy ilyen válaszüzenet, akkor a támadó nem-elenyésző valószínűséggel hamisítani képes valamelyik becsületes résztvevő aláírását, ez pedig ellentmond azon feltevésünknek, hogy az alkalmazott aláírás séma biztonságos.

4. Összegzés

A cikkben egy olyan modellt mutattunk be, melyben precízen definiálható, hogy mit értünk biztonságos útvonalválasztás alatt, és így lehetőség nyílik annak igazolására (vagy cáfolására), hogy egy adott, igény szerinti, forrás alapú, ad hoc útvonalválasztó protokoll biztonságos-e. A módszer gyakorlatban történő használatát egy példán keresztül szemléltettük, melyben igazoltuk, hogy az endairA protokoll biztonságos.

A jövőben hasonló modellt szeretnénk kidolgozni a táblázat alapú ad hoc útvonalválasztó algoritmusokra is (például SEAD, ARAN, S-AODV). Továbbá szeretnénk a bizonyításokat automatizálni valamilyen alkalmas formális nyelv (például processz algebra) és kapcsolódó ellenőrző eszköz segítségével.

Köszönetnyilvánítás

A bemutatott munka támogatói a következők voltak: OM (BÖ2003/70), OTKA (T046664), és IKMA.

Irodalom

[1] Ács G.,
Ad hoc útvonalválasztó protokollok bizonyított biztonsága, TDK dolgozat, 2004. nov. 9.

[2] L. Buttyán, I. Vajda,
Towards provable security for ad hoc routing protocols, In Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks, Washington DC, USA, October, 2004.

[3] Y.-C. Hu, A. Perrig,
A survey of secure wireless ad hoc routing, IEEE Security and Privacy Magazine, June 2004.

[4] O. Goldreich,
The Foundations Of Modern Cryptography, Cambridge University Press, 2001.

[5] M. Bellare, R. Canetti, H. Krawczyk,
A modular approach to the design and analysis of authentication and key exchange protocols, In Proceedings of the ACM Symposium on the Theory of Computing, 1998.

Latin négyzetek alkalmazásai a titkosításban

DÉNES TAMÁS

tdenest@freemail.hu

Kulcsszavak: korai módszerek, latin négyzetek tulajdonságai, kódfejtés

A rejtjelző rács figyelemreméltó „divattá” vált évszázadokon keresztül a kriptográfiában. A Cardano-rács történetét és alkalmazását a titkosításban e folyóirat már közölte [5], ezért jelen dolgozatom a permutációs mátrixokkal és latin négyzetekkel való kapcsolatát mutatja be, amely egyúttal rávilágít eme 450 éves találmány 21. századi rendkívüli lehetőségeire. A digitális technika új perspektívákat nyit a sztegonográfiának és ezen belül a rejtjelző rácsoknak is.

Girolamo Cardano (1501–1576) korszakos és mai napig ható módszercsaládja – amely a sztegonográfia [6] új ágát indította útjára –, a róla elnevezett *Cardano-rács.* Tulajdonképpen egy *betűmátrixra helyezhető sablonról* van szó. A pontosabb megértéshez idézzük fel magának Cardanonak a szavait:

„Végy két azonos méretű pergamen lapot és azonos vonalak mentén készíts kivágásokat különböző helyeken. Ezek a kivágások legyenek kicsik, de mégis legalább akkorák, mint az ABC nagybetűi. Az összes kivágásokba összesen 120 betűt lehessen elhelyezni. Az egyik pergamen lapot majd a levelező társadnak adod. Amikor alkalom adódik, először írd az üzenetedet olyan tömören, ahogy csak lehetséges, így az üzenet kevesebb betűt is tartalmazhat, mint amennyi a kivágott ablakokban elhelyezhető. Amikor beírtad az üzeneted az egyik pergamen lapra, tedd ugyanezt a másikkal is. Ezután töltsd ki az első lapon az üresen maradt helyet úgy, hogy teljes mondatokra egészítsék ki a már ráírt szöveget. Ez a kitöltés úgy történjen, hogy a teljes szöveg stílusa és tartalma összefüggő és egységes legyen. Amikor a levelező társad megkapja a te üzenetedet, ráhelyezi a megfelelő kivágásokkal ellátott pergament és így elolvashatja az üzenetet.”

Latin négyzetek és permutációs mátrixok kapcsolata

Egy P(n) nxn-es, (0,1)-es mátrixot *permutációs mátrix*nak nevezünk, ha a mátrix pontosan *n* darab *1*-t tartalmaz úgy, hogy minden sorban és oszlopban pontosan egy darab *1* lehet, a többi elem nulla.

Érdekes és a rejtjelző-rácsok szempontjából fontos eredmény az alábbi:

Egy L(n) nxn-es latin négyzet kölcsönösen-egyértelműen felbontható *n* darab permutációs mátrix összegére [2,3], azaz

$$L(n) = 1 \bullet P_{i1} + 2 \bullet P_{i2} + \ldots + n \bullet P_{in} \qquad (1)$$

ahol P_{ik} az i_k-adik permutációs mátrix, azaz a mátrixban *1* szerepel mindenhol, ahol L(n)-ben *k* van, *a mátrix többi eleme nulla*. (A „+” összeadás művelet a mátrixok összeadását, míg a „•” szorzás a mátrixok skalár szorzását jelöli.)

Ezen megfeleltetések következménye, hogy az így adódó permutációs mátrixok jól felhasználhatók rejtjelző rácsként. A következő szemléltető példában a (2)-beli L(4) latin négyzet P_1, P_2, P_3, P_4 permutációs mátrixokra való egyértelmű felbontása látható:

$$L(4) = \begin{matrix} 1&2&3&4 \\ 3&4&2&1 \\ 2&1&4&3 \\ 4&3&1&2 \end{matrix} \qquad (2)$$

(3)

$$P_1 = \begin{matrix} 1&0&0&0 \\ 0&0&0&1 \\ 0&1&0&0 \\ 0&0&1&0 \end{matrix} \quad P_2 = \begin{matrix} 0&1&0&0 \\ 0&0&1&0 \\ 1&0&0&0 \\ 0&0&0&1 \end{matrix} \quad P_3 = \begin{matrix} 0&0&1&0 \\ 1&0&0&0 \\ 0&0&0&1 \\ 0&1&0&0 \end{matrix} \quad P_4 = \begin{matrix} 0&0&0&1 \\ 0&1&0&0 \\ 0&0&1&0 \\ 1&0&0&0 \end{matrix}$$

A rejtjelző rács tulajdonképpen egy betűkeverési rejtjelző eszköz, amely az úgynevezett nyílt szöveg betűit egy betűmátrixba képezi le. Mindegyik P_i permutációs mátrix egy rejtjelző rácsként fogható fel, ahol az *1*-esek helyén „ablakok” vannak.

Példaként legyen a nyílt szöveg a „SZIA” és használjuk a P_1 permutációs mátrixot rejtjelző rácsként. Ekkor egy tetszőleges *B 4x4*-es betűmátrixban hagyjuk üresen azokat a cellákat, ahol P_1-ben *1*-es van (ezek a rejtő „ablakok”).

$$B = \begin{matrix} [\,] & E & I & M \\ B & F & J & [\,] \\ C & [\,] & K & O \\ D & H & [\,] & P \end{matrix} \qquad (4)$$

Majd az „ablakokba” balról-jobbra, fentről-lefelé írjuk be a nyílt szöveget, így kapjuk a P_1-nek megfelelő ráccsal rejtjelzett B_1 betűmátrixot.

$$B_1 = \begin{matrix} S & E & I & M \\ B & F & J & Z \\ C & I & K & O \\ D & H & A & P \end{matrix} \qquad (5)$$

Így a permutációs mátrixok (mint rácsok) egymás utáni betűmátrixra helyezésével tudjuk a kívánt szöveget a betűmátrixba írni és a fordított eljárással kiolvas-

ni. Mivel a latin négyzetekre vonatkozó fenti egyértelmű felbontási tétel miatt az így készített rácsok ablakai pontosan lefedik a betűmátrix n^2 mezőjét, ezzel a módszerrel elértük, hogy a teljes betűmátrixot kitölthetjük rejtett szöveggel. További előny, hogy a latin négyzet felbontásának egyértelműsége nem sérül, ha a felbontást adó permutációs mátrixok (rácsok) sorrendjét megváltoztatjuk. Így a felbontások számának $n!$-szorosa a lehetséges rácsfelhasználások száma.

