híradástechnika

VOLUME LVII.

2002/1

Január

Elmélet

Hálózatok működtetése

Távközlés-politika

Beszámolók

a Hírközlési és Informatikai Tudományos Egyesület folyóirata

Tartalom

Nagy múltja van a telefoniának. Kovács O.: Beszédminősítés

Visszatekintés és köszöntő

Sok szeretettel üdvözöljük hűséges olvasóinkat az új év és a folyóirat új évfolyamának indulásakor.

Az elmúlt év emlékezetes eseményekkel búcsúzik. A történelemben és a világpolitikában történteket nem e szakmai folyóiratnak kell felidéznie. A hazai eseményekből is csupán a szakmaiak tartoznak ránk. Itt sem szűkölködünk. 2001-ben született meg az egységes hírközlési törvény, az elektronikus aláírásról szóló törvény és a Nemzeti Információs Társadalom Stratégia. Az EHT átalakította a hírközlés szervezeti struktúráját és megnyitotta az utat a nyílt piaci versenyhez. Ennek jelentőségét aligha lehet túlbecsülni. A törvénnyel és várható következményeivel részletesen foglalkoztunk folyóiratunk hasábjain is.

A törvénnyel összefüggő esemény, hogy karácsony előtt néhány nappal lejárt a Matáv távközlési monopóliuma. A törvény biztosítja a sokszereplős távközlési piac feltételeit, de nem tudja kijelölni, vagy éppen biztosítani a piac szereplőinek megjelenését. Az események alakulása azonban megfelelt az előzetes várakozásoknak. Máris jelentkeztek az új feladatokat vállalni kívánó telefontársaságok, és számuk növekedése igen valószínű. Érdeklődve várjuk, hogy a piac alakulása követni fogja-e az előrejelzéseket. A hazai internetes kultúra további növekedési pályája ugyanis jelentősen függ majd attól, milyen tarifapolitikát tudnak és akarnak folytatni a távközlési társaságok.

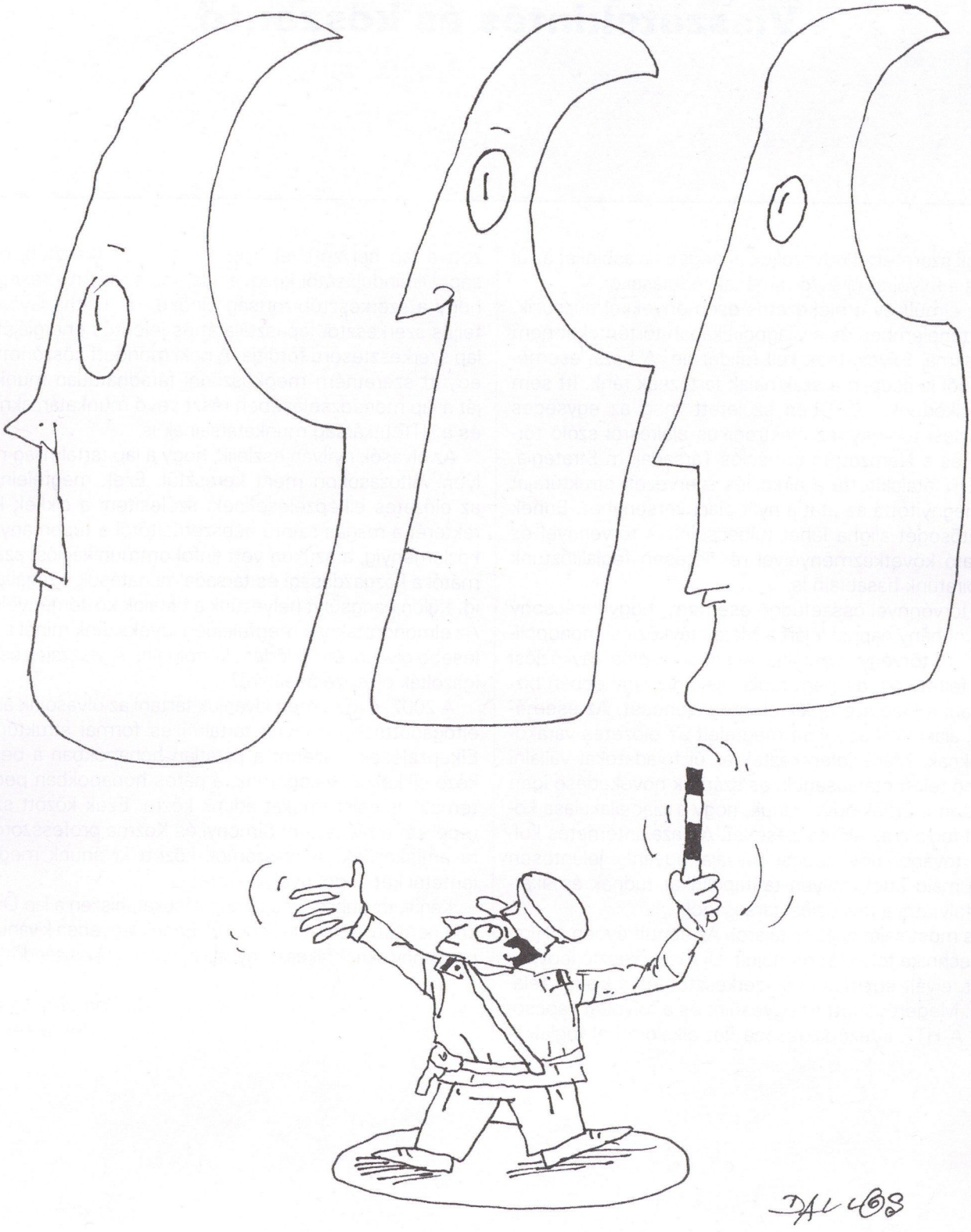
És most saját házunk tájáról. Az elmúlt évben a Híradástechnika folyóirat megújult. Új főszerkesztő jegyzi a lapot, elvált egymástól a szerkesztés és a kiadás feladata. Megerősödött az egyesület és a folyóirat kapcsolata. A HTE intézőbizottsága két alkalommal foglalkozott a lap helyzetével. Újjáalakult a szerkesztőbizottság. Újraindulásától kezdve a lap hatalmas nyeresége, hogy a szerkesztőbizottság elnöke, dr. Lajtha György teljes szerkesztői tapasztalatát és jelentős energiáját a lap szerkesztésére fordítja. A neki mondott köszönettel együtt szeretném megköszönni fáradhatatlan munkáját a lap menedzselésében részt vevő munkatársaknak és a HTE titkárság munkatársainak is.

Az olvasók nyilván észlelik, hogy a lap tartalmilag milyen változásokon ment keresztül. Ezek megfelelnek az előzetes elképzeléseknek: szélesíteni a cikkek karakterét a magas szintű népszerűsítőtől a tudományos közleményig, a szűken vett (infokommunikációs) szakmától a közgazdasági és társadalmi hatások vizsgálatáig. Külön hangsúlyt helyezünk a fiatalok közleményeire. Az elmondottaknak megfelelően igyekszünk minél szélesebb olvasói érdeklődést kiszolgálni. A visszajelzések igazolták elképzeléseinket.

A 2002. évben meg kívánjuk tartani az olvasóink által elfogadottnak bizonyult tartalmi és formai struktúrát. Elképzeléseink szerint a páratlan hónapokban a beérkező cikkekből válogatunk, a páros hónapokban pedig tematikus célszámokat adunk közre. Ezek között szerepel két emlékszám: Simonyi és Kozma professzorokra emlékezünk. A célszámok között kívánunk megjelentetni két angol nyelvű számot is.

Kérjük további szíves támogatásukat, hiszen a lap Önökért nem születhet Önök nélkül. Ennek jegyében kívánunk mindannyiuknak sikeres, nyugodt, boldog új esztendőt!

Dr. Zombory László
főszerkesztő



Neurális skalár és vektor hiszterézis operátor

KUCZMANN MIKLÓS – IVÁNYI MIKLÓSNÉ

Budapesti Műszaki és Gazdaságtudományi Egyetem (BME)
Elméleti Villamosságtan Tanszék

L

A klasszikus Preisach hiszterézis modell a legáltalánosabban alkalmazott szimulációs technika a mágneses anyagok viselkedésének matematikai leírására. Weiss hipotézise szerint a ferromágneses anyagok adott irányítottságú, telítésig mágnesezett elemi térrészekből, ún. doménekből épülnek fel, amelyek téglalap alakú elemi hiszterézis operátorokkal, hiszteronokkal reprezentálhatók. A Preisach-modell a mágneses anyag mágnesezettségét sok elemi, ideális hiszterézis operátor együttes hatásaként írja le, s az egyes hiszterézis operátorok állapota például Gauss típusú valószínűségi eloszlásfüggvény segítségével adható meg. Az előrecsatolt neurális hálózatok a Kolmogorov–Arnold-féle függvényreprezentációs tétel értelmében alkalmasak tetszőleges folytonos nemlineáris függvény közelítő előállítására. A cikkben bemutatásra kerülő hibrid skalár hiszterézis modell a neurális hálózatok approximációs képességére, továbbá egyszerű hipotéziseken alapuló ha-akkor típusú szabályokat magába foglaló tudásbázisra épít. A kifejlesztett modell alkalmas nem kongruens minor hurkok szimulálására is, működését a klasszikus skalár Preisach-modell eredményeivel hasonlítjuk össze. A skalár modell általánosításaként kidolgoztuk a 2 és a 3 dimenziós vektor modelleket, amelyek identifikációjára módszert ajánlunk. Az eljárás hatékonyságát ábrákon illusztráljuk.

Kulcsszavak: hiszterézis karakterisztika, Everett felület, vektor hiszterézis, előrecsatolt neurális hálózatok, backpropagation tanító algoritmus.

Bevezetés

A hiszterézis karakterisztika szimulációja, azaz a ferromágneses anyagok mágnesezettségének, vagy mágneses indukciójának ismerete a külső mágneses térerősség függvényében rendkívül fontos az egyre nagyobb teret hódító számítógéppel segített tervezés (CAD) és a különböző elektromágneses térszámítási programcsomagok alkalmazása során. A skaláris hiszterézis modellek megfelelően leírják a $H(t)$ mágneses térerősség és az $M(t)$ mágnesezettség közötti nemlineáris és többértékű függvénykapcsolatot, amennyiben ezen vektorok mindvégig párhuzamosak maradnak egymással. Az esetek túlnyomó részében, a gyakorlati életben is előforduló alkalmazások során azonban a mágneses térerősség és a mágnesezettség vektorok nem párhuzamosak. Például a transzformátorok egyes tartományaiban (sarkok) elkerülhetetlen a mágneses indukcióvektor elfordulása. Az egyes berendezések tervezése, analízise során szükség van olyan modellre, amely leírja a mágneses térerősség vektor és a mágnesezettség vektor közötti kapcsolatot.

A mágneses anyagok hiszterézis karakterisztikája tehát a $H(t)$ mágneses térerősség és a mágneses anyag $M(t)$ mágnesezettsége között teremt kapcsolatot. Az $M(t)$ mágnesezettség adott t időpontbeli értéke nemcsak a $H(t)$ mágneses térerősség adott időpontbeli értékétől függ, hanem az anyag mágneses előéletétől is [1]. Ezen erősen nemlineáris és memóriával bíró rendszer modellezésére meglehetősen nehéz megfelelő struktúrát találni.

A mágneses jelenségek vizsgálata során több modell is született már a hiszterézis karakterisztika, illetve a vektor hiszterézis szimulálására, a mágneses anyagok viselkedésének reprodukálására, mint például a Preisach-modell, illetve annak általánosításai, módosításai [1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 19], a Jiles–Atherton-modell [1], vagy a Stoner–Wohlfarth-modell [1, 6, 7, 19], stb.

A cikkben röviden bemutatjuk a klasszikus skalár Preisach-modellt, illetve egy a neurális hálózatok függvényapproximációs képességén és egy szabálybázison alapuló hiszterézis modellt [14, 15, 16, 22, 23, 24, 25, 26, 27], illetve annak vektoriális általánosítását izotróp anyagok esetén.

A klasszikus skalár Preisach-modell

Preisach Ferenc, a Németországban dolgozó magyar mérnök 1935-ben ajánlotta számítási módszerét a hiszterézis jelenségének leírására [1,2,3,6,19]. A klasszikus Preisach-modell Weiss hipotézisén, azaz a mágneses domének elméletén alapszik, amely azt feltételezi, hogy a ferromágneses anyagok telítésig felmágnesezett, adott irányítottságú elemi térrészekből, ún. doménekből állnak. Lemágnesezett állapotban az egyes domének elemi mágnesezettségei egymás hatását kölcsönösen kiegyenlítik, ezért az anyag mágnesesen semleges. Külső mágneses tér hatására a domének fokozatosan rendeződnek, s így az anyag M(t) mágnesezettsége a hiszterézis karakterisztikának megfelelően változik. Ezen domének viselkedése tég-

lalap alakú elemi hiszterézis operátorokkal, ún. hiszteronokkal reprezentálhatók. Az elemi hiszterézis hurok az a és a b paraméterekkel jelölt fel- és lekapcsolási értékekkel egyértelműen leírható. Ezen két adat adja meg, hogy egy elemi hiszterézis operátor a H mágneses térerősség mely értékeinél vált előjelet.

A skalár Preisach-modell a mágneses anyag $M(t)$ mágnesezettségét egy adott t időpillanatban tehát sok elemi, ideális hiszterézis operátor együttes hatásaként tekinti (kölcsönható operátorok), azaz

$$M(t) = \iint_{\alpha \geq \beta} P(\alpha,\beta)\gamma(\alpha,\beta)H(t)\,d\alpha\,d\beta \tag{1}$$

ahol $P(\alpha,\beta)$ egy megfelelően konstruált – tipikusan Gauss típusú – kétváltozós eloszlásfüggvény, amely az egyes elemi hiszterézis operátorok valószínűségi eloszlásának modellezésére szolgál, továbbá a szorzat az elemi hiszterézis operátorok mágnesezettségét reprezentálja.

A Preisach-modell memóriájának szemléletes ábrázolása a matematikai általánosítások eredményeképp született meg. Ez az ún. Preisach-háromszög. A mágneses térerősség változásával az ún. lépcsős görbe mozog, s így határozza meg az egyes $\gamma(\alpha,\beta)H(t)$ szorzatok előjelét, az (1) integrál értékét.

A $P(\alpha,\beta)$ Preisach-eloszlásfüggvény számítására a

$$P(\alpha,\beta)=\begin{cases}\exp\left[-\dfrac{(\alpha-\beta-c)^2}{10^a}-\dfrac{(\alpha+\beta-d)^2}{10^b}\right], & \text{ha } \alpha+\beta \leq 0,\\ \exp\left[-\dfrac{(\alpha-\beta-c)^2}{10^a}-\dfrac{(\alpha+\beta+d)^2}{10^b}\right], & \text{ha } \alpha+\beta > 0\end{cases} \tag{2}$$

formulát használtuk [2], ahol $\alpha \in$ [-1.1], $\beta \in$ [-1.1]. Az a, b, c és d paraméterek segítségével a fő hiszterézis hurok mérete és formája hangolható, tehát egy valós mágneses anyagon mért hiszterézis karakterisztikához illeszthető [2,3]. A paraméterek valamely beállítása mellett különböző típusú hiszterézis karakterisztikákat kaphatunk (klasszikus és letapadó típusút), s a koefficiensek megfelelő szélsőérték kereső algoritmussal valós mágneses anyagon mért hiszterézis karakterisztikához illeszthetők [17,18].

A határhiszterézis hurokról visszatérő elsőrendű hurkok alkalmasak az $E(\alpha,\beta)$ Everett felület felvételére, melyből az eloszlásfüggvény egyszerűen számolható a

$$P(\alpha,\beta) = -\frac{\partial^2 E(\alpha,\beta)}{\partial\alpha\partial\beta} \tag{3}$$

kifejezéssel [1,19]. Az Everett felület felépíthető az

$$E(\alpha,\beta) = \tfrac{1}{2}\left(M_\alpha - M_{\alpha,\beta}\right), \tag{4}$$

formulának megfelelően, ahol $\alpha(H/H_s)$, $\beta(H/H_s)$, továbbá M_α a határhurkon elhelyezkedő α visszatérési pontnak megfelelő mágnesezettség, $M_{\alpha,\beta}$ pedig a β térerősséghez tartozó mágnesezettség az (α,M_α) pontból visszatérő görbe mentén. Az Everett felület és a visszatérő görbék között egyértelmű kapcsolat van, azaz az Everett tábla ismeretében az elsőrendű visszatérő görbék meghatározhatók, $M_{\alpha,\beta} = M_\alpha - 2E(\alpha,\beta)$

Az előrecsatolt neurális hálózatok

A nemlineáris függvényapproximáció feladata a klaszszikus eljárások mellett alternatív megoldásként megfogalmazható a neurális hálózatok elméletének felhasználásával is [12,13]. Az alkalmazások alapját a Kolmogorov–Arnold-féle függvényreprezentációs tétel képezi, melynek értelmében minden n változós $f(x_1,x_2,...,x_n)$ folytonos függvény approximálható az

$$f(x_1,x_2,...,x_n) = \sum_{q=0}^{2n} \phi_q\left(\sum_{p=1}^{n}\varphi_{pq}(x_p)\right) \tag{5}$$

formula felhasználásával, ahol az egyváltozós $\varphi_{pq}(\cdot)$ függvények folytonosak, monoton növekvők és a [0,1] intervallumon értelmezettek. A $\phi_q(\cdot)$ függvények szintén egyváltozósak.