A rejtjelzésben a kulcstér mérete is fontos tényező, ezért igen érdekesek a latin négyzetek számára vonatkozó eredmények. Az L(n) nxn-es latin négyzetek permutációs mátrixokra való felbontásainak száma megegyezik az összes *nxn*-es latin négyzetek számával. A latin négyzetek számára pontos formula egyelőre nem létezik, azt azonban tudjuk, hogy ha T_n-nel jelöljük az úgynevezett redukált *nxn*-es latin négyzetek számát (redukált latin négyzet, melynek első sora és oszlopa az 1,2,...,n természetes számokat alapsorrendben tartalmazza), akkor $T_n \geq (n-2)!(n-3)!...(2!)(1!)$, míg az összes *nxn*-es latin négyzetek számára fennáll az $U_n = n!(n-1)!$ T_n összefüggés.

A redukált latin négyzetek számának pontos értékét eddig csupán n=10-ig sikerült számítógéppel meghatározni, hogy mekkora számokról van szó, annak illusztrálására álljon itt T_9= 377.597.570.964.258.816 [1]. Ez a szám kb. 38 milliószorosa a Földön ma élő emberiség létszámának. A rejtjelzésben javasolható rácsméretek az $20 \leq n \leq 30$ értékek!

A következőkben megmutatjuk, hogy a permutációs mátrixok (és bizonyos feltételek mellett a latin négyzetek is) megsorszámozhatók, azaz az *nxn*-es permutációs mátrixok és az 1, 2, ..., n! természetes számok között kölcsönösen egyértelmű megfeleltetés létesíthető. Az 1.,2.,3. tételek bizonyítása megtalálható [4]-ben.

1.Tétel

Bármely P_i *nxn*-es permutációs mátrixhoz kölcsönösen egyértelműen hozzárendelhető egy p_i *n*-edfokú permutáció.

Az 1.tétel illusztrálásához lássuk el a (3)-beli P_1 permutációs mátrixot perem elemekkel. Ekkor a (6) mátrixot kapjuk.

	1	2	3	4
1	1	0	0	0
2	0	0	0	1
3	0	1	0	0
4	0	0	1	0

(6)

A P_1 permutációs mátrixhoz rendeljük a p_1 permutációt a következőképpen:

– A P_1 mátrix első sorában található 1-hez tartozó vízszintes és függőleges perem elemeket írjuk egymás alá, ez lesz a p_1 permutáció első oszlopa.
– Tegyük ugyanezt a P_1 mátrix második, harmadik, negyedik sorával, így kapjuk a p_1 permutáció megfelelő oszlopait, azaz, ha P(i,j)=1, akkor p_1 megfelelő oszlopa $\begin{pmatrix} i \\ j \end{pmatrix}$ (lásd a (7) levezetést).

$$P_1 = \begin{matrix} 1&0&0&0 \\ 0&0&0&1 \\ 0&1&0&0 \\ 0&0&1&0 \end{matrix} \xrightarrow{(6)} p_1 = \begin{pmatrix} 1&2&3&4 \\ 1&4&2&3 \end{pmatrix} \qquad (7)$$

Permutációk és a „faktoriális alapú” számrendszer

Ahhoz, hogy a permutációs mátrixokhoz sorszámot rendeljünk, az 1.tétel alapján elegendő a permutációk megsorszámozása. Erre ad módot a következő 2. és 3. tétel.

2. Tétel („faktoriális alapú” számrendszer)

Legyenek m és b_i természetes számok, melyekre teljesül, hogy

$$1 \leq m \leq n! \qquad (8)$$

$$0 \leq b_i \leq i-1 \qquad (i=1,2,3,...,n) \qquad (9)$$

$$m = 1 + \sum_{i=2}^{n} b_i (i-1)! \qquad (10)$$

Ekkor bármely (8)-nak megfelelő m-hez pontosan egy b_i sorozat létezik, amely eleget tesz a (9), (10) összefüggéseknek.

Amint azt láttuk, az összes n-ed rendű latin négyzet előállítása teljesen megoldatlan probléma, hiszen akkor egyúttal megoldódna a leszámlálásuk is, de $n > 10$ esetén még az összes latin négyzetek pontos számát sem ismerjük. Így a latin négyzetek alkalmazása szempontjából különleges jelentősége van, ha bizonyos típusú latin négyzet osztályok előállítására tudunk algoritmust adni, főleg ha ez egyszerre a természetes számokhoz való egyértelmű hozzárendelést is jelent. Ekkor ugyanis a rejtjelzésben jelentős véletlenszám generátorok felhasználására is mód nyílik, másrészt tárolási és továbbítási előnye van. A következőkben olyan latin négyzet osztályt állítunk elő, amelynek soraiban lévő permutációk elemi transzpozíciókkal származtathatók egymásból. Az algoritmus részletes leírása [4]-ben megtalálható.

Az eljárás elemi transzpozíciók segítségével állítja elő a permutációkat. Legyen a kiindulási permutáció (a π_1 kezdőpermutáció megválasztása tetszőleges lehet):

$$\pi_1 = \begin{pmatrix} 1\,2\,...\,n \\ 1\,2\,...\,n \end{pmatrix} \qquad (11)$$

Ekkor a rekurziós formula a következő:

$$\pi_{m+1} = \sigma_m \cdot \pi_m \qquad 1 \leq m \leq n!-1 \qquad (12)$$

σ_m meghatározásához soroljuk a természetes számokat az $A_1, A_2, ..., A_k$ osztályokba úgy, hogy

$$m \in A_k \quad \Leftrightarrow \quad k! \mid m \quad \text{és} \quad (k+1)! \nmid m \qquad (13)$$

$$\sigma_m = \begin{cases} \tau_1 \cdot \tau_3 \cdot \tau_5 \cdot ... \cdot \tau_k & \text{ha} \quad m \in A_k \text{ és } k = 2r+1 \\ \tau_2 \cdot \tau_4 \cdot \tau_6 \cdot ... \cdot \tau_k & \text{ha} \quad m \in A_k \text{ és } k = 2r \end{cases} \qquad (14)$$

A σ_m transzpozíció szorzatot a továbbiakban σ_m transzformációnak nevezzük.

A τ_i jelölés elemi transzpozíciót jelöl, azaz τ_i=(i i+1), így (14) a következőképpen írható:

$$\sigma_m = \begin{cases} (12)(34)(56)...(k\ k+1) & \text{ha } m \in A_k \text{ és } k = 2r+1 \\ (23)(45)(67)...(k\ k+1) & \text{ha } m \in A_k \text{ és } k = 2r \end{cases} \quad (15)$$

Az eljárás tehát a következő transzformáció-szorzatot állítja elő:

$$\pi_{k+1} = \sigma_k \cdot \sigma_{k-1} \cdot \ldots \cdot \sigma_2 \cdot \sigma_1 \cdot \pi_1 \qquad (k=1, 2, ..., n!-1) \quad (16)$$

Osztályozzuk a transzformációkat az indexük szerint, vagyis σ_r és σ_s akkor és csak akkor tartozik egy osztályba, ha *r* és *s* a (13) definíció szerint egy osztályba tartozik.

Ekkor könnyen belátható, hogy az egy osztályba tartozó transzformációk egyenlők, hiszen *r* és *s* egyértelműen határozzák meg a (15) definíció *k* osztályindexét.

A (13)-(16) osztályozási definíciók és a transzformációk egyenlősége miatt igaz a következő:

$$\begin{aligned} \sigma_1 &= \sigma_{(n-1)!+1} = \sigma_{2(n-1)!+1} = \ldots = \sigma_{(n-1)(n-1)!+1} \\ \sigma_2 &= \sigma_{(n-1)!+2} = \sigma_{2(n-1)!+2} = \ldots = \sigma_{(n-1)(n-1)!+2} \\ &\vdots \\ \sigma_{(n-1)!} &= \sigma_{2(n-1)!} = \sigma_{3(n-1)!} = \ldots = \sigma_{n(n-1)!} \end{aligned} \quad (17)$$

Helyettesítsük be (16)-ba a (17) egyenlőségrendszerben kapottakat:

$$\pi_{n!} = \sigma_{(n-1)!-1} \cdot \ldots \cdot \sigma_1 \cdot \left[\sigma_{(n-1)!} \cdot \ldots \cdot \sigma_1\right]^{n-1} \cdot \pi_1 \quad (18)$$

Mivel a $\sigma_{(n-1)!-1} \cdot \ldots \cdot \sigma_1$ transzformáció szorzat nem más, mint az összes (n-1)-ed fokú permutációk előállításához szükséges transzformációk szorzata, vezessük be a következő egyszerűbb jelölést:

$$\rho_r = \sigma_{r!-1} \cdot \ldots \cdot \sigma_1 \quad (19)$$

Ahol tehát ρ_r az összes r-ed fokú permutáció előállításához szükséges transzformációk szorzatát jelöli. Ekkor (18) így írható:

$$\rho_n = \rho_{n-1} \cdot \left[\sigma_{(n-1)!} \cdot \rho_{n-1}\right]^{n-1} \cdot \pi_1 \quad (20)$$

Latin négyzetek megszámozása

3. Tétel

A (20) formula n! különböző permutációt állít elő.

Következmények:

K3.1.

A 3. tétel következményeként adódik, hogy a (17) egyenlőségrendszer minden sorának első eleme különböző permutációt állít elő. Az egy sorban levő transzformációk a teljes n-edfokú ciklus (C_n) különböző hatványaival szorozzák a sor első (kezdő) permutációját, így ezek is különbözőek és teljes ciklust alkotnak.

Ebből következik, hogy *(17) minden sora n darab olyan permutációt generál, amelyek egy latin négyzetet alkotnak.*

K3.2.

Másrészről (17) minden sora különböző latin négyzetet állít elő, így a fenti rekurzív eljárással (n-1)! latin négyzet könnyen előállítható.

K3.3.

A K3.1. következményből adódik, hogy az így generált latin négyzetek reprezentálhatók a megfelelő sor kezdőpermutációjával. Azaz a kezdőpermutációhoz rendelt sorszámmal azonosíthatók. A fentiekben bevezetett jelölésekkel az alábbi sorszámozott latin négyzeteket kapjuk:

$$L_m(n) = \begin{bmatrix} \pi_m \\ \pi_{(n-1)!+m} \\ \pi_{2(n-1)!+m} \\ \vdots \\ \pi_{(n-1)(n-1)!+m} \end{bmatrix} \qquad 1 \le m \le (n-1)! \quad (21)$$

Példa: n=4, m=3 (lásd az *1. táblázatot*)

$$L_3(4) = \begin{bmatrix} \pi_3 \\ \pi_9 \\ \pi_{15} \\ \pi_{21} \end{bmatrix} = \begin{matrix} 2 & 3 & 1 & 4 \\ 1 & 4 & 3 & 2 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 2 & 3 \end{matrix} \quad (22)$$

Az (1) felbontásnak megfelelően permutációs mátrixok összegeként felírva:

$$LP_m(n) = 1 \bullet P_m + 2 \bullet P_{(n-1)!+m} + 3 \bullet P_{2(n-1)!+m} + \ldots + n \bullet P_{(n-1)(n-1)!+m}$$
$$1 \le m \le (n-1)! \quad (23)$$

Példa: n=4, m=3 (lásd az *1. táblázatot*)

$$\pi_3 = \begin{pmatrix} 1234 \\ 2314 \end{pmatrix} \Rightarrow P_3 = \begin{matrix} 0100 \\ 0010 \\ 1000 \\ 0001 \end{matrix} \qquad \pi_9 = \begin{pmatrix} 1234 \\ 1432 \end{pmatrix} \Rightarrow P_9 = \begin{matrix} 1000 \\ 0001 \\ 0010 \\ 0100 \end{matrix} \quad (24)$$

$$\pi_{15} = \begin{pmatrix} 1234 \\ 3241 \end{pmatrix} \Rightarrow P_{15} = \begin{matrix} 0010 \\ 0100 \\ 0001 \\ 1000 \end{matrix} \qquad \pi_{21} = \begin{pmatrix} 1234 \\ 4123 \end{pmatrix} \Rightarrow P_{21} = \begin{matrix} 0001 \\ 1000 \\ 0100 \\ 0010 \end{matrix}$$

$$LP_3(4) = 1 \bullet P_3 + 2 \bullet P_9 + 3 \bullet P_{15} + 4 \bullet P_{21} = \begin{matrix} 2134 \\ 4312 \\ 1423 \\ 3241 \end{matrix} \quad (25)$$

Latin négyzet alapú rejtjelzés

Használjuk a példa permutációs mátrixait rejtjelző-rácsként. Legyen a nyílt szöveg: „AMI TITOK AZ TITOK!” és legyen a rácsok sorrendje a fenti (3, 9, 15, 21), ekkor a rejtett betűmátrix a következő (26):

$$R_3=\begin{matrix}0A00\\00M0\\I000\\000T\end{matrix}\quad R_9=\begin{matrix}I000\\000T\\00O0\\0K00\end{matrix}\quad R_{15}=\begin{matrix}00A0\\0Z00\\000T\\I000\end{matrix}\quad R_{21}=\begin{matrix}000T\\O000\\0K00\\00!0\end{matrix}\Rightarrow R_3+R_9+R_{15}+R_{21}=\begin{matrix}IAAT\\OZMT\\IKOT\\IK!T\end{matrix}$$

Mint azt megjegyeztük, ugyanezzel a négy ráccsal 4!=24-féleképpen állíthatjuk elő a rejtett betűmátrixot. Példaként bemutatjuk a 15, 3, 21, 9 sorrendhez tartozó betűmátrixot is (27):

$$R_{15}=\begin{matrix}00A0\\0M00\\000I\\T000\end{matrix}\quad R_3=\begin{matrix}0I00\\00T0\\O000\\000K\end{matrix}\quad R_{21}=\begin{matrix}000A\\0T00\\00I0\\0!00\end{matrix}\quad R_9=\begin{matrix}T000\\000O\\00K0\\0!00\end{matrix}\Rightarrow R_{15}+R_3+R_{21}+R_9=\begin{matrix}TIAA\\ZMTO\\OTKI\\T!IK\end{matrix}$$

A fenti rekurziós algoritmus az összes n-edfokú permutációknak egy egymásbaskatulyázott blokkos elrendezését adja *(1.táblázat)*, amelyre teljesülnek az alábbiak:

A1) Minden blokk utolsó oszlopában azonos elemek vannak.

A2) Azonos fokszámú, de különböző blokkok utolsó oszlopai különbözők.

A3) Az A1., A2. tulajdonságokból következik, hogy egy tetszőleges $\pi_m=\begin{pmatrix}1\ 2\ \dots\ i\ \dots\ n\\ a_1a_2\dots a_i\dots a_n\end{pmatrix}$ n-edfokú permutáció minden eleme egyértelműen meghatároz egy blokkot, mégpedig az a_i elem egy (i-1)-edfokú blokkot, amelyhez hozzárendelhetjük a (9) szerinti b_i értéket. Az így nyert b_i (i=1,2,...,n) sorozat (10) szerint egyértelműen rendeli a permutációhoz az m természetes számot.