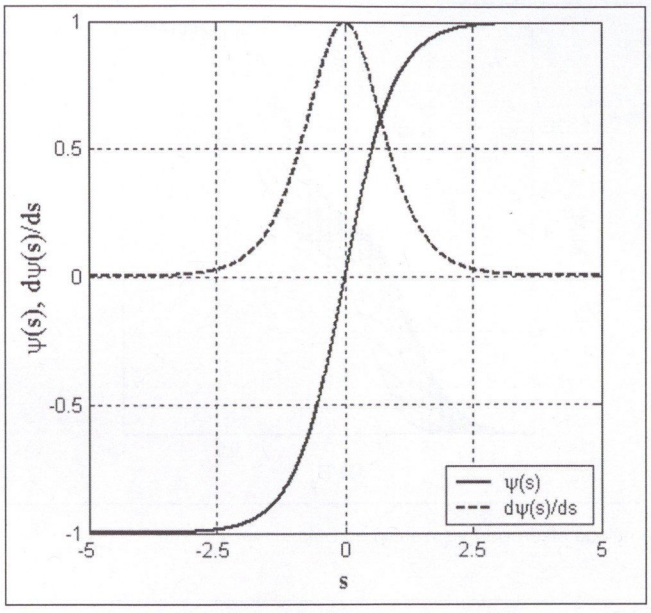
A neurális hálózatok egyszerű processzáló elemekből (neuron, processzáló elem) épülnek fel, amelyek nagymértékben összekapcsoltak. A neuronok y kimenete a bemenetükre érkező x értékek lineárisan súlyozott összege, amelyet egy folytonos, differenciálható és nemlineáris aktivációs függvény képez le, $y = \psi(\mathbf{W}^T\mathbf{x}+b)$, ahol $\mathbf{W}$ jelöli a súlyvektort, b pedig az eltolás. A $\psi(.)$ a kimeneti nemlineáris aktivációs függvény, amely tipikusan a bipoláris szigmoid függvény,

$$\psi(s) = \frac{2}{1+e^{-2s}} - 1. \tag{6}$$

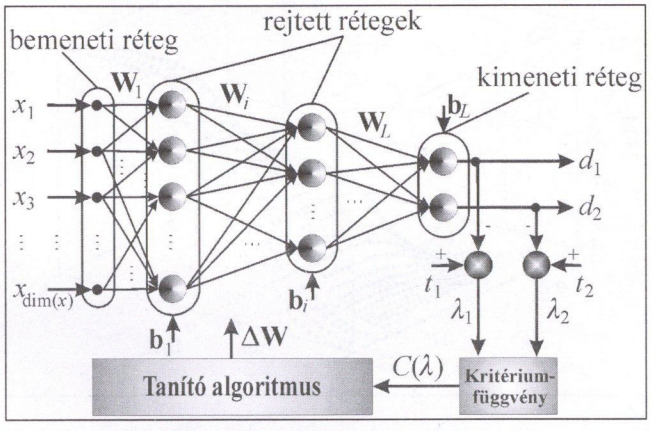
A szigmoid függvény és deriváltja az 1. ábrán látható. A $d\psi(s)/ds$ derivált analitikusan meghatározható, amely rendkívül fontos a gradiens alapú tanító algoritmusok alkalmazása során.

A neuronok rétegekbe történő szervezésével például a 2. ábrán látható L rétegű előrecsatolt hálózat építhető fel, amelynek (az aktivációs függvények rögzítése után) egyetlen szabadsági foka a W_i súlymátrixok és a b_i eltolási vektorok $(i = 1,...,L)$ beállítása. A súlyok a $\tau^{(N)} = \{(\mathrm{x}_k,\mathrm{t}_k), k = 1,...,N\}$ formában megadott tanítási mintahalmaz által reprezentált approximálandó $\mathrm{t} = f(\mathrm{x})$ függvény segítségével az ún. tanító algoritmussal hangolhatók, ahol $\mathrm{t}_k = f(\mathrm{x}_k)$, $\forall k$, $k = 1,...,N$.

A tanítás tehát egy olyan konvergens, iteratív optimalizáló eljárás, amelynek eredményeképp a neurális hálózat súlyait úgy állítjuk be, hogy az lehetőség szerint minél kisebb hibával közelítse meg a mintáival megadott folytonos függvényt. A neurális hálózat generalizációs képessége szerint nemcsak a tanítási mintahalmaz pontjaira ad egzakt választ, hanem nemlineáris interpoláció révén közöttük is.



1. ábra A szigmoid aktivációs függvény és deriváltja



2. ábra Az előrecsatolt neurális hálózat struktúrája, a tanítás művelete

Adott $\tau^{(N)}$ tanítási mintahalmaz mellett a cél tehát az optimális koefficienseket tartalmazó W^* vektor meghatározása, azaz a

$$\mathrm{W}^* : \min_{\mathrm{W}} \frac{1}{N} \sum_{n=1}^{N} \left(t_n - \emptyset\left(\mathrm{x}_n, \mathrm{W}\right)\right)^2 \tag{7}$$

minimalizálás elvégzése, ahol N a tanítási halmazban tárolt minták száma, a $d_i = \psi(\mathrm{x}_i,\mathrm{W})$ függvény pedig – az egyszerűség kedvéért – az egy kimenetű neurális hálózat által végzett leképezés. A tanítás lefutása után a neurális hálózat adott $\varepsilon>0$ hibával képes a mintáival adott $t = f(\mathrm{x})$ $\dim(\mathrm{x})$ függő- és egy független változós függvényt közelíteni, azaz

$$\exists \mathrm{W}^* : \left\| \psi\left(\mathbf{x}, \mathrm{W}^*\right) - f\left(\mathrm{x}\right) \right\| < \varepsilon \ . \tag{8}$$

A tanítás elvégezhető a gradiens alapú optimalizáló eljárások bármelyikével, melynek célja egy alkalmasan megválasztott az egyes $\lambda_i = t_i - d_i$ értékektől függő $(C)\lambda$ kritériumfüggvény minimalizálása. A legelterjedtebb módszer a backpropagation tanítás, vagy ennek egy módosítása, a gyorsabb Levenberg–Marquardt iteráció.

A neurális hálózat $\psi(\mathrm{x},\mathrm{W})$ leképzése matematikailag a

$$\psi\left(\mathrm{x}, \mathrm{W}\right) = \psi\left(\sum_i W_i^{(L)} \psi\left(\sum_j W_{ij}^{(L-1)} \ldots \psi\left(\sum_m W_{km}^{(1)} x_m\right)\right)\right) \tag{9}$$

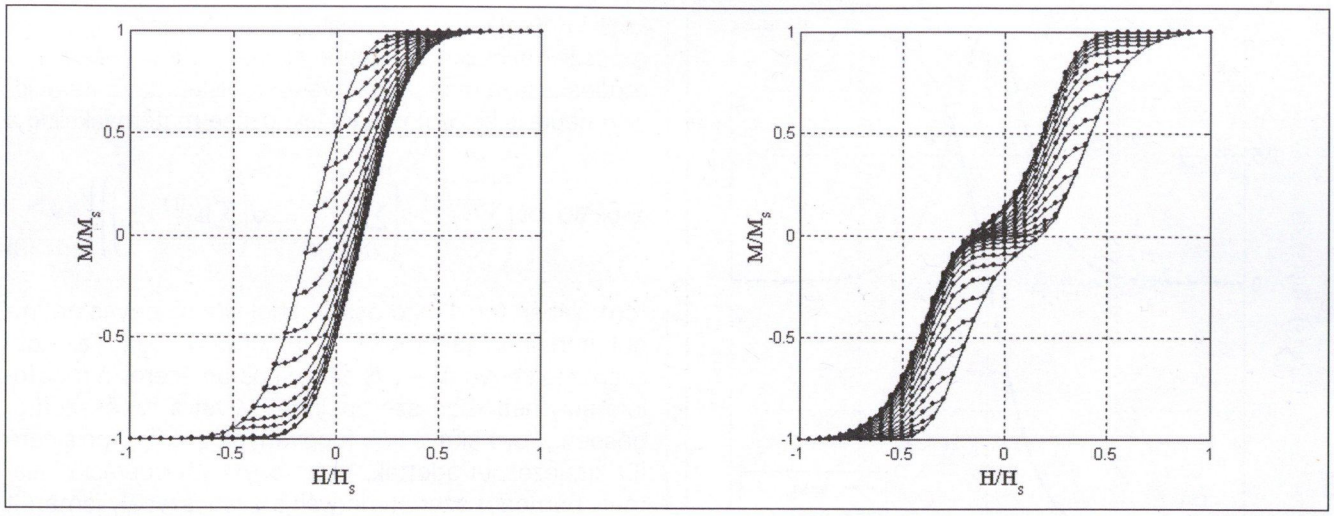
formulában foglalható össze, ahol $\psi(\cdot)$ az egyes neuronok nemlinearitását jelöli. A (9) kifejezésben – az egyszerűség kedvéért – a b_l eltolási paraméterek a megfelelő súlymátrixban szerepelnek. Mivel a (9) összefüggésben a $\psi(\cdot)$ aktivációs függvények a differenciálható (6) kifejezéssel adottak, ezért a $\psi(\mathrm{x},\mathrm{W})$ operáció valamely bemenet szerinti deriváltja a láncszabály ismételt alkalmazásával analitikus formában megadható.

A neurális skalár hiszterézis operátor

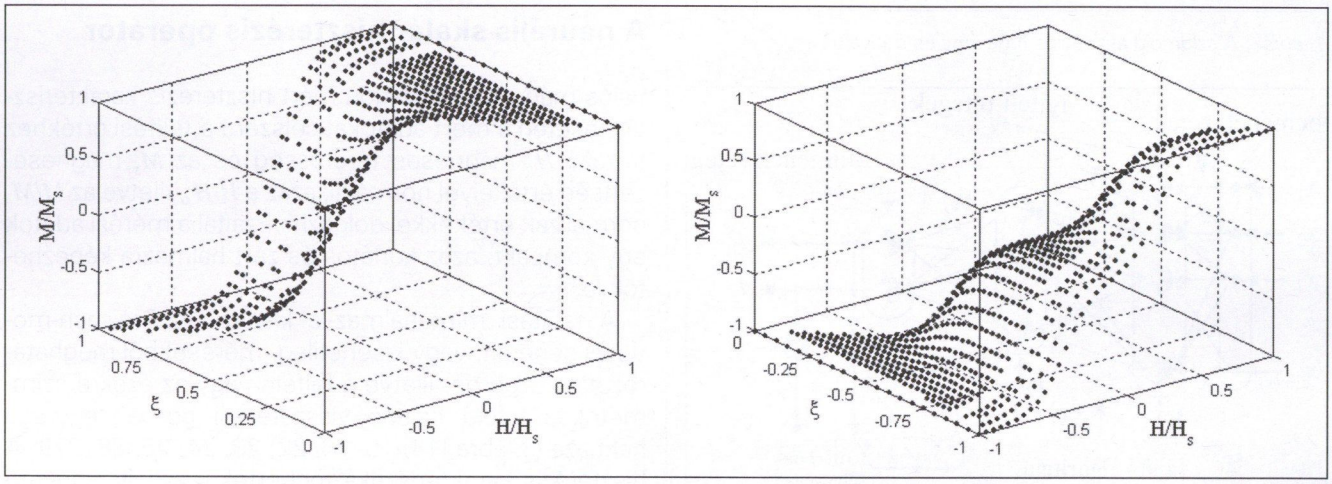
Valós mágneses anyagon mért hiszterézis karakterisztika esetén a mért adatokat célszerű a telítési értékhez tartozó H_s mágneses térerősség és az M_s mágnesezettség értékeivel normálni, azaz a H/H_s, illetve az M/M_s normalizált értékekkel dolgozni. Ezáltal a mérési adatok egy kompakt, azaz korlátos és zárt halmazra képezhetők le.

A tanítási mintahalmaz a klasszikus Preisach-modellel generált, vagy kísérletileg, mérésekből meghatározott szűzgörbe, illetve a felfelé vagy az ezekre szimmetrikus lefelé haladó visszatérési görbék egy-egy halmaza (3. ábra [14, 15, 16, 22, 23, 24, 25, 26, 27]). A hiszterézis karakterisztika többértékű, amely alapvető probléma az előrecsatolt neurális hálózatokkal történő approximáció során. Ez egy előfeldolgozó eljárással kezelhető, amely bármely hiszterézis karakterisztikára alkalmazható. A mért görbesereg felfelé haladó ágai egy pozitív, lefelé haladó görbéi pedig egy negatív skalárral megkülönböztethetők. A ζ betűvel jelölt paraméter a visszatérési értékekhez (turning point) tartozó H_{tp} mágneses térerősség értékekhez a felfelé vezető ágakon a $\zeta = 1-(1+H_{tp})/2$ formula alapján (4.a. ábra), míg a lefelé haladó görbéken a $\zeta = -(1+H_{tp})/2$ összefüggéssel határozható meg (4.b. ábra). A ζ paraméter a felfelé vezető elsőrendű visszatérési görbékre a [0,+1], a lefelé vezető ágakra pedig a [–1,0] intervallumba esik. Végeredményben tehát két független (H,ζ) és egy függő (M) változójú, egyértékű felületeket, azaz kétváltozós függvényeket kapunk, amelyek egyszerű előrecsatolt struktúrájú neurális hálózattal approximálhatók. A ζ paraméter szerepét az 5. ábra illusztrálja.

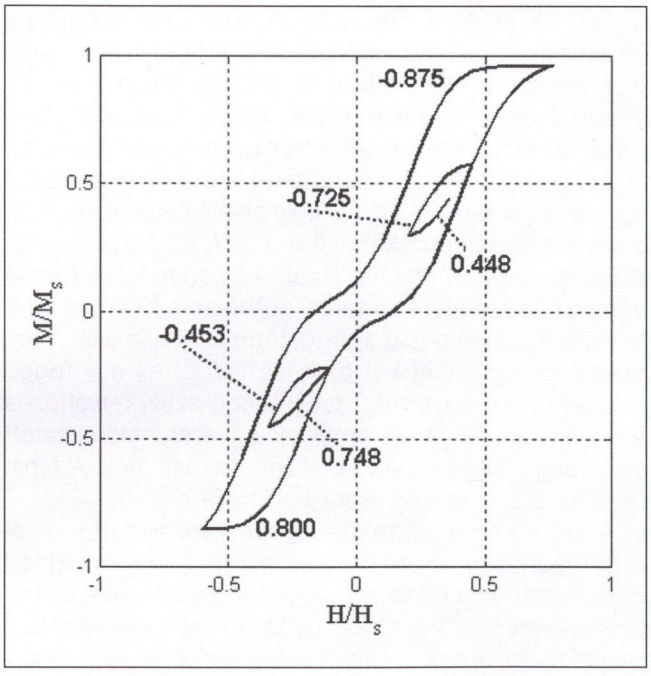
A szűzgörbe egyértékű függvénykapcsolatot realizál a H mágneses térerősség és az M mágnesezettség között, approximálása egy egyetlen rejtett réteget tartalmazó egy bemenetű és egy kimenetű neuronhálóval megoldható, amely a rejtett rétegben 8 neuront tartalmaz. A tanításhoz 41 $H - M$ mintapárt használtunk. Az előfeldolgozás eredményeképp kialakult felületek



3. ábra Példák különböző tanítási mintahalmazokra, a felfelé és a lefelé haladó elsőrendű visszatérő görbék



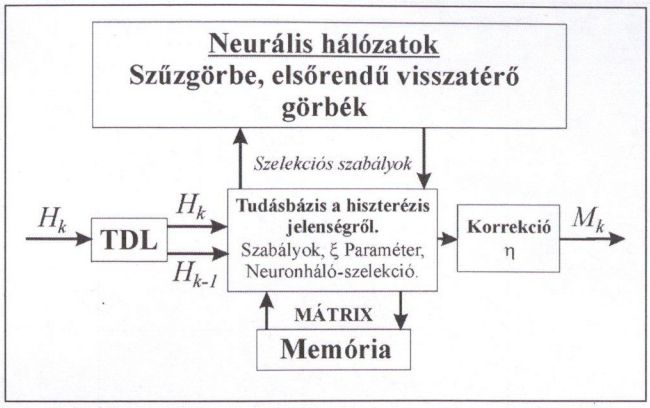
4. ábra A visszatérő görbék, az előfeldolgozás után



5. ábra Illusztráció a járulékos paraméter szerepére

approximálása egy három rejtett rétegből felépülő két bemenetű és egy kimenetű hálózattal megoldható, amely 7 neuront tartalmaz az első, 11 processzáló elemet a második és 2 neuront a harmadik rétegben. Tapasztalatunk szerint 500-800 mintából álló tanítási mintahalmaz elegendő egy megfelelő pontosságú approximáció megvalósításához. A 2 neurális hálózat tanítása a Levenberg–Marquardt backpropagation eljárással maximálisan kb. 10-30 percet vesz igénybe $5 \cdot 10^{-6}$ értékű célfüggvény eléréséhez, egy Celeron 566MHz számítógépen (192Mbyte RAM), MATLAB környezetben.

A kifejlesztett neurális hiszterézis modell tehát két neuronháló rendszeréből, illetve a köréjük épített járulékos szervekből áll. A hibrid modell blokkvázlata a 6. ábrán látható. Egy neuronháló az első mágnesezési görbe approximációját, egy pedig a felfelé vagy a lefelé futó elsőrendű visszatérő görbéket modellezi. Ezek a görbék tehát egy-egy fekete dobozban tárolódnak. Ezek után a feladat csupán annyi, hogy egy adott k diszkrét időpillanatban a mágneses anyag előéletének figyelembe vételével kiválasszuk a szükséges neuronhálót. A mágneses anyagok tulajdonságainak modellezését egy ún. tudásbázis realizálja, amely ha-akkor for-



6. ábra A neurális skalár modell blokkvázlata

mátumban hipotetikus szabályokat tartalmaz, illetve az egyes járulékos tagok vezérlését végzi. A modell memóriája csupán az előélet matematikai absztrakciója, amely a visszatérési pontokat reprezentáló értékeket tartalmazza egy-egy mátrix formájában. Egy mátrix tartalmazza a lefelé vezető görbék visszatérési értékeit, egy másik mátrixban történik a felfelé haladó ágak visszatérési értékeinek mentése. A mátrix egy oszlopában három érték tárolódik el a $[H_{tp},M_{tp},\zeta_{tp}]^T$ formában.

A visszatérési pont detektálása és a megfelelő neurális hálózat kiválasztása rendkívül egyszerű egy késleltető sorral (Tapped Delay Line, TDL) előállított $\{H_{k-1},H_k\}$ szekvencia vizsgálatával. A $H_k < H_{k-1}$, vagy a $H_k > H_{k-1}$ feltétel teljesülése egy (H_{tp},M_{tp}) koordinátákkal megadott visszatérési pontot reprezentál. Egy $H_{tp} = H_{START} = H_{k-1}$ $(M_{tp} = M_{START} = M_{k-1})$ visszatérési pont detektálása és memóriába mentése után a cél a megfelelő visszatérési ág kiválasztása egy görbeseregből, majd illesztése az adott (H_{tp},M_{tp}) visszatérési pontban. Ez ekvivalens a pontra legjobban illeszkedő visszatérési görbe ζ paraméterének meghatározásával, ami egyszerűen megoldható a regula falsi módszerével.

A neurális modell implementálásakor első lépésben feltételeztük, hogy a kialakuló minor hurkok önmagukban záródnak. Ha a H mágneses térerősség változása olyan, hogy egy minor hurok nyitása után azt zárni igyekszik, akkor a modell nem üres memória esetén az alábbi szabályok szerint működik: ha a mágneses térerősség értéke növekszik (csökken), akkor az aktuális minor hurok a modell memóriájában tárolt lefelé (felfelé) vezető ágakhoz tartozó visszatérési pontok közül a minimális (maximális) mágneses térerősség értékűnél záródik, azaz $H_{GOAL} = \min H_{tp}$ $(H_{GOAL} = \max H_{tp})$. A keresett minimális (maximális) H_{tp} érték mindig a memória utolsó oszlopában található, hiszen a H térerősség először mindig az utolsó nyitott minor hurkot igyekszik zárni. A minor hurok zárása után a memória utolsó oszlopait törölni kell.

Ha egy minor hurok nyitása során a memória valamely mátrixa egyetlen oszlopot sem tartalmazna, akkor visszatérési pont detektálása esetén a szimmetrikus hiszterézis karakterisztika feltételezése lép életbe, azaz $H_{GOAL} = -H_{START}$, $M_{GOAL} = -M_{START}$.

Ha a mágneses térerősség értéke növekszik (csökken), s egy minor hurok záródása után a törlési művelet következtében a lefelé (felfelé) haladó visszatérési pontokat tartalmazó mátrix üres lesz, akkor a $H_{GOAL} = +1$ $(H_{GOAL} = -1)$ és $M_{GOAL} = +1$ $(M_{GOAL} = -1)$ feltételeket kell alkalmazni.

Azt tapasztaltuk, hogy a H_{START} visszatérési pontra illeszkedő elsőrendű ág nem feltétlenül megy át azon az M_{GOAL} mágnesezettség értéken, ahol az aktuális minor hurok záródik. Ezt az eltérést egy $\eta = \eta(H)$ korrekciós taggal fokozatosan eliminálni lehet, $\eta = M_{GOAL} - M_{GOAL}^{(Hálő)}$.

A megfelelő neurális hálózat kiválasztása egyszerű szabályokon alapszik, azaz

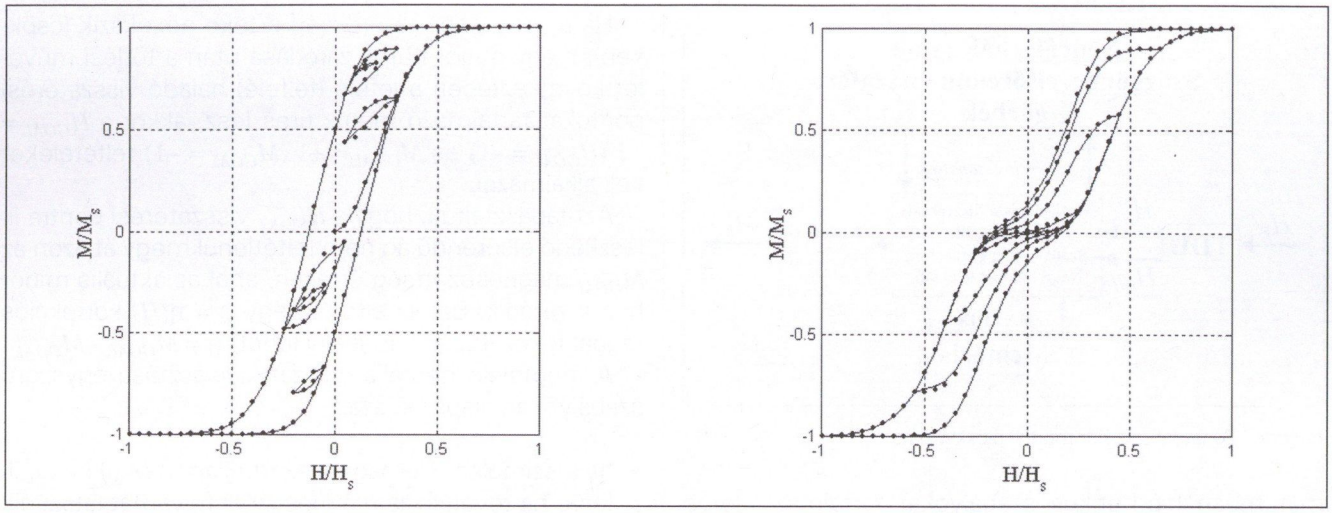
- ha a szimuláció lemágnesezett állapotból ( ) indul, illetve ha reverzibilis mágnesezési folyamat játszódik le, akkor a szűzgörbét approximáló hálót kell kiválasztani,
- ha egy visszatérési pontban lefelé (felfelé) vezető görbét kell illeszteni, akkor a lefelé (vagy felfelé) vezető ágakat modellező neuronhálót kell alkalmazni, figyelembe véve a szimmetriát,
- ha egy minor hurok záródása után a memóriában a megfelelő mátrix nem tartalmaz visszatérési pontokat, akkor az első mágnesezési görbét approximáló hálót kell kiválasztani, hiszen a szűzgörbéről induló minor hurok zárása után a szűzgörbén kell tovább haladni.

A szűzgörbe egy adott értékű mágneses térerősség alatt reverzibilis mágnesezési folyamatot ír le, ezen határ felett irreverzibilis mágnesezés játszódik le. Ez a normalizált határérték a modell paramétere, amely egy megfelelően kis érték, például 0,05.

A mágneses anyagok jellegzetes tulajdonsága, hogy a minor hurkok stabilizálódásához több oda-vissza történő mágnesezésre van szükség a H_{START} és a H_{GOAL} értékek között. Ez az aszimptotikusan lejátszódó jelenség az ún. akkomodáció. Mindez modellezhető az ún. moving modell szerinti általánosítással, amely egy pozitív visszacsatolást jelent, $H_k < H_k + \alpha M_{k-1}$, ahol α a mágnesezettségtől független, megfelelően kis érték [1].

A X_{diff} differenciális szuszceptibilitás analitikus formulával megadható, hiszen a neurális hálózatok kimenete folytonos és képlet formájában felírható függvénye a bemenetnek, s így a $X_{diff} = dM/dH$ analitikusan kifejezhető. Ezen tétel jelentősége abban rejlik, hogy az elektromágneses térszámítás során egy nemlineáris differenciálegyenletet kell megoldani, s mivel a dM/dH értéke analitikus formában kifejezhető, ezért alkalmazni lehet a Newton–Raphson iterációs technikát, amely gyorsabb, mint például a bevált fix pontos eljárás.

A kidolgozott módszert összehasonlítottuk a klasszikus Preisach-modellel. A 7. ábrán különböző gerjesztésekre adott karakterisztikákat ábrázoltunk, ahol pontsor jelöli a neurális hiszterézis modell, folytonos vonal pedig a Preisach-modell által generált kimeneti értékeket. Az ábrákból látható, hogy a modell alkalmas nem kongruens és magasabb rendű minor hurkok szimulációjára.



7. ábra A Preisach- és a neurális modell összehasonlítása különböző gerjesztések mellett

A neurális hiszterézis modell egy $M = \zeta(H)$ leképezést valósít meg, ami a skalár neurális hiszterézis operátor.

Az izotróp vektor modell

A mágneses térerősség és a mágnesezettség vektorok között fennálló függvénykapcsolat 2 és 3 dimenziós vektor modellek segítségével írhatók le pontosabban. Első lépésben az izotróp anyagok vektoriális leírásával és a vektor modellek identifikációjával foglalkozunk [1, 4, 6, 8, 11, 19].

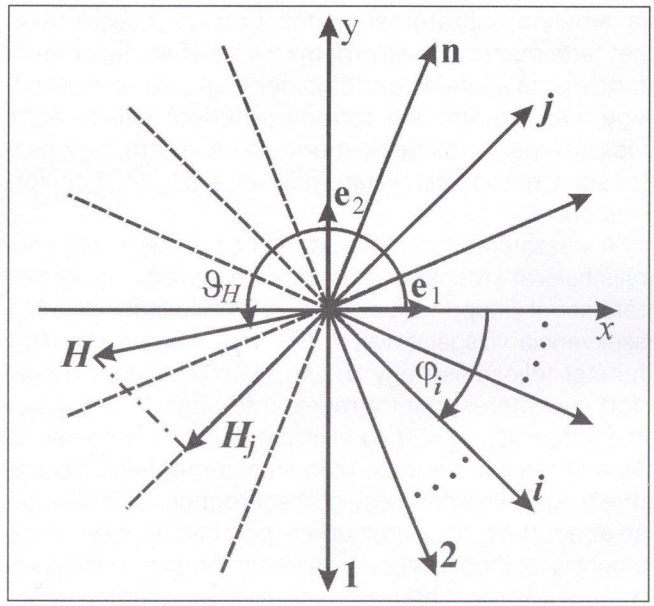
A 2 dimenziós vektor hiszterézis modell által szimulált $M(t)$ mágnesezettség az

$$\mathrm{M}(t)=\int_{-\pi/2}^{\pi/2}\mathrm{e}_{\varphi}\,\zeta\left(H_{\varphi}\right)\mathrm{d}\varphi \qquad (10)$$

integrálképlettel számolható [19], ahol e_{φ} a φ szög irányába mutató egységvektor, ξH_{φ} az ugyanezen irányban értelmezett skalár neurális hiszterézis operátor kimenete a $H_{\varphi} = |H|\cos(\varphi_H-\varphi)$ bemenetre, φ_H pedig a H mágneses térerősség szöge. Izotróp anyag esetén minden φ irányban azonos $\xi(H_{\varphi})$ karakterisztikát írhatunk elő. Numerikus modellezés során a $[-\pi/2,\pi/2]$ intervallumot egyenletesen fel kell osztani n irányra, azaz $\varphi_i = -\pi/2+(i-1)\pi/n$, ahol $i=1,\ldots,n$ és $\varphi_i = -\pi/2$ (8. ábra). A modell kimenete tehát a következőképp írható fel:

$$\mathrm{M}(t)\cong\sum_{i=1}^{n}\mathrm{e}_{\varphi_i}\,\zeta\left(\mathrm{H}_{\varphi_i}\right). \qquad (11)$$

Az M mágnesezettség vektorának két egymásra merőleges M_x és M_y komponense az egyes skalár modellek $M_i = \zeta(H_{\varphi i})$ kimeneteinek összegzett vetülete az x és az y irányokra, azaz



8. ábra Az irányok definiálása 2 dimenziós modell esetén

$$\mathrm{M}_x=\sum_{i=1}^{n}\mathrm{M}_i\cos\varphi_i\,,\quad \mathrm{M}_y=\sum_{i=1}^{n}\mathrm{M}_i\sin\varphi_i\,, \qquad (12)$$

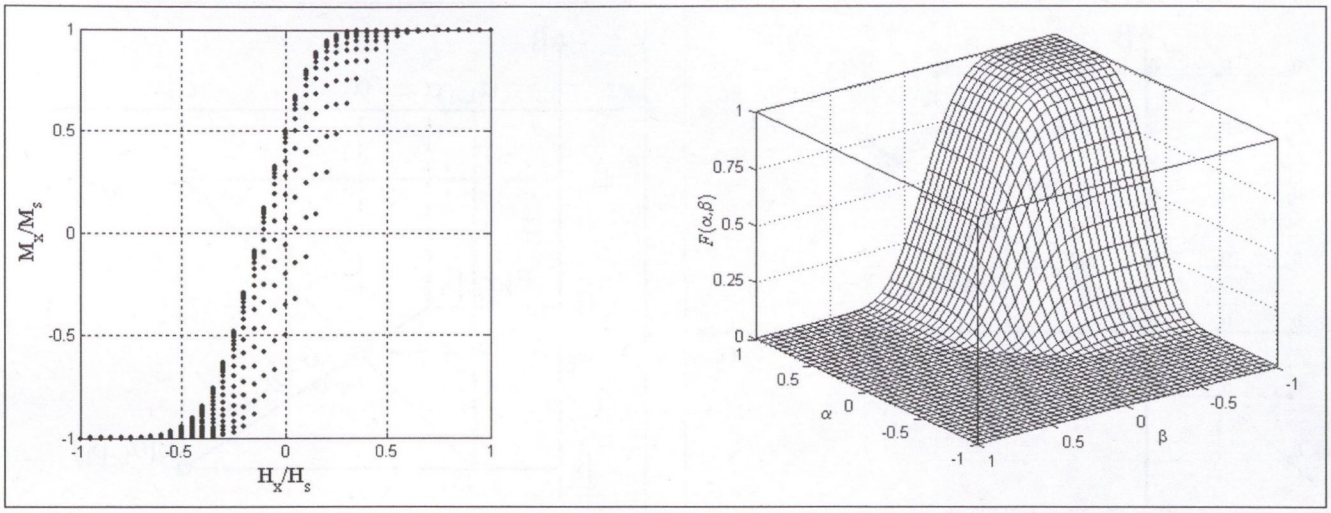
tehát az M mágnesezettség felírható az $M = M_x\mathrm{e}_1 + M_y\mathrm{e}_2$ alakban is, ahol e_1 és e_2 az x és y irányokba mutató ortogonális egységvektorok.