1. táblázat

1.	1	2	3	4
2.	2	1	3	4
3.	2	3	1	4
4.	3	2	1	4
5.	3	1	2	4
6.	1	3	2	4
7.	3	1	4	2
8.	1	3	4	2
9.	1	4	3	2
10.	4	1	3	2
11.	4	3	1	2
12.	3	4	1	2
13.	4	3	2	1
14.	3	4	2	1
15.	3	2	4	1
16.	2	3	4	1
17.	2	4	3	1
18.	4	2	3	1
19.	2	4	1	3
20.	4	2	1	3
21.	4	1	2	3
22.	1	4	2	3
23.	1	2	4	3
24.	2	1	4	3

Ha a permutációs mátrixokat rejtjelző-rácsként alkalmazzuk, akkor a P_i mátrix, illetve az ehhez tartozó p_i permutáció helyett elegendő az i szám tárolása az azonosításhoz.

Egy n-ed fokú permutáció tárolásához (csak a képelemeket tároljuk!) *c(n)* számú karakterre van szükség, ahol

$$c(n)=\left(\left[\log_{10} n\right]+1\right)n \qquad (28)$$

Az n! szám számjegyeinek száma (jelöljük *j(n)*-nel):

$$j(n)=\left[\log_{10} n!\right] \qquad (29)$$

Ekkor bár fennáll, hogy (30)

$$\frac{j(n)}{c(n)}=\frac{\left[\log_{10} n!\right]}{n\left(\left[\log_{10} n\right]+1\right)}=\frac{\sum_{i=1}^{n}\log_{10} i}{n\left(\left[\log_{10} n\right]+1\right)}$$

amelyre $\lim_{n\to\infty}\frac{j(n)}{c(n)}=1$ (31)

mégis a gyakorlatban ez a megfeleltetés jól használható, mivel az általában használatos $10\le n\le 500$ értékekre a *2. táblázat (jobbra)* értékei adódnak, ami azt mutatja, hogy 25-50% helymegtakarítást érhetünk el.

Latin négyzet alapú digitális aláírás

Az elektronikus pénz átutalás (EFT=Electronic Fund Transfer) és általában az elektronikus posta elterjedése felvetette a hagyományos aláírás helyettesítését digitálisan előállított (kódolt) elektronikus aláírással. A számítógépes terminálok használóinak, vagy az adatbankokhoz való hozzáférés jogosságának ellenőrzésénél hasonló problémákat kell megoldani, mint a hagyományos levél, illetve más papíralapú dokumentumok hitelesítésénél, ahol ezt a célt szolgálta a kézi aláírás. Nyilvánvaló, hogy egy digitális, teljesen elektronizált rendszerben a kézi hitelesítést is helyettesíteni kell, erre való a digitális aláírás, amely azonban olyan kódolási módszereket használ, amelyek nem csupán a dokumentum aláíróját, hanem a dokumentum tartalmát is hitelesítik.

Sok módszer ismeretes a digitális aláírás megvalósítására. Most egy olyan eljárást mutatok be, amely latin négyzeteken alapul és közvetlenül alkalmas párhuzamos működésű számítógépen való implementálásra, ami rendkívüli módon megnöveli a működési sebességet.

Legyen adott egy $U=a_1,a_2,\dots,a_n$ üzenet ahol az üzenet betűi (a_i) egy q elemű ábécéből valók. Az üzenet hitelesítését (digitális aláírását) az üzenettel azonos ábécé-ből vett s darab ($A=b_1,b_2,\dots,b_s$) betűvel kívánjuk elvégezni. Tegyük fel az egyszerűség kedvéért, hogy n osztható s-sel, vagyis $n=s\cdot t$. Válasszuk szét az üzenetet s darab részüzenetre (a szétválasztás egy kulcs szerint fog történni, ami esetünkben egy latin négyzet).

Minden részüzenet t darab betűből fog állni és minden egyes részüzenet az elektronikus aláírás egy betűjét határozza meg.

Az eljárást egy példán fogom szemléltetni, amely a könnyebb áttekinthetőség érdekében kis n és q értékekre vonatkozik. Legyen az üzenet U=1032203101231003 (vagyis n=16, q=4, s=4). A kulcs amely szerint az üzenetet részüzenetekre bontjuk egy s-ed rendű (jelen esetben 4-ed rendű) latin négyzet:

$$\begin{matrix}0\ 2\ 3\ 1\\2\ 1\ 0\ 3\\1\ 3\ 2\ 0\\3\ 0\ 1\ 2\end{matrix} \qquad (32)$$

2. táblázat

n	j(n)	c(n)	$\frac{j(n)}{c(n)}$
10	7	20	.35
100	158	300	.526
200	375	600	.625
300	614	900	.682
400	869	1200	.724
500	1134	1500	.756

A (33) mátrix egy segédtáblázat, amelynek felhasználása a következőkben kerül ismertetésre.

$$\begin{matrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{matrix} \qquad (33)$$

Az *U* üzenet U_1, U_2, U_3, ..., U_s részüzenetekre való bontásának lépései a következők:

Válasszuk ki a (32) latin négyzetben szereplő azonos elemek sorszámát a (33) mátrix szerint úgy, hogy például a 0 elemekhez tartozó sorszámok a (33) mátrix ráhelyezésével a következőknek adódnak: 1, 7, 12, 14. Ugyanezt az eljárást alkalmazva a (32) latin négyzet 1-es, 2-es és 3-as elemeire is, a sorszámokat négy osztályba osztjuk: (1, 7, 12, 14), (4, 6, 9, 15), (2, 5, 11, 16), (3, 7, 9, 13).

Ezután a sorszámokat (megtartva az osztályozást) helyettesítjük az *U* üzenetnek az illető sorszám szerinti helyén álló elemével. Így a következő kevert részüzeneteket kapjuk: U_1= (1, 3, 3, 0), U_2= (2, 0, 0, 0), U_3= (0, 2, 2, 3), U_4= (3, 1, 1, 1). Most lássuk el a (32) latin négyzetet perem elemekkel:

	0	**1**	**2**	**3**
0	0	2	3	1
1	2	1	0	3
2	1	3	2	0
3	3	0	1	2

(34)

Így tulajdonképpen a (0,1,2,3) halmazon definiáltunk egy * műveletet, amelynek művelettáblája a (34) latin négyzet. A (34) művelettáblát pontosan úgy használjuk, mint a jól ismert szorzótáblát, például azt kapjuk, hogy 0*1=2, 1*2=0, stb.

A nem matematikus olvasó számára talán szokatlan, hogy a * művelet nem asszociatív, vagyis $a*(b*c) \neq (a*b)*c$, azaz például $2*(3*1)=2*0=1$, de $(2*3)*1=0*1=2$, vagyis $2*(3*1) \neq (2*3)*1$. Ennek a tulajdonságnak nagy jelentősége van a következőkben bemutatott kódolási eljárásnál.

A példánkban szereplő *U* üzenet digitális aláírásához az egyes U_1, U_2, U_3, U_4 részüzenetek szorzatát kell előállítani a (34) művelettábla alapján:

$$\begin{aligned} b_1 &= ((1*3)*3)*0 = (3*3)*0=2*0= 1 \\ b_2 &= ((2*0)*0)*0 = (1*0)*0=2*0= 1 \\ b_3 &= ((0*2)*2)*3 = (3*2)*3=1*3= 3 \\ b_4 &= ((3*1)*2)*1 = (0*1)*1=2*1= 3 \end{aligned} \qquad (35)$$

vagyis az *U* üzenethez tartozó hitelesítő aláírás:

$$A=(b_1b_2b_3b_4)=1133$$

A fenti eljárás teljesen egyértelmű eredményre vezet, hiszen az *U* üzenet felbontása részüzenetekre a latin négyzet elemeinek diszjunkt osztályozásán alapul, ez viszont a fentiekben ismertetett permutációs mátrixokra való felbontási tétel miatt kölcsönösen egyértelmű.

A latin négyzeteken alapuló művelettáblák nem asszociatív algebrai struktúrát (úgynevezett kvázicsoportot) reprezentálnak, aminek nagy jelentősége van az illetéktelen hamisítás elleni védekezésnél, mivel két karakter egyszerű felcserélését is kimutatja. Ezzel a képességgel a paritás ellenőrzésen alapuló módszerek, vagy a numerikus eljárások nem rendelkeznek.