A 3 dimenziós vektor hiszterézis modell $M(t)$ kimenete az

$$\mathrm{M}(t)=\int_{-\pi/2}^{\pi/2}\int_{0}^{\pi}\mathrm{e}_{\vartheta,\varphi}\,\zeta\left(H_{\vartheta,\varphi}\right)d\vartheta\,d\varphi \qquad (13)$$

összefüggés szerint számolható [19]. Az adott ϑ és φ szögekkel jelzett irányba mutató vektorra vetített $H_{\vartheta,\varphi}$ érték a

$$H_{\vartheta,\varphi}=\left[a_1\ a_2\ a_3\right]_{\vartheta,\varphi}\left[H_{\mathrm{x}}\ H_{\mathrm{y}}\ H_{\mathrm{z}}\right]^{\mathrm{T}}, \qquad (14)$$



9. ábra Az identifikálandó visszatérő görbék és az Everett felület

összefüggéssel számolható, ahol $a = a_1e_1 + a_2e_2 + a_3e_3$ és $|a|=1$ [20]. Az M mágnesezettség ortogonális komponensei tehát az alábbiak:

$$M_x = \sum_{i=1}^{n} M_i \cos\theta_i\,,\quad M_y = \sum_{i=1}^{n} M_i \cos\zeta_i\,,\quad M_z = \sum_{i=1}^{n} M_i \cos\psi_i\,, \tag{15}$$

ahol θ_i, ζ_i és ψ_i az M vektor és a pozitív koordinátatengelyek közötti szögek, s így $M = M_xe_1 + M_ye_2 + M_ze_3$.

Ha 2 dimenziós vektor modellt feltételezünk és $F(\alpha,\beta)$ jelöli az x irányban mért visszatérő görbékből számított Everett felületet, $E(\alpha,\beta)$ pedig az egyes φ irányok mentén futtatott skalár hiszterézis modellek Everett felületét, akkor közöttük az

$$F(\alpha,\beta) = \int_{-\pi/2}^{\pi/2} \cos\varphi\; E(\alpha\cos\varphi, \beta\cos\varphi)\, d\varphi \tag{16}$$

összefüggés áll fenn [19], amelynek diszkretizált formája a következő:

$$F(\alpha_k,\beta_l) \cong \sum_{i=1}^{n} \cos\varphi_i\; E(\alpha_k\cos\varphi_i, \beta_l\cos\varphi_i), \tag{17}$$

ahol $\alpha_k = 2(k - (N+1)/2)/N$, $\beta_l = 2((N+1)/2-l)/N$, $k,l = 1,\ldots, N+1$ és az Everett tábla $(N+1)\times(N+1)$ méretű. Az identifikálandó normalizált hiszterézis karakterisztika a visszatérő görbékkel és a neki megfelelő Everett felület a 9. ábrán látható.

Ha $\beta_l = 0$, akkor a (17) összefüggés csak az α_k értékétől függ,

$$\begin{aligned} F(\alpha_k,0) &\cong \sum_{i=1}^{n} \cos\varphi_i\; E(\alpha_k\cos\varphi_i, 0) \\ &= \sum_{i_1=1}^{n_1} \cos\varphi_{i_1}\; E(\alpha_k\cos\varphi_{i_1}, 0) \\ &\quad + \sum_{i_2=1}^{n_2} \cos\varphi_{i_2}\; E(\alpha_k\cos\varphi_{i_2}, 0), \end{aligned} \tag{18}$$

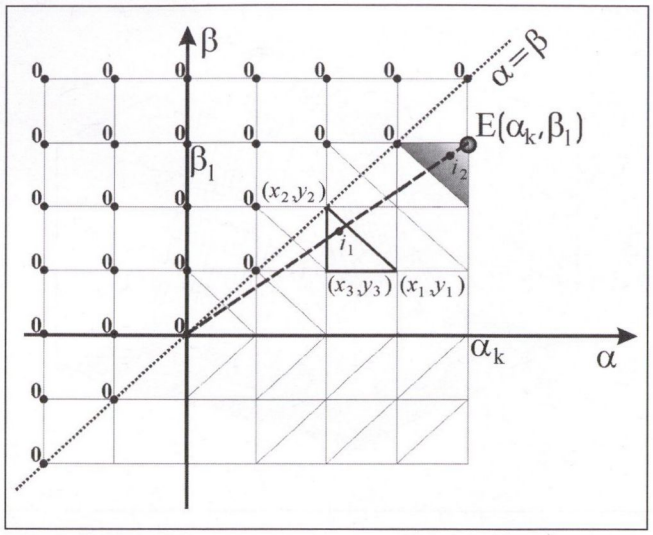
ahol az első szumma a már kiszámított értékeket tartalmazza, míg a második szumma az ismeretlen adatokat foglalja össze. Az első esetben az $E = (\alpha_k\cos\varphi_{i_1}, 0)$ érték két ismert érték közé esik, $\alpha_{j-1} \le \alpha_k\cos\varphi_{i_1} \le \alpha_j$, és $j<k-1$, második tagja pedig a keresett $E(\alpha_k,0)$ értéket tartalmazza $(\alpha_{k-1} \le \cos\varphi_{i_2} \le \alpha_k)$. Lineáris interpoláció alkalmazása, s a kiindulási (18) képletbe történő visszahelyettesítés után az

$$\begin{aligned} F(\alpha_k,0) = \sum_{i_1=1}^{n_1} \cos\varphi_{i_1} \Bigg\{ & E(\alpha_{j-1},0) \\ & + \frac{E(\alpha_j,0) - E(\alpha_{j-1},0)}{\alpha_j - \alpha_{j-1}} \left(\alpha_k\cos\varphi_{i_1} - \alpha_{j-1}\right) \Bigg\} \\ & + E(\alpha_{k-1},0) \left\{ (1+b_k) \sum_{i_2=1}^{n_2} \cos\varphi_{i_2} - a_k \sum_{i_2=1}^{n_2} \cos^2\varphi_{i_2} \right\} \\ & + E(\alpha_k,0) \left\{ a_k \sum_{i_2=1}^{n_2} \cos^2\varphi_{i_2} - b_k \sum_{i_2=1}^{n_2} \cos\varphi_{i_2} \right\} \end{aligned} \tag{19}$$

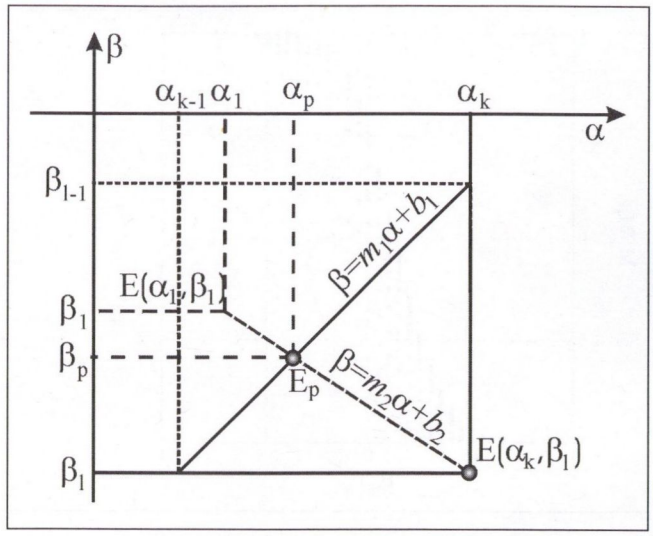
összefüggés kapható, ahol $a_k = \alpha_k/(\alpha_k - \alpha_{k-1})$, $b_k = \alpha_{k-1}/(\alpha_k - \alpha_{k-1})$, s amely már csak az $E = (\alpha_k,0)$ ismeretlen értéket tartalmazza. Az Everett felület szimmetrikus az $\alpha = -\beta$ egyenesre, tehát $E(0, \beta_k) = E(\alpha_k,0)$.

Ha $\beta_l \neq 0$, akkor a (18) összefüggéshez hasonló reláció írható fel. A számítás sematikusan a 10. ábrán követhető nyomon. Az $(\alpha_k\cos\varphi_{i_1}, \beta_l\cos\varphi_{i_1})$ pont már kiszámolt értékek közé esik, azaz $\alpha_{j-1} \le \alpha_k\cos\varphi_{i_1} \le \alpha_j$ és $\beta_m \le \beta_l\cos\varphi_{i_1} \le \beta_{m-1}$ $(m>l, j<k)$, akkor az $E(\alpha_k\cos\varphi_{i_1}, \beta_l\cos\varphi_{i_1})$ értéket az $A(x_1y_1z_1)$, $B(x_2y_2z_2)$, $C(x_3y_3z_3)$ pontok által határolt háromszögön lineáris interpolációval lehet megkapni, ahol $x_1 = \alpha_j$, $y_1 = \beta_m$, $x_2 = \alpha_{j-1}$, $y_2 = \beta_{m-1}$, $x_3 = \alpha_{j-1}$, $y_3 = \beta_m$. Három ponton átmenő sík egyenlete koordinátás írásmódban megadható a

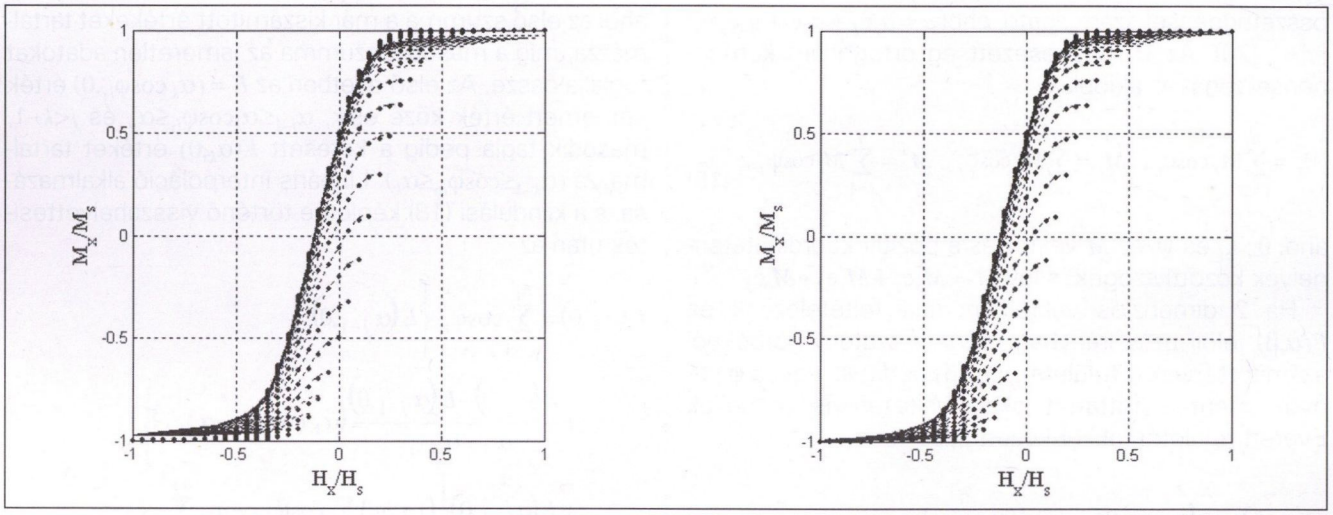
$$\begin{vmatrix} x - x_1 & y - y_1 & z - z_1 \\ x_2 - x_1 & y_2 - y_1 & z_2 - z_1 \\ x_3 - x_1 & y_3 - y_1 & z_3 - z_1 \end{vmatrix} = 0 \tag{20}$$



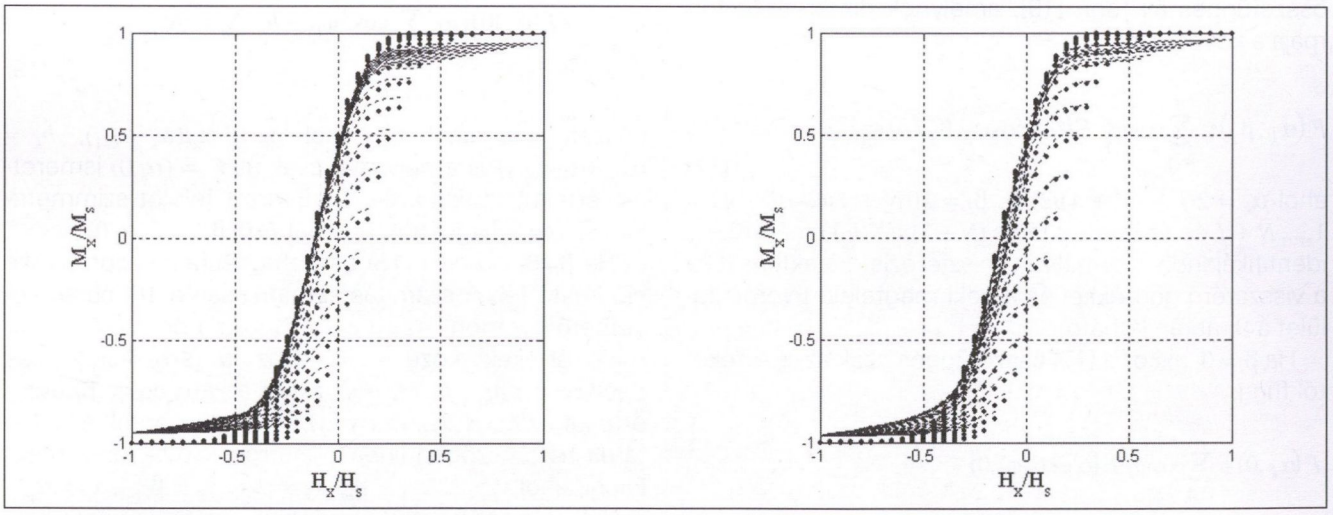
10. ábra Illusztráció az Everett tábla ismert értékeinek számításához



11. ábra Illusztráció az Everett tábla számításához



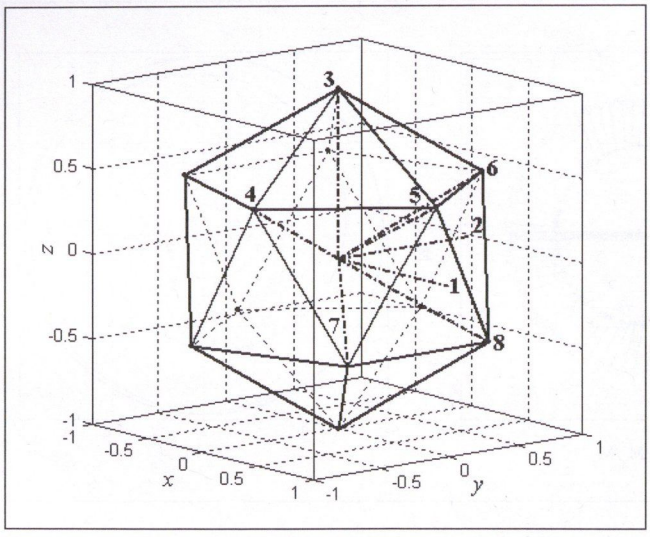
12. ábra A 2 dimenziós modell identifikációjának eredménye 10 (a) és 20 (b) irány figyelembevételével



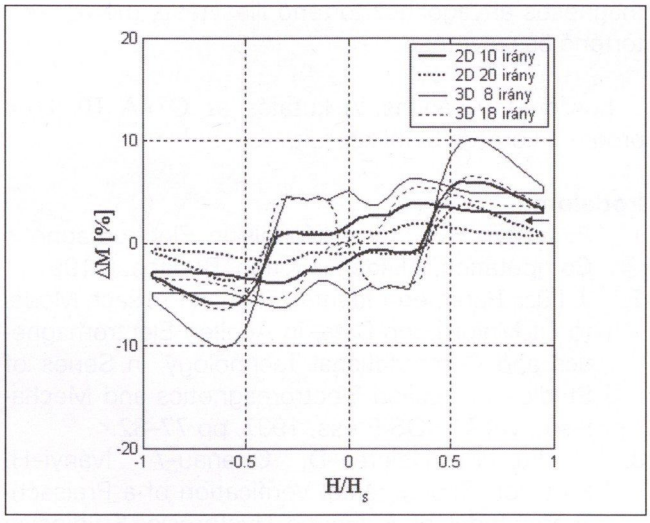
13. ábra A 3 dimenziós modell identifikációjának eredménye 8 (a) és 18 (b) irány figyelembevételével

kifejezéssel [20], melyből a keresett $z = E(\alpha_k \cos\varphi_{i_1}, \beta_l \cos\varphi_{i_1})$ érték átrendezéssel megkapható $(x = \alpha_k \cos\varphi_{i_1}, y = \beta_k \cos\varphi_{i_1})$.