Záró megjegyzés

Végül szeretném felhívni az olvasó figyelmét arra, hogy a rejtjelzés, hitelesítés, illetve a digitális aláírás numerikus módszereinek biztonsága (feltörhetősége) alapvetően függ a pillanatnyi számítástechnikai eszközök kapacitásától. Azaz a feltörhetetlenség mellett szóló érvek, a több ezer éves számolási igény a rejtett kulcsok megfejtéséhez, a gyors hardver fejlődéssel bizonytalanná válnak.

Bízom benne, hogy a latin négyzetek titkosítási alkalmazásainak e vázlatos ismertetéséből egyértelműen kitűnik, hogy a latin négyzeteken alapuló strukturális módszerrel aláírt és rejtjelzett elektronikus dokumentumok esetén nem kell tartani a számítógépek sebesség és kapacitás növekedésétől.

Irodalom

[1] J. Dénes, A.D. Keedwell:
Latin squares and their applications,
Akadémiai Kiadó, Budapest, 1974.

[2] J. Dénes, A.D. Keedwell: Latin squares and 1-factorizations of complete graphs, I.
Ars Combinatorica, 25A (1988), pp.109–126.

[3] J. Dénes, A.D. Keedwell: Latin squares and 1-factorizations of complete graphs, II.
Utilitas Math., 34 (1988), pp.73–83.

[4] Dénes Tamás: Algoritmusok az összes n-edfokú permutáció előállítására, I.-II.
Információ Elektronika, 1975/1.-2.

[5] Dénes Tamás: A rejtjelző rácsok születése
Híradástechnika, 2001/10, pp.57–63.

[6] Dénes Tamás:
SZTEGONOGRÁFIA – rejtett információk rejtjelzés nélkül
Híradástechnika, 2001/8, pp.15–21.

Beszámoló a IV. magyar WDM Workshopról

lajtha.gyorgy@ln.matav.hu

Paksy Géza negyedik alkalommal rendezte meg a fotonikával és fénytávközléssel kapcsolatos tudományos ülésszakot. Ez alkalommal különösen színvonalas előadások és kiemelkedő szakemberek tették érdekessé a reggel 8.30-tól 17.30-ig tartó összejövetelt. A színvonalra és az újdonságokra jellemző, hogy még késő délután is nagyon sokan hallgatták az előadásokat. Paksy Géza és egyik szervezőtársának, Jakab Tivadarnak a munkáját dicséri, hogy kilenc kiemelkedő, nemzetközileg elismert szakember mutatta be elméleti, vagy gyakorlati eredményeit.

A Workshopról kiadvány és a fóliákat tartalmazó CD jelent meg, tehát ezek részletes ismertetése felesleges és nem is lenne az újság feladata. Szeretnénk azonban néhány különlegesen értékes előadásra felhívni a figyelmet. Ezek napi munkánkban és a következő évek lehetőségeinek felmérésében segíthetik az olvasókat. A beszámolóban a szubjektíven legjobbnak ítélt néhány előadást mutatjuk be egy-egy bekezdés erejéig, annak érdekében, hogy az új gondolatokra irányítsuk olvasóink figyelmét.

Talán a legtöbb tudományos újdonsággal *Prof. Steve Ferguson* Optical network developments: a reality check című előadása szolgált. Mondani valóját a ROADM technológiával, vagyis a távolról irányítható optikai leágazó, becsatoló multiplexerekkel (remotely reconfigurable optical add-drop multiplexers) kezdte. Ezek megvalósításához azonban számos új eszköz alkalmazására lesz szükség, melyeket egymás után szemléltetett. Az első a fotonikai integrált áramkörök kidolgozása volt, melyek története több mint tíz évre nyúlik vissza és ma már a lézerrel egy tokba integrálják a különböző feladatok megvalósításához szükséges további elemeket. Ezekből leágazó átkapcsolók építhetők ki.

Előadása további részében azokra az eszközökre hívta fel a figyelmet, melyek már a mikro méret alá csökkentek, vagyis a nanotechnika témakörébe tartoznak. A photonic band gap devices (PBG) az anyag tervszerűen létrehozott inhomogenitásait használják fel a fénysugarak irányítására és csatolására. Ezekkel az eszközökkel kvázi periodikus rácsokat készítenek, melyek akár számítástechnikai célokra is felhasználhatók lesznek. Ide kapcsolódik a holey fibres, vagyis az üreges fényvezető, mellyel további sávszélesség növelés és jelkezelés valósítható meg. Előadása alapján érdemes átnézni mindazon cikkeket, melyeket a Marconi Fejlesztési Intézet az utóbbi évben tett közzé, mert meghatározó lesz a következő évek műszaki fejlesztésében.

Dr. Per O. Andersson (Ericsson) egy általános fejlődési világképről számolt be, ahol az 1999-től 2004-ig terjedő időszakra vonatkozóan bemutatta a fejlődés mértékét, melyből látszott, hogy a fénytechnikában öt év alatt minden hálózati síkban megtízszereződött az átviteli kapacitás. Ennek alapján általánosította a Moore's törvényt és megbecsülte, hogy mi várható 2009-re. Eszerint a gerinchálózatban 1 Terrabit/sec, a városi hálózatban 15 Mbit/sec és a felhasználói csatlakozásoknál 6 Mbit/sec lesz az átlagos sebesség. Ez minden területen újabb feladatokat és lehetőségeket jelent. Hatása lesz a távol eső falvak és területek kulturális és gazdasági fejlődésének gerjesztésében, a forgalomirányításban és várhatóan a szórakozásban is. Különös érdekesség, hogy a sávszélesség növekedése és a holográfia alkalmazása együttesen realitássá teszi a térhatású képek megjelenítését. Ezt különösen kiemelte a szerző.

Óvatosságra intett, de elképzelhetőnek tartja, hogy a következő 5 éves periódusban még egy tízszeres szorzóval növekszik az átviteli kapacitás, amelynek hatását az üzletre, a kultúrára és az egész társadalomra alig lehet megjósolni. Ezt kombinálva a mobilitással, egy gyökeresen átalakuló társadalom képét vetíti előre. Arról nem szólt, hogy vajon a sokkal lassabban fejlődő emberi elme, hogy fogja ezt befogadni.

Sjaak Antheunise (Lucent Technologies, Optical Business Development Branch) a városi hálózatok fejlődéséről beszélt. Előadásának felépítése eltért a korábbiaktól. Gazdasági szempontokkal indított, vizsgálva, hogy hogyan lehet növelni a profitot és ennek előfeltételeit, tárgyalta a bevétel növelését, ehhez a felhasználók számának gyarapítását és a költségek csökkentését. Ez utóbbi akkor valósítható meg, ha a hálózatot mindig az igényekhez tudjuk illeszteni és ehhez rendelkezésre állnak a megfelelő eszközök.

Első helyen említette ezek közül a ROADM-et, a hangolható lézereket és a megfelelő vezérlősíkot. Ezeknek az ITU G709 csomagképzése és a GMPLS címkézés az előfeltétele. Így áttért a műszaki kérdésekre, melyeknek célja a gazdaságosság. A ROADM megvalósításához megfelelő hullámhosszszűrők, hullámhosszkapcsolók és MEMS-es vezérelhető kapcsolók kellenek. Ezek segítségével kialakított egy rugalmas hálózatot, mely a gyorsan változó igényekhez alkalmazkodni tud és előfeltétele a gazdaságos nagyvárosi

hálózat kiépítésének. Az eredmény, amire zárszavában visszatért, kis mértékű emelkedés a capexben és nagymértékű, hosszú távú csökkenés az opexben.

Ugyancsak a rugalmasságot hangsúlyozta *Kalmár András* az Alcatel Ausztria fejlesztőmérnöke. Az ismert elemekből különböző módon kiépített kapcsolási és hálózati struktúrákkal az igényekhez illeszkedő, gyorsan átkonfigurálható hálózatot épített ki. Ugyancsak igen színvonalas gyakorlati hálózatépítési tapasztalatokat tett közzé *dr. Ralf-Peter Braun* a T-Systems németországi fejlesztő részlegének vezető mérnöke. Munkája során az MPRS alapú hálózat kiépítését hangsúlyozta és bemutatta, hogy az ITU ebben a periódusban milyen kérdésekre keresi a választ. Ezek döntőmértékben az Ethernet alkalmazására alapulnak. Ez a T-Systems-nek is célja és várhatóan minden hálózati síkban alkalmazni fogják.

A nemzetközi együttműködésben elért tapasztalatokról, a célokról és eredményekről három érdekes előadást hallhattunk, melyek jól vázolták a fényvezetős hálózatok fejlődési kérdéseit. Időrendi sorrendben az előadók a következők voltak: *Berceli Tibor dr., Antonella Bogoni, Hagen Woesner* és *dr. Jan Späth,* akinek az előadását a korábban már említett Steven Ferguson olvasta fel. Az említett kutatók munkája a nemzetközi projekteket jelentősen előmozdította.

Cinkler Tibor oktató jellegű, jól felépített, érthető előadásban mutatta be a különböző hálózatok összekapcsolási és kiépítési lehetőségeit. Előadása kitért a tartalékolásra, a hibavédelemre és a különböző átviteli protokollok értelmezésére. Újszerű és érdekes volt a Multi-Domain és a Multi-Layer hálózatok vizsgálata, amely problémákat érthetően illesztette az általános hálózat tervezési koncepciójához.

Meg kell még emlékeznünk *Joe Fragoso* FlexLight Networks USA előadásáról, aki a sávszélesség növekedését és az ehhez kapcsolódó prognózisokat, hálózatkiépítési struktúrákat mutatta be. Az általa felhasznált Moore's elv összhangban volt dr. Per O. Andersson jövőképével. A különböző távolságok áthidalása és a védelmi elvek bemutatása minden hallgató számára tanulságos lehetett.

A szervezők gondosságát dicséri, hogy egy szekciót szántak a doktoranduszok eredményeinek bemutatására. *Szegedi Péter, Szigeti János, Lakatos Zsolt* és *Pándi Zsolt* 15-20 percben ismertette, hogy eddig milyen eredményeket ért el a hálózattervezés, a fényvezetők alkalmazása, a biztonság növelése és a jelzéstechnika területén. A hallgatóság egyértelműen úgy látta, hogy ezekből a fiatalokból néhány év múlva olyan kiváló szakemberek lesznek, akik a különböző nemzetközi összejöveteleken előadásaikkal méltóan fogják képviselni a hazai mérnökképzést és kutatást.

Reméljük, hogy két év múlva hasonló lelkes beszámolóval értékelhetjük a szervezők, az előadók és a fiatalok munkáját.

Hírek

A **Matáv** és a **Cisco Systems** képviselői ünnepélyesen átadták azt az országos gerinchálózatot, amely nagysebességű internet-hozzáférést biztosít a Nemzeti Információs Infrastruktúra Fejlesztési Iroda (NIIFI) budapesti központja, hét regionális központként működő egyetem, valamint számos további kutatási és oktatási intézmény számára. Az új hálózat biztosítja a GEANT2 (az Európai Unió által támogatott pán-európai kutatóhálózat) számítógéphálózatához való egyenszilárdságú hozzáférést az NIIFI tagintézményi kör közel 700 hazai intézményének, csaknem 600 000 felhasználója számára.

A Matáv DWDM hálózata több szempontból is fontos szerepet tölt be az akadémiai hálózatokban: biztosítja a nagysebességű összeköttetéseket az NIIFI nagykapacitású IP gerinchálózatának csomópontjai között; ugyanakkor ez a hálózat teszi lehetővé, hogy Magyarország és a kelet-európai régió országai az egész Európára kiterjedő nagysebességű akadémiai hálózathoz (GEANT) kapcsolódjanak.

A 10 Gbs sebességre való bővítés megerősíti az ország helyzetét és szerepét a kontinens kutatási-oktatási hálózati együttműködésében. A kialakított DWDM hálózat lehetővé teszi a Matáv számára azt is, hogy a jövőben egyszerre több országos gerinchálózat működjön ugyanazon az optikai infrastruktúrán.

A **VPOP** központjában és regionális kirendeltségein 2004. decemberétől összesen 143 helyszínen, a magas szintű hálózatbiztonságot nyújtó **Cisco** VPN útválasztók biztosítják az adatkapcsolatot. A telephelyek az Elektronikus Kormányzati Gerinchálózaton (EKG) keresztül kapcsolódnak a VPOP országos rendszeréhez.

A VPOP hálózata a biztonság kérdését elsődleges szempontként kezeli, a tervezésnél messzemenően szem előtt tartotta a későbbi hálózat-fejlesztési lehetőségek biztosítását, mint például az IP telefónia egyszerű és gyors bevezetését.

Immár tizenöt éves a Magyar Mérnökakadémia

SIPOS LÁSZLÓ

A mérnöki munkával és kutatással kapcsolatos két, egymástól 40 év távlatában elhangzott véleményt szeretnénk idézni: Guillet professzor szerint a jó mérnök csaz az lehet, akinek lelki és szellemi képességei a következő arány szerint oszlanak meg: „50% erkölcsi erő, 25% általános műveltség, 25% szaktudás." (Technika folyóirat, 1931.) Szentgyörgyi Albert Nobel-díjas tudósunk hazalátogatása alkalmával egy televíziós előadásában szintén hasonló nézeteket vallott: ő is fontosabbnak tartotta a szorgalmat és a szerencsét, mint a kiemelkedő szaktudást. Természetesen a tudás sem elhanyagolható, hiszen valamennyi jelentős tudományos és műszaki eredmény azért egy-egy tudós nevéhez kötődik...

A rendszerváltást követően a magyar műszaki élet vezető személyiségei közül néhányan – ismerve az ipar technológiai színvonalának a gazdaság aktuális állapotára gyakorolt hatását – elhatározták, hogy élve az 1989. évi II. törvény, az egyesülésről adta lehetőséggel, a külföldi példák nyomán, idehaza is megalapítják a mérnöktársadalom és a műszaki tudóstársadalom elitjéből szerveződő mérnökakadémiát a gazdaság mielőbbi fellendítésének elősegítése érdekében.

Tekhné-érem, Lapis András szobrászművész alkotása

A szervezési, előkészítési munkákban nagy segítséget jelentett a külföldön már régóta működő, nemzeti mérnökakadémiák tapasztalatait a születő Magyar Mérnökakadémia (MMA) rendelkezésére bocsátó Mérnökakadémiák Világszövetsége, a Council of Academies of Engineering and Technological Sciences (CAETS) és annak főtitkára, Steven N. Anastasion.

Így a közép-kelet európai térségben elsőként, 1990. január 29-én a MTESZ Kossuth Lajos téri székházában negyvenkét fővel megalakult a Magyar Mérnökakadémia. Az alakuló mérnökakadémia első reprezentánsaként olyan mérnököt kellett találni, aki kreativitása révén nemzetközileg is ismert és elismert személyiség, aki a megalakuló nemzeti mérnökakadémiát és Magyarországot a nemzetközi szintéren is méltóképen jegyzi és képviseli. Ezen követelményeknek Dr. Rubik Ernő személye felelt meg, akinek neve a világban Magyarország szinonimájaként szerepelt. Dr. Rubik Ernő, felismerve az ügy fontosságát és jelentőségét, elvállalta a formálódó Magyar Mérnökakadémia elnöki tisztét. A megalakulást Dr. Ginsztler János tanszékvezető egyetemi tanár vezetésével dolgozó Bizottság készítette elő.