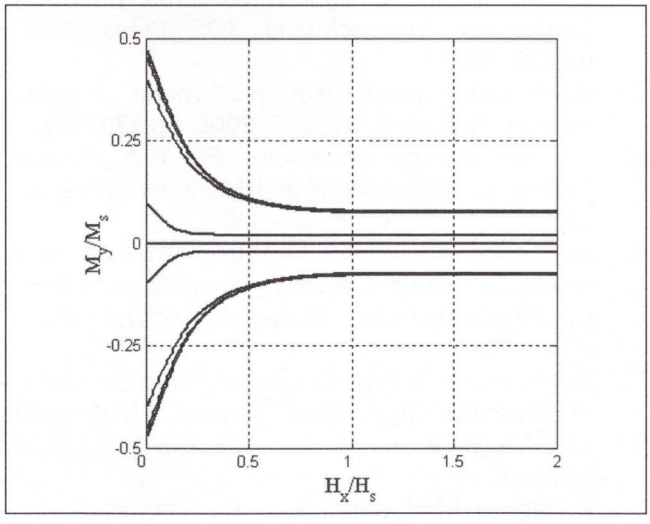
Az ismeretlen $E(\alpha_k,\beta_l)$ érték a 11. ábrának megfelelően fejezhető ki (például $\alpha_k>0$, $\beta_l<0$). Az (α_k,β_{l-1}), (α_{k-1},β_l) és az (α_1,β_1) (α_k,β_k) pontokon átmenő egye-



14. ábra Az ikozaéder



15. ábra A szimuláció hibája



16. ábra Anizotrópia

nesek metszéspontja adja az (α_p,β_p) pontot, ahol $E_p = E(\alpha_p,\beta_p)$ lineáris interpolációval kifejezhető. Az (α_p,β_p,E_p) pont és a $\beta = m_2\alpha + b$ egyenes ismeretében az $E(\alpha_k\cos\varphi_{i_2}, \beta_l\cos\varphi_{i_2})$ érték kiszámolható. Ezen összefüggések (17) képletbe történő visszahelyettesítése és átrendezése adja az ismeretlen $E(\alpha_k, \beta_l)$ értéket.

A 2 dimenziós modell identifikációja során $n = 10$, illetve $n = 20$ számú irány figyelembevételével a 12. ábrán látható eredményt kaphatjuk. Az ábrákon pontsor jelöli az eredeti hiszterézis görbét, szaggatott vonal pedig az identifikáció eredményét.

3 dimenziós modell esetén olyan térbeli alakzatokat célszerű választani, amelyek gömbbe írhatók. Ezek az ún. szabályos poliéderek (tetraéder, kocka, oktaéder, dodekaéder, ikozaéder), melyek közül a 20 szabályos háromszögből álló ikozaédert használtuk. Az ikozaédernek 12 csúcsa van, amelyek 6 pozitív irányt definiálnak, ezek mellett az x, y és z tengelyek pozitív irányát is figyelembe véve összesen 8 irányt kapunk. Ha az egyes háromszögek tömegközéppontjait is felhasználjuk, akkor 18 irányt lehet figyelembe venni. A két eset szimulációs eredménye a 13. ábrán látható. Az ikozaédert a 14. ábrán tüntettük fel [20,21].

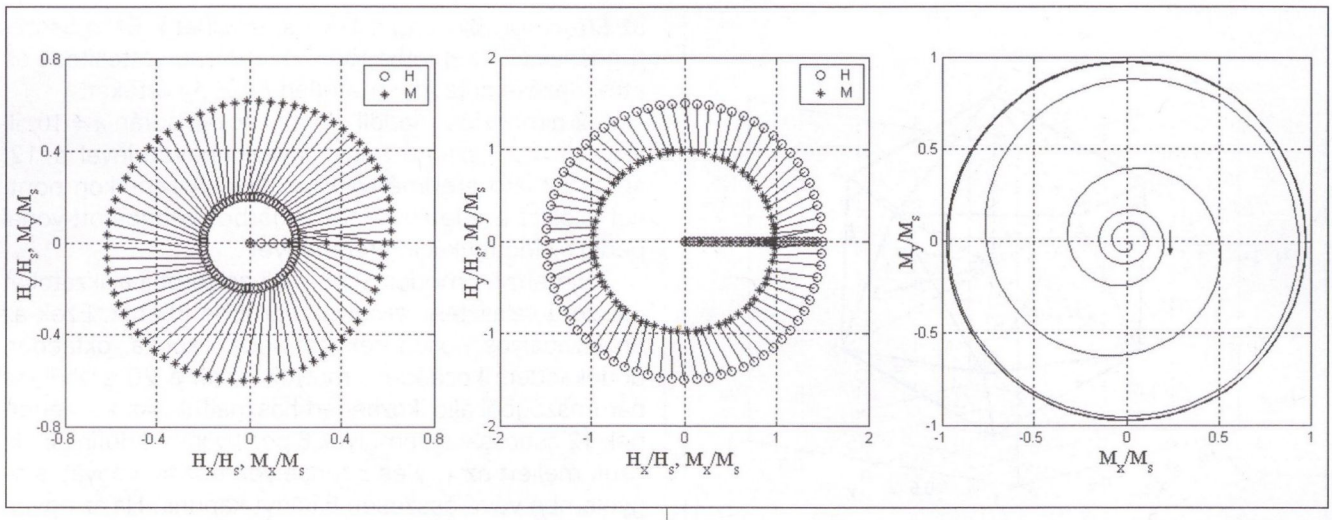
Megfigyelhető, hogy az irányok számának növelésével egyre jobb egyezést kapunk, ugyanakkor elektromágneses térszámításban nem célszerű figyelembe venni nagyszámú irányt, hiszen a vizsgált anyag több pontjában is futtatni kell egy-egy vektor modellt, amely meglehetősen növeli a szoftver futási idejét és memóriaigényét. A véges számú irány és az identifikáció során használt lineáris interpoláció miatt azonban mindig marad hiba, amely az irányok számának növelésével csökken, ahogy az a 15. ábrán látható a fő hiszterézis hurokra. A szimuláció relatív hibáját a $\Delta M = 100(M_{x,m} - M_{x,sz})$ összefüggéssel számolhatjuk, ahol $M_{x,sz}$ az x irányban mért, $M_{x,sz}$ pedig a vektor modellel szimulált normalizált mágnesezettség. Látható, hogy a relatív hiba a 2 dimenziós modell esetében kb. 5%-nál, 3 dimenziós modell esetén pedig kb. 10%-nál kisebb.

Sok esetben az identifikált Everett felületből kapott visszatérő görbék a mágneses térerősség nagyon szűk intervallumában nyújtanak elegendő információt a hiszterézis karakterisztika viselkedéséről. Ebben az esetben célszerű a H mágneses térerősséget tovább normálni, s csak a normalizáló érték alatt használni a neurális hálózatot, felette pedig az $M = M_s = 1$ normalizált értéket.

A vektor modell jellegzetes tulajdonságai

Az anyag mágneses előéletétől függő anizotrópia figyelhető meg a 16. ábrán [19]. Első lépésben az anyagot az y tengely mentén adott értékig felmágnesezzük, majd a mágneses térerősséget lecsökkentjük zérusra. Ezen mágnesezési folyamat M_y értékű remanens mágnesezettséget eredményez. Ezek után az anyagot az x tengely mentén mágnesezzük, amely azt eredményezi, hogy az ortogonális remanens mágnesezettség lecsökken.

Adott H_m amplitúdójú, ω körfrekvenciájú forgó mágneses térben történő mágnesezési folyamat látható a



17. ábra A mágneses anyag viselkedése forgó mágneses térben

17. ábrán. Ekkor a H mágneses térerősség vektorának változása megadható a

$$H(t)=\left\{H_x(t)=H_m\cos(\omega t),\ H_y(t)=H_m\sin(\omega t)\right\} \qquad (21)$$

formulával. A telítésig fel nem mágnesezett anyag forgó mágneses térben való viselkedése a 17.a. ábrán, míg a telítésig felmágnesezett anyag mágnesezettségének alakulása a 17.b. ábrán látható. Megfigyelhető, hogy a mágnesezettség vektora elmarad a mágneses térerősséghez képest [6,19]. Ha az anyagot egy fokozatosan növekvő H_m amplitúdójú, ω körfrekvenciájú forgó mágneses térben mágnesezzük fel, akkor a 17.c. ábrán látható mágnesezettséget kapjuk az óramutató járásával megegyező mágnesezési folyamatban [19].

A szimulációk során 2 dimenziós vektor modellt használtunk $n = 10$ irány figyelembe vételével.

Összefoglalás

A cikk egy neurális architektúrát ajánl a skalár hiszterézis karakterisztika modellezésére. A modell a neurális hálózatok függvény-approximációs képességét használja ki, s a ferromágneses anyagok elméletén alapuló szabálybázist használ. A megtanított neurális hálózatok fekete dobozként eltárolják a megtanított szűzgörbét és az elsőrendű visszatérő görbéket, s egyszerű szabályok felhasználásával vezérli azok kimenetét. Szimulációs eredményekkel, a klasszikus Preisach-modellel történő összevetéssel bizonyítottuk a modell működésének helyességét, a nem kongruens- és a magasabb rendű minor hurkok megjelenését.

Kidolgoztuk a 2 és a 3 dimenziós izotróp vektor modellek identifikációját, s ábrákon mutattuk be az ajánlott eljárás használhatóságát.

További célunk a vektor modell identifikációjának általánosítása anizotróp anyagokra, valamint a modellek beépítése elektromágneses térszámítási szoftverekbe, elsősorban az örvényáramos roncsolásmentes anyagvizsgálati eljárás szimulációjának kidolgozása ferromágneses anyagok esetére, illetve a modell valós mágneses anyagokhoz történő illesztése, mérésekkel történő összevetése.

Köszönetnyilvánítás. A kutatás az OTKA T034164 program keretén belül készült.

Irodalom

1. A. Iványi: Hysteresis Models in Electromagnetic Computation, Akadémia Kiadó, Budapest, 1997.
2. J. Füzi: Parameter Identification in Preisach Model to Fit Major Loop Data, in Applied Electromagnetics and Computational Technology, in Series of Studies in Applied Electromagnetics and Mechanism, vol.11, IOS Press, 1997, pp.77–82.
3. J. Füzi–E. Helerea–D. Oltenau–A. Iványi–H. Pfützner: Experimental Verification of a Preisach-Type Model of Magnetic Hysteresis, Studies in Applied Electromagnetics and Mechanics, Vol. 13, Non-linear Electromagnetic Systems, 8th ISEM Conference Braunschweig, IOS Press, 1997, pp.479–482.
4. J. Füzi–A. Iványi: Isotropic vector Preisach particle, Physica B, vol. 275, 2000, pp.179–182.
5. J. Füzi: Anisotropic Vector Preisach Particle, Journal of Magnentism and Magnetic Materials, vol.215–216, 2000, pp.597–600.
6. Zs. Szabó–A. Iványi: Anizotróp anyagok hiszterézis karakterisztikájának vektoriális szimulációja, Híradástechnika, Budapest, Vol.1, 1999/9, pp.15–38.
7. Zs. Szabó–A. Iványi: Computer-Aided Simulation of Stoner-Wohlfarth Model, Journal of Magnetism and Magnetic Materials, vol. 215–216, 2000, pp.33–36.
8. C. Ragusa–M. Repetto: Accurate Analysis of Magnetic Devices with Anisotropic Vector Hysteresis, Physica B 275, 2000, pp.92–98.
9. C. Serpico–C. Visone: Magnetic Hysteresis Modeling via Feed-Forward Neural Networks, IEEE Trans. on Magn., vol.34, 1998, pp.623–628.

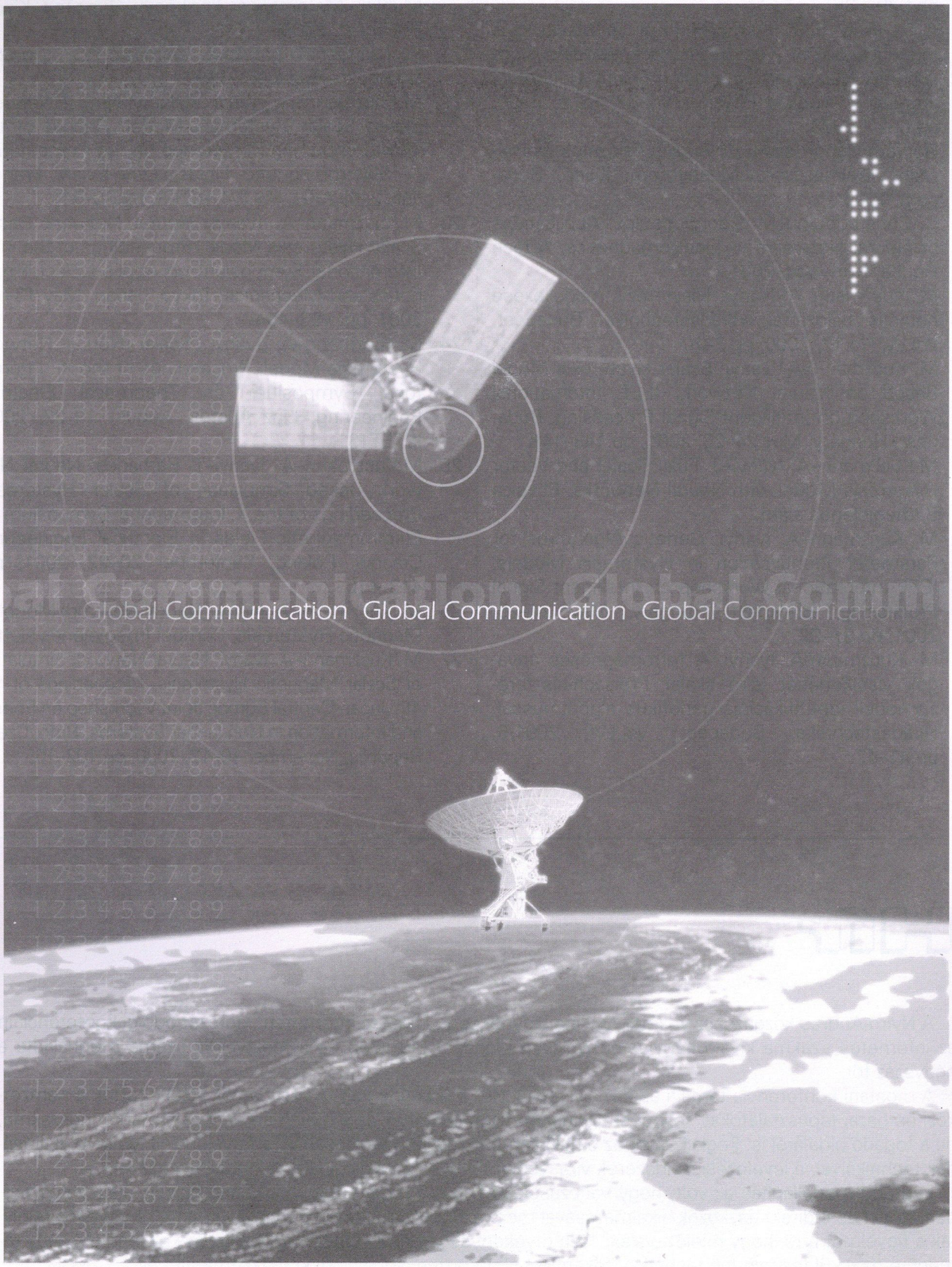
10. A. A. Adly–S. K. Abd-El-Hazif: Using Neural Networks in the Identification of Preisach-Type Hysteresis Models, IEEE Trans. on Magn., vol.34, 1998, pp.629–635.
11. A. A. Adly–S. K. Abd-El-Hafiz–I. D. Mayergoyz: Identification of Vector Preisach Models from Arbitrary Measured Data Using Neural Networks, Journal of Applied Physics, Vol.87, No.9, 2000, pp.6821–6823.
12. Horváth Gábor (szerk.): Neurális hálózatok és műszaki alkalmazásaik, Műegyetemi Kiadó, Budapest, 1995.
13. C. Christodoulou–M. Georgiopoulos: Applications of Neural Networks in Electromagnetics, Artech House, Norwood, 2001.
14. M. Kuczmann–A. Iványi: Hiszterézis modellezése neurális hálózattal, Híradástechnika, Budapest, Vol.LV, No.12, 2000, pp.2–10.
15. M. Kuczmann–A. Iványi: Scalar Hysteresis Model Based on Neural Network, IEEE International Workshop on Intelligent Signal Processing, Budapest, Hungary, May 24–25, 2001, pp.143–148.
16. M.Kuczmann–A. Iványi–J. Füzi: Scalar and Vector Hysteresis Model with Neural Networks, Physica B (megjelenés alatt).
17. M. Kuczmann–A. Iványi: Genetic Algorithms for Parameter Identification in Hysteresis Models, IEEE International Workshop on Intelligent Signal Processing, Budapest, Hungary, May 24–25, 2001, pp.87–92.
18. M. Kuczmann-A. Iványi: A ferromágneses anyagok viselkedését leíró skalár Preisach-hiszterézismodell identifikációja genetikus algoritmussal, Híradástechnika, Budapest, Vol.LVI, 2001/6, pp.41–47.
19. D. Mayergoyz: Mathematical Models of Hysteresis, Springer, 1991.
20. I. N. Bronstejn–K. A. Szemengyajev–G. Musoil–H. Mühlig: Matematikai kézikönyv, TypoTeX Kiadó, Budapest, 2000.
21. Füzi János: 3D grafika és animáció PC-n, Computer Books, Budapest, 1997.
22. M.Kuczmann–A. Iványi: A New Neural Network Based Scalar Hysteresis Model, Record of the 13th Compumag Conference on the Computation of Electromagnetic Fields, Lyon-Evian, France, July 2–5, 2001, Vol.2/4, PC1-9, pp.30–31.
23. M.Kuczmann–A. Iványi: Neural Network Based Scalar Hysteresis Model, Proceedings of the 10th International Symposium on Applied Electromagnetics and Mechanics, Tokyo, Japan, May 13–16, 2001, pp. 493–494.
24. M.Kuczmann–A. Iványi: Scalar Neural Network Hysteresis Model, Proceedings of the XI. Internatonal Symposium on Theoretical Electrical Engineering, Linz Austria, August 19–22, 2001, ISTET131.
25. M.Kuczmann–A. Iványi–T. Barbarics: Neural Network Based Simulation of Scalar Hysteresis, Proceedings of the X. International Symposium on Electromagnetic Fields in Electrical Engineering, Cracow, Poland, September 20–22, 2001, pp. 413–416.
26. M. Kuczmann–A. Iványi: Neural Network Model of Magnetic Hysteresis, Compel (megjelenés alatt).
27. M. Kuczmann–A. Iványi: Neural Network Simulation of Scalar Magnetic Hysteresis, Proceedings of the 4th Japan-Central Europe Joint Workshop on Energy and Information in Non-Linear Systems, Brno, Czech Republic, November 10–12, 2000, pp.102–105.