A Bizottság a megalakítási cél szem előtt tartásával a magyar műszaki élet, lehetőség szerinti teljes spektrumát képviselő, szakmai elithez tartozó reprezentánsokat jelölt a mérnökakadémia tagságra. A megkeresett személyek között akadémikusok, egyetemi tanárok, az ipar és a tudományos élet meghatározó személyiségei szerepeltek, akik egyetértve a megalakuló mérnökakadémia céljaival, vállalták az aktív közreműködést. (A híradástechnika és informatika területéről néhány ismert személyiség: Dr. Dibuz Sarolta, Dr. Gordos Géza, Fodor István, Havass Miklós, Dr. Keviczky László, Dr. Kóczy T. László, Dr. Tófalvi Gyula.)

Megalakulásának tizenötödik évfordulójára február 4-én ünnepi ülésszakot szerveztek a Magyar Szabadalmi Hivatalban. Szentgyörgyi Zsuzsa, az öttagú szervező bizottság vezetője vállalta a levezető elnöki feladatot is. Megnyitó szavai után Dr. Keviczky László: Mérnök és Akadémia című előadása következett. A 90-es évek eleje turbulens időszak volt, az 1825-ben alakult MTA-t is többen szorongatták, létét is megkérdőjelezve. Így érthető, hogy az MTA-n belül jó néhányan féltek attól, hogy az MMA konkurens szervezet lesz. Az előadó külön kiemelte Dr. Vajda György akadémikus nevét, aki sokat segített az ellenséges nézetek feloldásában. Keviczky úr, az MTA alelnöke, az MMA tagja igazi mérnökként a definíciók kibontásával folytatta mondandóját. Megismerhettük a brit, az amerikai, majd a magyar mérnökakadémia stratégiai célját. A brit mérnökakadémia célja, hogy az ország legjobb mérnökeit hozza össze valamennyi területről. Stratégiai prioritásai közé tartozik, hogy növelje az angol mérnökök tudását, elismerje a kiválóságokat, és inspirálja a jövő nemzedékét. Az amerikai mérnökakadémia célja a mérnöki technológia vezető szerepének biztosítása a nemzet érdekében.

A Magyar Mérnökakadémia céljai:

– Szervezeti keretek nyújtása a műszaki tudományok képviselőinek a szakmai véleménynyilvánítás, állásfoglalások, javaslatok adása érdekében.
– Szervezett együttműködés a világ mérnökakadémiáival a legújabb műszaki – tudományos – technológiai ismeretek megszerzése érdekében.
– Kölcsönös előnyökön alapuló együttműködés a Magyar Tudományos Akadémiával, a MTESZ-szel és más hazai tudományos és mérnöki szervezetekkel, valamint a felsőoktatási és kutatási intézményekkel.

– Felhasználva a tagság által képviselt szakterületek multidiszciplinaritását, a tagok jelentős hazai- és nemzetközi elismertségét és az ebből származó tapasztalatokat, az ország és a nemzet szolgálata minden olyan szakterületen, amely összefügg a technika és a technológiák fejlődésével.
– A mérnöki szakterületen működő, kiemelkedő alkotókészségű személyek, munkacsoportok munkájának segítése; a fiatal szakemberek, a kiváló, tehetséges doktoranduszok, egyetemi hallgatók nemzetközi életbe való bekapcsolódásának elősegítése és támogatása az Akadémia alapítványán keresztül.

Dr. Ginsztler János Elnök úr „A 15 év néhány emlékezetes pillanata" címmel megtartott diavetítéses előadása igazi sikert aratott, immár az interneten is (www.mernokakademia.hu) tanulmányozható.

Dr. Bendzsel Miklós, a Magyar Szabadalmi Hivatal Elnöke „Mérnök és Társadalom" c. előadását is nagy érdeklődés kísérte. A MMA tag házigazdánk felvázolta mind azt a nagyon gazdag karaktert, amit a mérnöki hivatásunk takar. Kritikus éllel megjegyezte: *„A mérnöki erények egy jelentős része hiányzik a társadalom vezető személyiségeinek és testületeinek szemléletéből. A mérnökakadémia egyik hivatása lehet a jövőben, hogy segít meghonosítani ezeket a következő években."*

Dr. Ratkó István, az MMA egyik alapító tagja testvére Ratkó József gyönyörű és tartalmas verseit elszavalva lenyűgözte a hallgatóságot. Döbbenetesen meghatómlékpercek voltak.

A szünet előtt Dr. Boda Miklós, a Nemzeti Kutatási és Technológiai Hivatal elnöke ismertette az új nemzeti innovációs rendszer elemeit, majd Dr. Ginsztler János MMA elnökkel aláírtak egy Együttműködési Megállapodást, ami tanulmányozható a jelzett internetes honlapon.

Szünet után Dr. Somlyódy László akadémikus, a Víz Világszövetség Elnöke „A víz az úr?" című előadásával sikerült elgondolkoztatnia a hallgatóságot.

Havass Miklós, a MMA tagja saját bevallása szerint „agitátor" az éppen most készülő – 2007-2013 közötti időszakot meghatározó – Európa Tervre irányította a figyelmet, természetesen mindannyiunk érdekében: *„Most helyzet van! Hallatni kell a hangunkat!"*

Dr. Barátossy Jenő, az MMA alapító tagja előadásában megosztotta gondolatait a mérnöki etikai kódex fontosságáról. A Nemzeti Mérnökszervezetek Európai Szövetsége (Fédération Européenne d'Associations Nationales d'Ingénieurs – FEANI) Etikai kódexét ajánlotta a tagság számára.

Legvégül Králik István, a MMA tagja tájékoztatta a hallgatóságot a tehetségtámogatás terén eddig elért eredményekről. A részletes összefoglaló, a pályázati lehetőségek valamint a jelzett FEANI Etikai kódex a Magyar Mérnökakadémia internetes honlapján elérhetők: www.mernokakademia.hu

Hírek

A **[freemail]**, Magyarország első, 1997 óta működő, ingyenesen használható, magyar nyelvű publikus levelező-szolgáltatása mára közel kétmillió postafiók üzemeltetésével a hazai internethasználók közel felét, mintegy egymillió internetezőt szolgál ki.

Egy átlagos hétköznapon az összes [freemail]-postafiókra beérkező levelek száma meghaladja a két és fél milliót, „kifelé" pedig egymilliónál több levelet küldenek, amely körülbelül megegyezik a hagyományos postai forgalomban megforduló napi 2,2 millió levéllel. A [freemail] már a magyarországi internetes kultúra hőskorának tekinthető első években nagy népszerűséget vívott ki, használói az indulást követő három év múlva már 150 ezren voltak, a félmilliós határ átlépésére pedig 2000. decemberében került sor. Ezt a számot megduplázva az egymilliomodik postafiókot 2002. júniusában regisztrálták, az elmúlt napokban pedig megtörtént a kétmilliomodik postafiók létrehozása. A számok értékelésekor figyelembe kell venni, hogy a [freemail] rendszere automatikusan megszünteti azokat a fiókokat, amelyeket 90 napon át nem használnak.

Az elektronikus levelezés ma is az internethasználat egyik legnépszerűbb „közmű"-funkciója. A World Internet Projekt kutatás 2004-es adatai szerint a hazai internetezök 73%-a küld és fogad rendszeresen elektronikus levelet.

Az **Ericsson** társadalmi felelősségvállaló programját, az Ericsson Response kezdeményezést elismerésben részesítette a GSM Szövetség, és „A mobiltechnológia legjobb hasznosítása veszélyhelyzetben" díjjal tüntette ki. Az Ericsson a kitüntetést az iráni Bámban 2003. decemberében történt súlyos földrengés során végzett katasztrófaenyhítő tevékenységének elismeréseként kapta. A vészhálózat gyors (az érkezést követő 24 órán belüli) telepítése és az ötezer felhasználó kommunikációjának támogatása jelentősen hozzájárult a humanitárius segélyszervezetek hatékony munkájához.