Hír

A Nyírő András közgazdász vezette On-line Ügynökség „Üzlet az interneten" sorozat eddigi konferenciáin az internetes szakma kiváló képviselői nyolcvan előadást tartottak, és a résztvevők száma meghaladta a négyszáz főt.

A mostani konferencia témája az E-mail/Newsletter marketing volt. A résztvevők áttekintették a nemzetközi és hazai tapasztalatokat, fejlődési trendeket. Megvizsgálták az e-mail-marketinget a marketingszakma, de a fogadó oldaláról is. Foglalkoztak az e-mail-kampányok lebonyolításának, a figyelemfelhívó levelek írásának technikáival, a levelezési rendszerek vírusvédelmével és a levélküldés jogi szabályozásával.

Legfőbb megállapítás az volt, hogy változások várhatók a hazai e-mail-marketing piacán. Változatos módon, direkt és indirekt eszközök alkalmazásával megkezdődött az internetes címgyűjtés. A résztvevők felhívták a figyelmet arra, hogy mielőtt valaki ilyen tevékenységet kezd, feltétlenül tisztában kell lennie a nagy tömegű e-mail-küldés minden technikai, főként azonban biztonsági és jogi következményével.


Global Communication Global Communication Global Communication

Hibás a kép? – ne állítsd át okvetlenül a készülékedet!

(Gondolatok a távközlési konvergenciákról)

STEFLER SÁNDOR

villamosmérnök
az Antenna Hungaria szakértője

A távközlési iparban az utóbbi időben már mániává vált a konvergencia emlegetése, és erre különböző koncepciók gyártása. A legtöbbet lehet hallani a fix és a mobil hálózatok, a vezeték nélküli rendszerek és az internet, az internet és a telefónia, a távközlés és a műsorszórás, az információtovábbítás és a szórakoztatás konvergenciájáról. Ez még korántsem kimerítő lista, de jól jelzi, hogy mennyire változásban van a távközlés fogalma és tartalma. Az azonban látszik, hogy jelentős összefonódások (konvergenciák) vannak a különböző technológiai, kereskedelmi és ipari szinteken. Az is világos, hogy nem minden konvergencia azonos ütemű és mértékű. Némely ezek közül csak „egyszerű" fejlődés, mások viszont földrengésszerű változásokkal járnak együtt.

Az említett scenáriókban általában felvetik, hogy szükséges-e konvergált ipari struktúrák kialakítása abból a célból, hogy hasznosítsák őket. Innen nézve minden konvergenciás változás kulcsszereplőjének a válasza a laza szövetségtől és társulástól a teljes összeolvadásig terjed. A Public Networks Europe 2001. októberi számában közölt cikke (Convergence: do not adjust your set) egy nem mérnök gazdaságpolitikus szemével vizsgálja a konvergencia különböző árnyalatainak a jelenségeit és a távközlési ipar változásainak hosszú távú következményeit. Az alábbiakban megkíséreljük visszaadni a szerző sajátos gondolkodásmódját, amit az alfejezetek (a TV-készülék legfontosabb kezelőszerveinek a terminológiáját alkalmazó) címei is jól illusztrálnak.

A vertikális igazítás

Az utolsó két évtized alatt a konvergencia ide-oda csúszkált a vertikális és a horizontális koncepciók között. Ez az oszcilláció tükrözi a trendek belső természetét mind az iparban, mind pedig a divatokban: minden újdonság először elbűvölő, aztán a háttérbe szorul, majd pedig vagy újra előkerül, vagy pedig teljesen eltűnik a felszínről.

Érthető módon a 80-as évekig a vertikális integráció volt a fontosabb, ekkor a hálózati szolgáltatók felismerték, hogy a hálózatok üzemeltetése és a szolgáltatások biztosítása nem csak a szükséges infrastruktúrák és végberendezések létrehozásától függ. Így a technológia „előállítása" bizonyos mértékben konvergált a hálózat- és szolgáltatásbiztosítás felé.

Az 1990-es évek során a horizontális integráció vált divattá, olyan szövetségek létrehozásával, amelyek a globális elérést és a végponttól végpontig történő szolgáltatást célozták meg. Ez a bizonyos mértékig megfoghatatlan cél határozta meg az operátorstratégiákat az évtized legnagyobb részében, és mellékessé tették a vertikális funkciókat, így pl. a technológiafejlesztést.

A múlt évszázad vége felé a horizontális és vertikális *dezintegráció* vált dominánssá. A szövetségek széthulltak, az elkülöníthető üzleti tevékenységek, mint pl. a vezeték nélküli szolgáltatások, önálló vállalkozásokba sodródtak ki. A globalizációs és konvergenciatrendek nem értékelődtek elég magasra ahhoz, hogy igazolják az integrált, monolitikus szolgáltatók létét.

Ez az utolsó pont különösen fontos. A horizontális és a vertikális közti eltérés gyorsan elferdíthető egy negyedfordulatos jobbra, vagy balra fordítással. Úgy is lehetne érvelni, hogy a vertikális és a horizontális a szemlélő nézőpontjától függ. Jelenleg különböző financiális krízisek következtében a legtöbb távközlési szolgáltató „fekszik". Ez pedig elszívta a lelkesedést a horizontális terjeszkedéstől és sok esetben a vertikális látszik ígéretesebbnek.

A horizontális igazítás

A kulcs a „monolitikus" szóban van. Könnyű figyelmen kívül hagyni a legtöbb európai távközlési szolgáltatónál a majdnem egy évszázados monopóliumuk és állami tulajdonlásuk során kialakult gondolkodásmódot. Ezek szó szerint kontrollálták az új technológiák beengedését, és így a távközlési univerzum mindentudó vezetőinek tűntek. Minden, ami történt, csak ezen mindenható szolgáltatók kifejezett kívánságára történhetett. Ez megfelelő szituáció lehetett egy olyan korban, amikor az új technológiák: a telex, a fax, az analóg mobiltelefon lassú ütemben érkeztek: úgy 10 évenként egy-egy. A 80-as évek óta azonban az új technológiák gyorsuló terjedése próbára tette a monolitikus szolgáltatók képességeit.

Az új technológiák lavinaszerű megjelenése – néha kiegészítve, néha versenyezve egymással – megnyitotta a kapukat a konvergencia előtt. A telco-k már-már vallásos küldetéstudata minden új távközlési technoló-

giát megteremtő szerepükben nem szívesen látták az új technikák és szolgáltatások megjelenését más kezekben. Ez különösen igaz akkor, amikor az új fejlesztések – mint pl. az internet – egészséges kereskedelmi termékként kezdenek önálló életet és teremtenek versenyhelyzetet. Az új technológiák fejlődési üteme és mennyisége néha „állva hagyta" a távközlési szolgáltatókat, akik nem tudták időben pótolni az ezekhez szükséges tudást. Ennek ellenére az az ötlet, hogy hagyják az újonnan érkezetteket alakulni – azaz a fejlődés irányításának az átengedése a most már versenytársak számára –, ellentétben állt a monopolhelyzetet élvezők gondolkodásmódjával.

A konvergencia kiutat mutat ebből a helyzetből. Lehetővé teszi a telco-k számára, hogy megtartsák pozícióikat, és a hiányzó tudást megszerezzék (felhasználva a régi tanácsot: akit nem tudsz legyőzni, azt vedd meg!). Sőt még azt is biztosítja, hogy bizonyos (bár korlátozott) mértékben befolyásolják azt az utat, amelyen a távközlési ipar fejlődik. Így nézve a dolgokat, a konvergencia tekinthető a pörgő érme egyik oldalának is, amelynek a másik oldalán a versenyhelyzet van.

De a konvergenciastratégiák használata a telco-k dominanciájának a megőrzésére csapdát rejt magában. A szolgáltatókat kiszolgáltatja a divatnak, vagy az ipari hóbortoknak. Ez megnyilvánul az integrációk és dezintegrációk ismétlődő ciklusaiban és az inga lengésében a horizontális és vertikális integrációk között.

Kontraszt

Annak a megértéséhez, hogy milyen hatással vannak ezek az iparra, lényeges megismerni azokat a metszéspontokat, ahol a konvergencia létrejön, vagy ahol ezeket létrehozzák. Ennek az a jelentősége, hogy a konvergencia különböző formái a távközlés különböző hierarchiasíkjaiban különböző válaszokat igényelnek az érintettektől. Ezért érdemes újra osztályozni a sok különféle konvergenciascenáriót. Itt azon rétegek kezdetleges lebontása van jelen, amelyeken a konvergencia végbemegy a jelenlegi távközlési környezetben:

hálózat: a csomagkapcsolt és az áramkörkapcsolt rendszerek közti különbségtétel eróziója jól halad. Szemben az internet körüli túldimenzionált várakozásokkal, nyilvánvalóvá vált, hogy a VoIP típusú szolgáltatásokat a meghonosodott szolgáltatók újrafogalmazott hálózatain keresztül bonyolítják le. Ebben az értelmezésben a konvergencia nem több, mint a nyilvános hálózatok megnövelt képessége és hatékonysága, amelyben a gerinchálózatok csomagkapcsolásban, de az utolsó mérföldek még a klasszikus vonalkapcsolt módban működnek. Érdekes módon a VoIP példa arra is, hogy amit korábban a telco-k hegemóniájának a fenyegetésének értelmeztek, az a bevett szolgáltatók hasznára változott.

Alkalmazások/szolgáltatások: a fix/mobil scenáriók esnek ebbe a kategóriába. A felhasználók növekvő száma tekinti úgy a mobiltelefonját, mint az igazi telefont. Ezek a mobilterminálok lassan alternatív hozzáférő eszközként is működnek az internetes tranzakciókhoz. Talány azonban, hogy míg pl. a 3G technológiát az USA-ban a mobiltelefonok elterjedését segítő eszköznek tekintik, addig ugyanezt Európában csupán az internethozzáférés egy lehetséges módozatának. Nagy kérdés ezek után, hogy a kétféle megközelítés közül melyik (mindegyik, vagy egyik sem) lesz a meghatározó.

Szolgáltatásmenedzselés: azok, akik a realitásokat a koncepciók elé helyezik, azok a szolgáltatások menedzselését hajlamosak konvergáló környezetbe, a különálló szerviz-platformok technikai fúziója elé pozicionálni. A FOBOCO (Front Office, Back Office, Cellar Office) modell azt jelzi, hogy ez alkotja a kötőanyagát csaknem minden konvergenciastratégiának. Az integrált FOBOCO rendszerek megadhatják a legtöbb egy, vagy több hálózatot is üzemeltető szolgáltató válaszát a konvergáló piac kihívásaira. Ez megnyitja a kapukat a keresztmarketing és a keresztszolgáltatási kedvezmények felé, melyek jelenleg a legtöbb alapszolgáltatót lelkesítik. Ezzel ellentétben a konvergenciajátékokat ámításnak mutathatja a FOBOCO rendszerek integrálásának a kudarca, ami gyakran előfordul a gyakorlatban.

Tartalom: bár a tartalom jelenleg még „csúnya szó" a távközlési szolgáltatók számára, a vertikálisan integrálódott multimédia-szolgáltatások új modelljei azt jelzik, hogy kulcsfontosságúvá vált az örök vita van a tartalom vagy a szállítás elsőbbségéről. Az erre vonzó válasz az, hogy miért válasszuk valamelyiket, ha mindkettőt megszerezhetjük. A hálózati szolgáltatók igényt tartanak a tartalom-előállítók profitjának egy részére, már csak azért is, mert a tartalomszolgáltatók a sávszélességet csupán olyan közszükségleti cikknek tartják, aminek megvan az ára. A valóságban azonban egy telco jelszétosztó hálózatának a kombinálása a nagy médiavagy más tartalomszolgáltatók kimeneteivel nem olyan szörnyű dolog, mint néhány vállalati struktúrában működő tevékenységkonglomerátum, ami pedig gyakran előfordul az üzleti életben.

Ezen konvergenciaféleségek mindegyikében alapkérdés az, hogy azonosítani lehessen azt a pontot, ahol az elméleti logika és a gyakorlati lehetőség találkozik. Nem mindig működik az, aminek értelme van, de ez nem állítja meg az embereket és szervezeteket abban, hogy próbálkozzanak.

Színhalványulás

A fentebb felsorolt scenáriók felvetik azt a kérdést, hogy mi az optimális telco-struktúra. Pontosan ez az a pont, ahol a legtöbb tradicionális távközlési szolgáltató elkezdi elveszteni a magabiztosságát monopolhelyzetének további fenntartását illetően, és egy bizonytalanabb jövőbe ugrik fejest. Haladékkeresésük ma megtalálható vagy az összeolvadási és akvizíciós modelljeikben, vagy a szövetségi és partnerkapcsolati modelljeikben. Kritikus a telco-k viszonylagos helyzete abban az értéklánccban, ami a konvergáló távközlési és informáci-

ótechnikai világban számukra kiharcolható. Kétségtelen, hogy a jelentősebb távközlési szolgáltatók és azok, akik analizálják őket, más szektorokból keresnek példákat. Az ilyen keresések eredményei vegyesek.

Mint hálózatalapú iparnak, a távközlésnek is úgy kell kinéznie, mint más konvergáló struktúrának az üzleti életben. Egy vezető példa lehet erre az olajipar, amelyben a globális játszótérrel rendelkező szereplők az értéklánc minden fokát kézben tartják: a kitermelést, a szállítást, a feldolgozást és az értékesítést is. A teljes folyamat ilyen végponttól végpontig történő menedzselése azonos a legtöbb nagy távközlési cégnek a szabad verseny előtti korban tanúsított magatartásával.

Az ellenkező szemlélet azt mondja, hogy ma lehetetlen menedzselni egy ilyen struktúrát, ehelyett inkább a termékek és szolgáltatások márkanévvel ellátott marketingjét kell folytatni. Egy példa lehet erre a banki tevékenységek „ipara", ahol egy sor elkülönülő funkció: a bank, a hitel, a beruházás, a biztosítás nagykereskedelmi és viszonteladói szinteken működik magán- és közületi ügyfelekkel, márkanevekkel fémjelzett ernyők alatt.

Egy másik, talán zavarosabb összehasonlítás tehető a légi közlekedéssel. A gyártók építik a repülőgépeket, a légitársaságok működtetik ezeket, a repülőterek biztosítják az üzemvitelt, a légügyi hatóságok szabályozzák a feltételeket. A legutóbbi időkig úgy tűnt, az utasok élvezik a rendszer összehangolt működéséből származó előnyöket, bár ez a gazdasági logikával szembeszállt.

Mindegyik modellnek megvan a maga belső gyengesége. Egy integrált és teljesen egy kézben tartott értékesítési lánc ki van téve a versenyellenesség vádjának. Mivel ez egy olyan terület, ahol manapság a szabályozók egyre aktívabbakká válnak, a rizikó nagy. Egy laza társuláson alapuló, végponttól végpontig terjedő operáció hasonlóan hibás, mert a versenytársak kiszedegetnek egyes – az egészhez csatlakozó – egységeket. Mivel ma olyan korszakot élünk, amikor a versenyhelyzet a nap kérdése, ez is rizikós. A légiforgalmi példa analógiáját használták azok, akik hiába várakoztak a távközlés liberalizáláshullámára a 90-es évek elején.

Fényesség

Az USA gazdaságpolitikai gyakorlata lehetővé teszi a vállalatok számára tevékenységük folytatását azután is, hogy megbüntették őket fizetésképtelenség miatt, vagy csődöt jelentettek. Ez a gyakorlat, ami az 1980-as és 90-es évek légiforgalmi anarchiájáért is felelős, most újra visszaütött. Az elmúlt hónapok tragikus amerikai eseményeiből való felocsúdás során most ismét alaposan visszaesik a légi forgalom gazdaságossága.

A grandiózus hálózatépítések, mint pl. a globális ellátású Iridium műholdas rendszer, vagy egyes transzatlanti kábelek már szinte az akciós boltok leárazott termékei között szerepelnek. Azok, akik megkísérlik távközlési tevékenységük egészséges alapokra való építését, jogosan érezhetik magukat megbántva azon potenciálisan destabilizáló hatások miatt, amelyeket a jogi kibúvók tesznek lehetővé. A távközlési tevékenységek gazdasági elveinek az aláaknázása révén az ominózus gyakorlat még inkább veszélyezteti az elfogadott távközlési szolgáltatók konvergenciáját. Miért invesztáljanak be milliókat a hálózatokba, amikor a likvidálások során kialakult alacsony értékesítési árak következtében azok tört értékükön is megszerezhetők az elvérzett konkurenstől. Ironikus módon csak az exmonopolista távközlési cégek képesek fenntartani gazdasági életképességüket és szolid bevételi forrásaikat, amelyek a piaci változások és a fogyasztói igények fluktuálása fölé emelik őket. Eltanácsolva a telco-kat a divat mindenáron való követésétől, sorsuk attól függhet, hogy mennyire képesek ellenállni ezen igényeiknek.

Fekete és fehér

Miközben ellenállunk annak a kísértésnek, hogy pszichoanalízisnek vessük alá az ipart, itt csak azokat a gyengeségeket és erősségeket – és bizonytalanságokat – vetjük fel, amelyek manapság befolyásolják a távközlési szolgáltatók stratégiáját. A korábban nemzeti monopóliumot élvező telefontársaságok nem írhatók le minden további nélkül a távközlési palettáról, sőt – amennyiben szerencsések és óvatosan intelligensek – akár még az „egyenlők között az elsők" is lehetnek.

Ostobaság lenne a telco-k számára annak a feltételezése, hogy rivalizálni tudnak a szoftverkreáció és -értékesítés területén az olyan társaságok hegemóniájával, mint pl. a Microsoft. Hasonlóképpen kevés telco aspirálhat a Fox, a Hollywood, vagy akár a Reuters médiauralmára. Azonban az elmúlt évek néhány emlékezetes összeolvadás és kereszt-tulajdonlás a szoftver-, a média-, a távközlési és a KTV-szektorok között (különösen az USA-ban) azt mutatja, hogy még élnek az álmok a végső, konvergált távközlési, média- és számítástechnikai rendszerek megteremtésére.

Ennek teljes kontrasztjában van a vezeték nélküli távközlés, ahol a tőzsde összezavarja a konvergáló szolgáltatási portfóliókat, éppen abban az időben, amikor az ilyen scenáriók már kezdenek gyümölcsöt hozni. Évekkel a fix-mobil konvergencia folyamatos prédikálása után, az üzemeltetők leszerelik integrált struktúráikat, amikor is a piac – úgy látszik – kezdi elfogadni ezeket az ideákat.

Ezen anomáliák – azaz egyik oldalon a szektorok közti kereszttulajdonlások és összeolvadások grandiózus méretei, a másik oldalon pedig a telco-k összetörése – egyik magyarázata az lehet, hogy a pénzvilág irányítja a piaci stratégiát az ipar döntéshozó folyamatában is. Mint ilyen, a konvergencia alig több mint egy hasznos címke, ami ráfüggeszthető a financiális irányítású ügyletekre, amikor ez kedvező, vagy nyugodtan elfelejthető, ha nem az. A nagy összeolvadásoknak („mega-mergers") jó időkben csakúgy, mint a szétválásoknak a rossz időkben, voltaképpen alig van közük a konvergenciához.

Epilógus

Mérnök szemmel olvasva a fenti fejtegetéseket, rádöbbenhetünk, hogy a jelenségek nagy része hazai körülmények között is tapasztalható, és a számunkra korántsem hízelgő megállapításokban mennyi igazság van. Különösen az érinti közvetlenül a technológiákat mindig javítani igyekvő és az új fejlesztéseket létrehozó, azoknak mielőbbi gyakorlati alkalmazását kereső mérnököket, hogy most ők már csak „termékeket" létrehozó munkaerők, akiknek a munkája eltörpül az értékesítés és a marketing divatos szólamait hangoztatók tevékenysége mellett. A magyar mérnökök kreativitása rövidesen csak a különféle nemzetközi kiállításokról hazahozott nagyszámú rangos helyezésben válik láthatóvá, a kutatók-fejlesztők nemigen számítanak a társadalom megbecsült és elismert tagjainak. Úgy tűnik, a mai piacközpontú és elmaterializálódott társadalom célul tűzte ki azt, ami nemrégiben egy jelentős távközlési konferencián hangzott el: „nem a termékek létrehozása, hanem azoknak az eladása a művészet." A magyar távközlés valódi értékeket létrehozó kutató-fejlesztő mérnökei bizony nem osztják ezt a véleményt. Ha nincs mit eladni, akkor az üzletemberek sem tudnak csodát tenni. Ötletes, új termékek, ha kellő időben jelennek meg, véget vethetnek a recessziónak. Tehát csak a fejlesztés visz előre, és ezen gazdagodhat meg a kereskedelem.

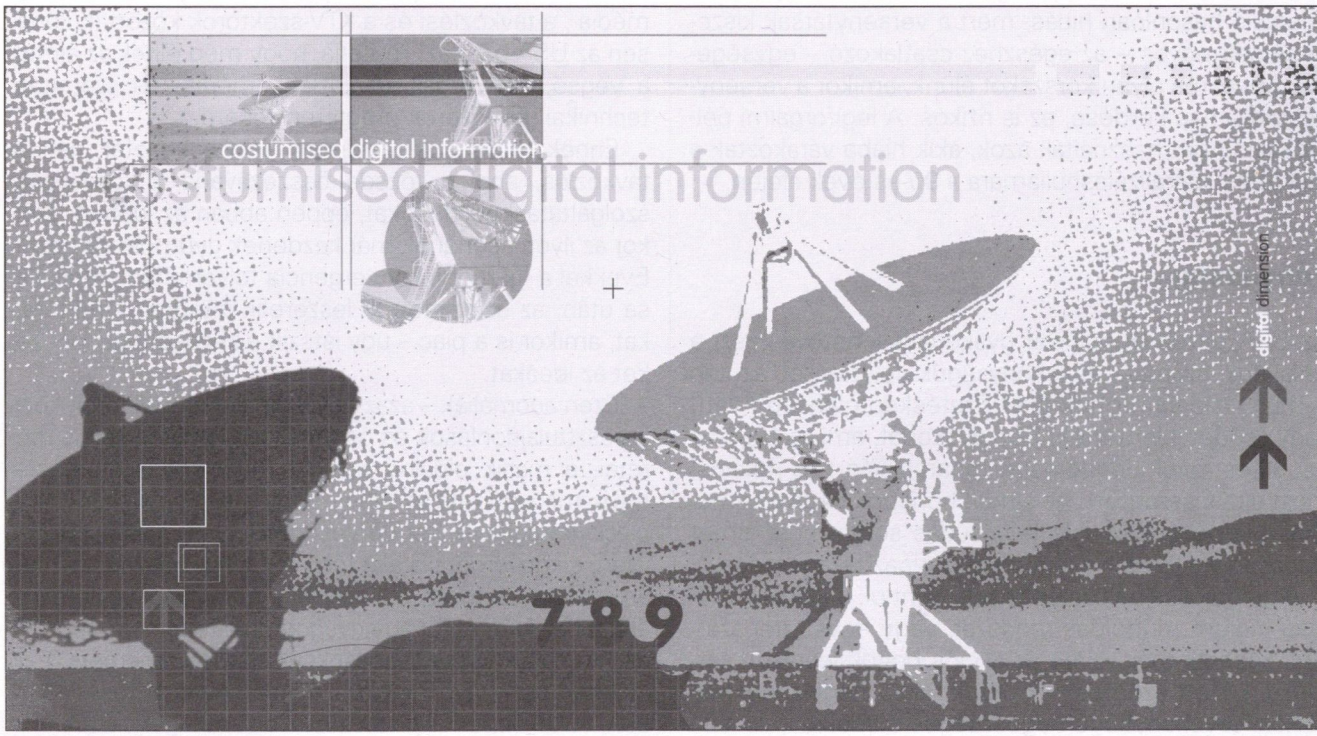
Hír

A Sun és a PricewaterhouseCoopers Consulting kiterjesztik eddigi szövetségüket és átfogó, iparági megoldásokat kívánnak biztosítani. A PwC Consulting üzleti stratégia- és integrációs szolgáltatásait, a Sun nagyvállalati szervereit, szoftvereit egybefogó – Open Net Environment (Sun ONE) architektúráját egyesítő szövetség közös szolgáltatásokat nyújt a Global 2000 vállalatok számára.

A kibővített kapcsolat részeként a PwC Consulting a Sunt választotta UNIX hardverplatformnak új CRM (Costumer Relationship Management – ügyfélkapcsolatok menedzsment) ACCEL kezdeményezéséhez (Architecture for Cross-channel Customer Experience and Loyalty).

A CRM ACCEL megfelelő rendszerbe szervezi az új és hagyományos marketing-, értékesítési és szolgáltatási csatornákat a back-office rendszerekkel. Az ügyfelek hatékony és specifikált ügyfélkapcsolat-kezelési megoldásaik révén csökkenthetik ügyfeleik kiszolgálási költségeit.

A PwC Consulting 3 éve élvonalbeli CRM-szolgáltató. A szervezet legutóbbi pénzügyi évében a 3600 tagú CRM-csoport több mint 1 milliárd dollár bevételt ért el szolgáltatásaival.



Hangkódolási módszerek összehasonlító elemzése

DR. KOVÁCS OSZKÁR

PanTel Rt.

A digitális rendszerek és a jelfeldolgozó processzorok terjedésével az elmúlt időszakban a beszéd-, a kép- és a hangjelek digitalizálása terén látványos fejlődés következett be. Lényegesen lecsökkent valós idejű alkalmazásoknál (pl. távközlés) adott minőségű hanginformáció átviteléhez szükséges sávszélesség, és a nem valós idejű alkalmazásoknál (pl. hangrögzítés) a szükséges tárolási kapacitás.

A kódolási módszerek megvalósítását elősegítette a VLSI félvezető technológia és a digitális jelfeldolgozó processzorok árcsökkenése. Ezek az elemek megjelentek a távközlő végberendezésekben. A gazdaságos átviteli kapacitás terén is rohamos a fejlődés, ennélfogva az alkalmazások köre rohamosabban bővül, mivel a kapacitásigények csökkenése és a lehetőségek bővülése egyidejűleg történik.

Bevezetés

Az audio kódoló-dekódoló feladata a mikrofonból érkező analóg jelek digitális jelfolyammá alakítása, illetve a hálózatból érkező digitális jelfolyam dekódolása a hangszóró felé. Elsősorban a távközlésben, de a hangrögzítésben, a beszédfelismerésben és -szintézisben is fontos eszköz.

Beszédcsatornában alkalmazott kódolási módszerek alapvetően két csoportba sorolhatók:

- *Hullámalak-kódolás*, melynek lényege, hogy az analóg jelalak hullámformáját számjegyes (digitális) módon írja le. A hullámalak kódolási módszerek nemcsak beszédjelek kódolására alkalmasak, hanem minden hangfrekvenciás jelet képesek kódolni, amely az átviteli sávon belüli spektrummal rendelkezik. Ilyenek a távbeszélő-hálózaton adatátvitelre alkalmazott modemek jelei. További figyelmet kíván a telefaxüzenetek továbbítása. A hullámalak-kódolási módszerek nem tömörítenek, és nem képesek kihasználni a beszédszüneteket.
- Léteznek olyan megközelítést használó megoldások, amelyek a hullámalak-kódolásnál kisebb átviteli sebességet igényelnek [1]. A *lineáris predikción alapuló kódolás* lényege, hogy a megelőző minták ismeretében megjósolják (predikció) a jel alakját a következő időszakban. Ezen módszerek sok esetben az *emberi beszéd* jellemzőinek elemzésével érnek el további megtakarításokat. Ennek az a következménye, hogy a nem beszédjelek (modemekből származó jelek) átvitele általában ilyen összeköttetéseken nem lehetséges.

A. H. Reeves 1938. évi szabadalmaira alapozva szabványosították és a digitális távbeszélő-hálózatban ma általánosan alkalmazzák a digitalizálást, ezért csak a lineáris predikciós eljárásokkal foglalkozunk.

Az ADPCM

A PCM-kódolásnál az egyes szomszédos minták egymástól függetlenek, ugyanakkor meglehetősen hasonlók, hiszen ugyanazon jelalak szomszédos szakaszait reprezentálják. Az ADPCM (Adaptive Differential PCM) kódolási módszer azon alapszik, hogy a soron következő minták bizonyos pontossággal előre megjósolhatók. A legegyszerűbb ilyen jóslás, hogy a soron következő minta a szomszédjával azonos lesz. A kódolás lényege, hogy megjósoljuk a következő mintát, és az ettől mért tényleges jel eltérését visszük át kódolt formában. A különbség átviteléhez kevesebb bitre van szükség, mint magára a mintára. A kódolási módszer képes alkalmazkodni a jel karakterisztikus jellemzőihez. Az ADPCM eljárás tehát az analóg jel hullámformájának redundanciáját használja ki. Ez a módszer a lineáris predikció legegyszerűbb formájának tekinthető.

Az ITU-T G.726 ajánlásának [5] megfelelő ADPCM eljárás nem a 8 bites mintavételezett értékeket, hanem az értékek közötti különbséget tárolja 4 biten. A 4 bites minták 15 féle értéket vehetnek fel. Ezek váltása lépésenként történhet, ugrás nincs megengedve. A lépcsők nagysága a jelszinttől is függ. A kódolási eljárás bitsebessége 40, 32, 24 és 16 kbit/s lehet. A leggyakoribb változat 32 kbit/sec sebességet igényel, azaz a G.711 kódolóénak a felét.

A G.722 ajánlás [3] szerinti eljárás SB-ADPCM (Sub-Band ADPCM) módszert alkalmaz, amely egyik változatában 16 kbit/sec sebességre kódol egy beszédcsatornát, másik változatában 7 kHz sávszélességű hangcsatornát kódol 48, 56 vagy 64 kbit/sec sebességre.

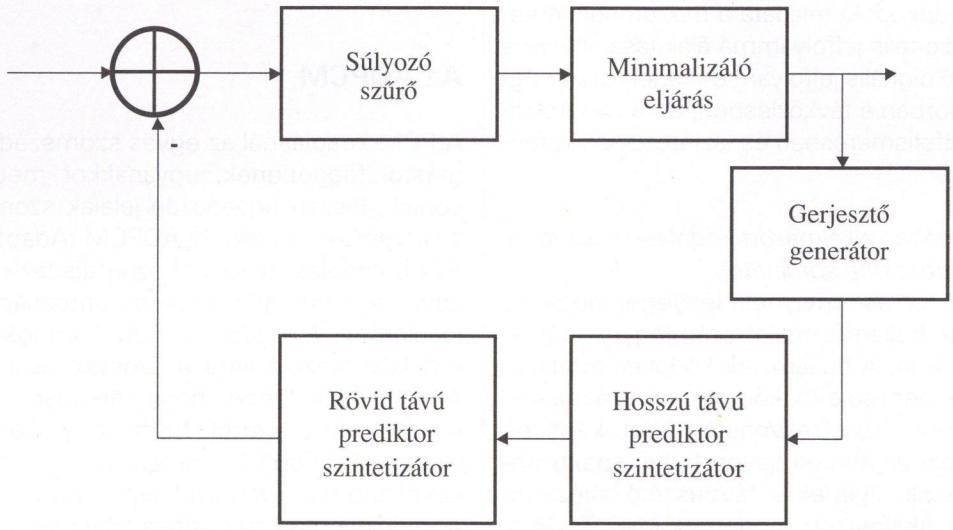
A frekvenciasávot két részre osztják, és ezeken alkalmazzák az ADPCM eljárást. Az alsó sávot (0–4 kHz) 4, 5 vagy 6 bites mintákká kódolják (mivel itt helyezkedik el a beszédteljesítmény jelentős része), attól függően, hogy 48, 56 vagy 64 kbit/sec kimenő sebességgel dolgoznak, a felső (4 kHz feletti) sávot pedig 2 bites mintákká kódolják. Ilyen kódolással a keskeny sávú ISDN-en 7 kHz-es hang-hordozószolgálat működik, amelyet műsorszóráshoz kommentátorhangként is használnak.