Hírek

Az **Oracle és a PeopleSoft** 2005. januárjában lezárult összeolvadása hatására egy 50 ezer fős vállalat jött létre, amely a világ számos országában 23 ezer felhasználó szervezet számára nyújt informatikai termékeket és szolgáltatásokat. Az egyesülés után az Oracle nyilvánosságra hozta a „Project Fusion" tervezetet, amely információközpontú rendszerarchitektúra és alkalmazásegyüttes kifejlesztésére egyesíti az Oracle, a PeopleSoft és a JD Edwards termékek funkcióit és folyamatait. Az összeolvadás Magyarországon 46 JD Edwards és néhány nemzetközi PeopleSoft felhasználót érint, amelyek ezentúl a helyi Oracle leányvállalaton keresztül közvetlen kapcsolatban lesznek a gyártóval.

A magyarországi felhasználók számára az Oracle februárban egynapos konferencián ismertette a felvásárlás hatásait. Füzes Péter, az Oracle Hungary ügyvezetője előadásában hangsúlyozta: a helyi PeopleSoft és a JD Edwards felhasználók mostantól egy olyan nemzetközi céget tudhatnak maguk és rendszereik mögött, amelynek nem csupán partnereken, hanem leányvállalatán keresztül is biztosítja számukra a támogatást. A JD Edwards termékek világszerte a gyártó, a logisztikai vagy a projekt rendszerű tevékenységet végző közép és nagyvállalatok körében terjedtel el elsősorban. A magyarországi JD Edwards felhasználók között találhatók például az Alterra Építőipari Kft., a Gyermely Holding Rt., a Középületépítő Rt., a MAL Magyar Alumínium Termelő és Kereskedelmi Rt. és a Tokaj Kereskedőház Rt.

Az új **Axelero Internet Webvarázsló** segítségével minden felhasználó elkészítheti saját weboldalát. Az Axelero előfizetők számára ingyenes szolgáltatás, melyhez elegendő a szövegszerkesztő programok ismerete. A saját honlap fogalma mára olyanná vált, mint a névjegykártya, vagy a mobiltelefon. Cégek, vállalkozások számára szinte elengedhetetlen az üzleti életben való érvényesüléshez, a magánszemélyek számára pedig olyan közkedvelt közösségi szokásoknak ad teret mint a bloggolás, a személyes képgalériák megosztása, vagy akár a fórumírás.

A honlapcenteren (www.honlapcenter.hu) és az Axelero Klubon (klub.axelero.hu) keresztül elérhető szolgáltatás minden csoportnak külön sablontípusokat kínál, amellyel mindenki saját ízlésvilágot alakíthat ki. Az Axelero Weblapvarázsló olyan webes alkalmazás, amelynek használata nem igényel a felhasználó számítógépén programtelepítést és adminisztrációt, csupán állandó internetkapcsolatot és MS Internet Explorer 5.5 vagy ennél magasabb verziószámú böngésző használatát. Így a szerkesztőfelület bárhol és bármikor elérhető. Az egyszerű és átlátható működést a WYSIWYG (What you see is what you get = Amit látsz, azt kapod) rendszer biztosítja. A Weblapvarázslót az Axelero előfizetéssel nem rendelkező ügyfelei a Honlap csomagok keretén belül használhatják, amelyet mindenki 15 napig díjmentesen kipróbálhat.

A hazai honlap piac fokozatosan növekszik. Magyarországon 2003-ban a vállalatok 22%-a rendelkezett weboldallal, amely 9%-os növekedés mellett 2004-ben már elérte a 31%-ot, és 2005-ben megközelítheti a 40%-ot. A 2004-es adatok mögé nézve azonban az látszik, hogy a mikro (27%) és kisvállalatok (50%) jelentős lemaradásban vannak a közepes (64%) és nagyvállalatokkal szemben.

Az Oracle-nak mint **e-learning** megoldásszállító cégnek mind Magyarországon, mind a világ más részein vannak tapasztalatai az elektronikus oktatás területén. Éppen ezért egy konferencia keretében globális áttekintést adotta gazdasági élet változását kísérő emberi erőforrás menedzsmentet érintő igényekről és az elektronikus oktatás bevezetéséhez kapcsolódó gyakorlati kérdésekről. Az elektronikus oktatás területén várható trendek: az előrejelzések szerint 2005-ben megduplázódik az e-learninget használó vállalatok száma, a vállalati képzések több mint 20%-a már az online módon lesz elérhető. Az elektronikus oktatási tartalmak kiegészítése dokumentumkezelő rendszerekkel pedig a vállalat tudásmenedzsmentjének alapjává válik.

E-learning rendszeréhez és a T-Mobile Magyarország több mint 3000 tanuló oktatási adminisztrációjához az Oracle iLearning virtuális oktatóterme, a cég trénercsapata által fejlesztett elektronikus tananyagok, valamint átfogó kérdőívkitöltő rendszer kapcsolódik. A rendszer bevezetési lépéseinek és a mindennapi működtetés rendszerének ismertetése rendkívül tanulságos volt.

DIGITAL BROADCASTING

Approved design principles of RRC04 in practice
Key words: broadcasting spectrum, equal access, interference immunization, international co-operation

Design principles and methodology approved at RRC04 conference form the results of a long preparatory work and international agreements. The practical use of these principles requires further clarification. One of the basic preconditions of success is to realize that administrations should formulate requirements according to their national interests but these requirements must be discussed with neighboring countries in advance.

The state of digital broadcasting – browsing news

RF stages of digital television transmitting equipment
Key words: DVB-T transmitter, digital pre-distortion, transistor power amplifier, linear and non-linear distortions,

Commercial terrestrial digital broadcasting is operating in nine European countries and it will be launched in five further countries later this year. Experiments concerning parameters, measuring methods and equipment construction are being accumulated. In addition to the coder the transmitter consists of an RF demodulator, a power amplifier and filtering units. It is important that these components slightly distort transmitted signals and be conform to spectral requirements. This article deals with their influenced parameters, construction and the correction of distortions.

"Hard work and diligence form the basis of all success" – interview with Béla Ladányi-Turóczy, CEO of Grante Co. Ltd.

E-ADMINISTRATION

Challenges and opportunities of m-government
Key words: data protection, mobile transactions, electronic signature, authentication

The use of information technology is an outstanding task of modernization of public administration. Its benefits are clear, however the innovative developments must not compromise two basic factors: data security and data protection. This paper reviews opportunities offered by the introduction of mobile public administration and also highlights the associated technical and legal challenges. The authors close their article with some open questions, such as the development of suitable security policies and certificates.

E-governance: opportunity, constraint and reality
Key words: joined-up governance, process engineering, future vision

The deployment of e-governance has been facilitated by the development of technical and technological infrastructure as well as by achievements of information and communication technologies. The infiltration of info-communications technology into economy and society was more rapid than that of any other technologies. The "electronization" of the public sector presents a huge potential market for the info-communications sector.

CHANGES AND SECURITY OF NETWORKS

Cause and consequence of changes in wireline networks
Key words: development of fixed stations, issues and trends of co-operation, future vision of networks

There are already considerable changes in traditional wireline telecommunications underway but the revolution of networks and services is still some way ahead. This article gives an overview of the present state of fixed networks and highlights some future trends as well.

Proved security of ad hoc routing protocols
Key words: source based ad hoc routing, ad hoc network, proved security, simulation paradigm

This article presents a formal method developed for the security analysis of on-demand, source routing protocols proposed for ad hoc networks. The method is based on the simulation paradigm which is a well known, general scheme for the verification of security of cryptographic protocols. The notion of secure routing is defined then a practical use of the method is demonstrated.

Latin Squares in cryptography
Key words: early methods, features of Latin Squares, decoding

Decoding grid has become a notable "fashion" in cryptography for several centuries. The author has already dealt with the history and application of the Cardano's grid in encryption in our periodical, this time its relationship with permutation matrices and Latin Squares is introduced. This relationship highlights the extraordinary opportunities of this 450-year old invention in the 21st century. Digital technology opens new perspective for stegonography and for encryption grids as well.

Summaries • of the papers published in this issue

Tartalom

Címlap: A robotok látnak, mozognak, sőt figyelik is egymást.