Lineáris predikción alapuló kódolási módszerek

A lineáris predikción alapuló módszerek (LPC) az emberi hangképzés mechanizmusának matematikai modellezésével kerültek kidolgozásra. Ha az adott szituációhoz legjobban illeszkedő hangképzési paraméterértékek átvitele után azok segítségével a fogadó oldalon egy beszédszintetizátort működtetünk, akkor az eredeti beszédjelhez közel álló hangot kapunk.

A CELP (Code Excited Linear Prediction) kódgerjesztésű lineáris predikciót alkalmazó eljárás a hangképzés modellezésén kívül kiszámítja az adott a bemeneti beszéd és az elsődleges kódolás közötti várható hibát, és a hiba értékét is átviszi. A hibák kódolt értékei egy *kódkönyv* megfelelő bejegyzésére mutatnak. A CELP eljárás továbbfejlesztett változata az ACELP (Algebraic Code Excited Linear Prediction) eljárás, amely a kódkönyvben történő keresésre ad egy tároló igénybevétele nélküli gyors eljárást (pl. több kódkönyv dinamikus váltása), ezáltal a hatékonyság tovább növelhető.

A gyakorlatban alkalmazott LPAS (Linear Prediction Analysis-by-Synthesis) dekódolási eljárás lényege, hogy a gerjesztő generátor által előállított jel a rövid és a hosszú távú prediktor szintetizátorokon keresztül egy különbségképzőbe kerül, ahol a bejövő beszédjel és a gerjesztett, jósolt jel különbségét képzik. Ha ez a különbség (a különbségi jel négyzetes középértéke) minimális, akkor a predikció jól közelíti a beszédjelet. A rövid és a hosszú távú prediktorok 8–16-od fokú transzverzális szűrők (all-pole IIR: - Infinite Impulse Response - filter), melyek paramétereit állandóan aktualizálják.



A *hosszú távú prediktor* a késleltetés és a jelszint adatait állítja be. Periodikus jelek esetében (pl. magánhangzók) a késleltetés értéke az alapharmonikus periódusideje, vagy annak egész számú többszöröse. A paraméterek aktualizálásának gyakorisága 100–200 aktualizálás/sec.

A *rövid távú prediktor* modellezi a beszédjelben lévő rövid idejű folyamatoknál a korrelációkat, amelyek elsősorban aperiodikus mássalhangzóknál, ajakzörejeknél fontosak. Ez tulajdonképpen egy 8–16-od fokú mindent áteresztő. A paraméterek aktualizálási gyakorisága 300–400 aktualizálás/sec.

A *súlyozó szűrő* működése azon az elven alapszik, hogy az aktuális beszédjel alapharmonikusának (hangmagasság) és a zaj spektrumának egymáshoz képesti elhelyezkedése más-más jel-zaj viszony követelményt határoz meg. Minél jobban különbözik a zaj és a beszédjel spektruma, annál nagyobb jel-zaj viszonyt lehet tartani. Ennek megfelelően kell tehát a súlyozó szűrő paramétereit beállítani.

A módszer továbbfejlesztéseként a prediktorok és a súlyozó szűrő paramétereit egy „kódkönyvből" képezik. Ez a CELP (Code Excited Linear Prediction) vagy ACELP (Algebraic CELP) eljárások megvalósítására alkalmazható digitális jelfeldolgozó processzorokhoz (DSP).

A beszédkódolás legfontosabb területe a távközlés. Az egyes területeken alkalmazott eljárások hasonlók, de a szabványosítás eltérő megoldásokra vezetett. Az egyes eljárások minőségének összehasonlítására a beszédminőségére vonatkozóan szabványosított szubjektív mértékegység, a MOS (Mean Opinion Score) érték szolgál [8], és az ezt jól követő műszer, mely a beszédminták eltérését érzékeli [26].

A fix távbeszélő-hálózatban alkalmazott hangkódolási módszerek

Az ITU ajánlások között a következő kódolók szerepelnek: G.711, G.726, G.728, G.729, G.723.1. Az alábbi táblázat ezen kódolók legfontosabb adatait tartalmazza. Az adatok között szereplő tömörítés által okozott késleltetést és a szükséges utasítások számát Texas Instruments 54x sorozatú 20 MHz-es DSP-re adtuk meg.

Ajánlás	ITU G.711	ITU G.722	ITU G.726	ITU G.728 (3)	ITU G.729	ITU G.729A	ITU G.723.1
Kodek típus	Companded PCM	SB-ADPCM	ADPCM	LD-CELP	CS-ACELP	CS-ACELP	MPC-MLQ & ACELP
Megjelenés éve	1972	1988	1990	1992/4	1995	1996	1995
Sebességigény [kbit/s]	56, 64	56, 64	16-40	16	8	8	6.3 ; 5.3
MOS-érték	4.1	5	3.85	3.61	3.92	3.7	3.9 ; 3.65
Komplexitás (2) MIPS]	0.34	10	14	33	20	10.5	16
RAM	1 byte	1 kbytse	<50 byte	2 kbyte	<2.5 kbyte	2 kbyts	2.2 kbyte
Keretidő [ms]	0.125	1.5	0.125	0.625	10	10	30
Look Ahead	0		0	0	5 ms	5 ms	7.5 ms
Algoritmikus késleltetés (1)	0.25 ms	1	0.25 ms	2.5 ms	25 ms	25 ms	67.5 ms
Sávszélesség [Hz]	300 – 3400	50 – 7000	300 – 3400	300 – 3400	300 – 3400	300 – 3400	300 – 3400

Megjegyzések
(1) A kódolás és a dekódolás idejének összege
(2) A táblázatban a MIPS-értékek fixpontos jelfeldolgozó processzorra vonatkoznak. A bitsebességeknél a kisebb érték a kódoló kimenetén megjelenő sebességet, a nagyobb érték a csatornakódolás utáni értéket mutatja.

A G.729A módszert a az AT&T és még néhány olyan cég támogatja, amelyek a kerettovábbítás (Frame Relay) területén érdekeltek, míg a G.723.1 módszert a Microsoft és az Intel támogatja, mivel a fejlesztésben jelentős szerepet játszottak.

A mobil távbeszélő-hálózatokban alkalmazott hangkódolási módszerek [1]

Ajánlás	ETSI GSM-(FR) GSM 06.10 [11]	ETSI GSM-(HR) GSM 06.20	ETSI GSM-(EFR) GSM 06.60	ETSI TETRA	TIA IS-54	TIA IS-96	RCR PDC (JDC 1)	RCR PDC (JDC 2) Half rate
Kodek típus	RPE-LTP (2)	VSELP	ACELP	ACELP	VSELP	CELP	VSELP	PSI-CELP
Megjelenés éve	1987	1994	1995	1994	1989	1993	1990	1993
Sebességigény [kbit/s]	13	5.6	12.2	4.56	7.95	0,8 - 8.5	6.7	3.45
MOS-érték	3.71	3.85	4.43	3,25	3,25	3,25	3.4/3.6	3.4/3.6
Komplexitás [MIPS]	2.5	17.5	15	15	20	20	20	48
RAM	1	4	9	4	2	2	2	4
Keretidő [ms]	20	20	20	20	20	20	20	40
Look Ahead	0	4.4 ms	0		5 ms	5 ms	5 ms	10 ms
Algoritmikus késleltetés (1)	40 ms	44.4 ms	40 ms		5	5	5	
Sávszélesség [Hz]	300 – 3400	300 – 3400	300 – 3400	300 – 3400	300 – 3400	300 – 3400	300 – 3400	300 – 3400

Megjegyzések
(1) A kódolás és a dekódolás idejének összege
(2) RPE-LTP: Residual Pulse Exitation – Long Term Prediction

A táblázatban szereplő egyes rendszerek rövid leírása:

IS-54 Első generációs TDMA alapú mobilrendszer Észak-Amerikában, amely a VSELP (Vector Sum Excited Linear Prediction) kódolási módszert alkalmazza. Ezt a TIA (Telecommunications Industry Association) dolgozta ki. A szubjektív vizsgálatok eltérést mutattak ki, de a MOS-értékben nem térnek el a többi kódoló jellemzőitől.

IS-96a Első generációs TDMA alapú mobilrendszer Észak-Amerikában, amely a QCELP (Qualcomm Code-Excited Linear Prediction) kódolási rendszert alkalmazza. A kódoló jellemzője, hogy a beszédszünetekben a bitsebesség kb. 0,8 kbit/s-re csökken.

IS-127 Második generációs CDMA alapú mobilrendszer Észak-Amerikában, amely az RCELP (Residual Code-Excited Linear Prediction) módszert alkalmazza.

IS-641 Második generációs cellás TDMA rendszer Észak-Amerikában, amely az ACELP eljárást alkalmazza. Ez a kódoló a G.729 kódoló versenytársának tekinthető, azzal lényegében egyenértékű. Először az IS-136 digitális TDMA rendszerhez használták.

GSM-FR Első generációs digitális európai cellás mobilrendszer (GSM), amely az RPE-LTP (Regular Pulse Excitation Long Term Prediction) módszert alkalmazza. [11].

GSM-HR A GSM számára kifejlesztett félsebességű kódoló változat, amely VSELP (Vector Sum Excited Linear Prediction) módszert alkalmaz. Eredetileg a Motorola fejlesztette ki a GSM rendszer kapacitásának növelése céljából. Ennél a bitsorozatban több bit szolgál a hibavédelemre, mint az előző verzióban. Az eredményül kapott jellemzők lényegében megegyeznek a RPE-LTP eljárásával. Ez a kódoló előfordul 7 kHz-es változatban, 5 kHz mintavételi frekvenciával.

GSM-EFR Második generációs európai cellás mobilrendszerek (GSM) számára kifejlesztett ACELP elárását alkalmazó eljárás. A NOKIA és a kanadai Sherbrooke Egyetem közös fejlesztése. Magyarországon 1999. március óta vezették be a GSM hálózatokban.

PDC Az első generációs japán mobilrendszer (PDC) számára kifejlesztett kódoló, amely a JVSELP (Japanese version of Vector Sum Excited Linear Prediction) eljárást alkalmazza. Ez az eljárás az RCR (Research and Development Center for Radio Systems) fejlesztésének eredménye és az STD-27B szabvány specifikálja. A korábbiakhoz képest a módszer újdonsága, hogy a két vektor összegét tartalmazó gerjesztő kódkönyv helyett ebben az esetben csak egy vektor van.

A GSM kódolók a fix hálózatban alkalmazott G.728 kódolóval (CELP) hasonlíthatók össze. Kivitelük egyszerűsége lehetővé teszi, hogy nem szükségszerű DSP alkalmazása.

Műholdas beszéd-összeköttetéseken alkalmazott kódolási módszerek

Mivel a műholdas csatornák kapacitása korlátos, a kis sebességű beszédkódolás igen nagy jelentőségű. Ezen csatornákon a hibaarány és a fading gyakori probléma, ami robusztus eljárások alkalmazását igényli.

Az alábbi táblázat a műholdas mobilrendszerekben használatos eljárások jellemzőit mutatja.

Ajánlás	AEEC (4)	Inmarsat (3)
	AMTS (2)	M
Kodek típus	Multipulse LPC	IMBE (5)
Megjelenés éve	1988	1990
Sebességigény [kbit/s]	9.6/19.2	4.15/6.4
Minőség	<GSM	<GSM
MOS-érték	n.a.	n.a.
Komplexitás [MIPS]	n.a.	n.a.
RAM	2	2
Keretidő [ms]	20	20
Look Ahead	n.a.	n.a.
Algoritmikus késleltetés (1)	n.a.	n.a.
Sávszélesség [Hz]	300–3400	300–3400

Megjegyzések
(1) A kódolás és a dekódolás idejének összege
(2) AMTS: Airborne Mobile Telephone Service
(3) INMARSAT: International Maritime Satellite Corporation
(4) AEEC: Airlines Electronics Engineering Committee
(5) IMBE: Imposed Multi-Band Excitation

Az AMTS rendszert a nagy légitársaságok műholdas távbeszélőrendszereinél használják. Az Inmarsat M rendszer IMBE eljárása a szinuszos összetevőkre és mellékinformációkra bontja a beszédjelet, és ezeket külön-külön kódolja. Ezt az eljárást más amerikai mobilrendszerekhez (segélykérés, rendőrség) is használják.

A fent ismertetett eljárásokon kívül katonai rendszerek is léteznek, amelyek sebessége akár 2.4 kbit/s-re is lecsökkenhet. Ennek ára, hogy a beszédminőség tovább romlik, és egyes eljárásoknál a beszélő személye sem azonosítható hang alapján.

Ahhoz, hogy a fenti táblázatokban ismertetett egyes kódolási eljárások összehasonlíthatók legyenek, érté-

kelésükre egységes módszerek alakultak ki. Ezek a következő paraméterek számszerűsítését jelentik:

- *Bitsebesség,* amely megadja, hogy valós idejű esetben a folyamatos működésnél a kódoló kimenetén mekkora sebességű bitfolyam keletkezik. Egyes eljárások nem igényelnek állandó bitsebességeket, a beszédszüneteket kihasználják. A csendes periódusokban a kódoló kimenetén nem jelenik meg digitális jel. A bitsebesség tehát sok esetben nem egy időfüggetlen abszolút számmal jellemezhető érték, hanem statisztikai jellemzők is hozzárendelhetők.
- *Késleltetés* a valós idejű rendszerek fontos jellemzője, mivel adott késleltetés felett csak egyirányú kommunikáció (pl. műsorszórás) lehetséges, párbeszéd nem. A rendszer eredő késleltetése a következőkből tevődik össze:
  - keretkésleltetés: a kódoló és a dekódoló a beszéd valamely szakaszának ismeretében határozza meg a kimeneti függvényt (blokk-kódolás), amelyhez az adott sebességet figyelembe véve a teljes szakasz beérkezését meg kell várni;
  - beszédfeldolgozási késleltetés, a műveleti bonyolultság és a processzor sebessége által meghatározott érték. Ez az érték a processzor típusának megválasztásával befolyásolható;
  - átviteli késleltetés (multiplexálási késleltetés, csomagkapcsoló hálózat késleltetése, konferenciahíd ideje – bridging delay stb.).
- *Algoritmus bonyolultsága,* amely a kódoláshoz és a dekódoláshoz szükséges matematikai eljárások műveleteinek mennyiségét adja meg, miáltal meghatározható a szükséges processzorteljesítmény és operatív tároló (RAM) mérete. Ebből következtetni lehet a szükséges energiaigényre is, ami hordozható rendszerek esetében fontos szempont lehet.
- *Beszédérthetőség, minőség,* amely a kódolási és az ezt követő dekódolási műveletből álló rendszer két végpontja közötti minőségi jellemzőket adja meg.

A fenti jellemzők alapján ki lehet választani az adott célra legmegfelelőbb eljárást, ha ismerjük pl. a rendelkezésre álló távközlési csatorna kapacitását vagy a költségkorlátokat (az algoritmus bonyolultsága utalhat erre).

Egyéb hangkódolási módszerek

Mint az előzőkben látható volt, a távközlésben elsősorban a beszédkódolásra optimalizált rendszerek fejlődnek. A hangrögzítés és -visszaadás azonban a beszéden kívül egyéb hangjelek (főként zene) kódolásával foglalkoznak.

Hangrögzítésnél, műsorelosztásnál alkalmazott kódolási eljárásoknál további megtakarítást érnek el azáltal, hogy az emberek nagy része a legmagasabb (18-20 kHz-es) hangokat nem hallja, így azok levághatók. A mély hangokat pedig elegendő mono rendszerben átvinni. Ez a *Joint stereo-IS.* A kisebb szintek esetén a kódolás módja kisebb bitsebességet igényel (Dual Channel), sőt a hallásküszöb alatti szintek nem kerülnek kódolásra. Az MP3 által is alkalmazott hangtömörítésnél egyes esetekben nem kell mind a két sztereocsatornát tárolni, elég csak az egyikhez vagy a másikhoz tartozó különbséggel foglalkozni. Ez a *joint stereo-MS* rendszerű átvitel.

Eljárás (szabvány)		**Mintavételi sebesség** [kHz]	**Működés**	**Sebesség (csatornánként)** [kbit/sec]	**Alkalmazási jellemzők**
MPEG 1 (ISO 11172-3)	Layer I	44.1	16 bites PCM	32 – 448 (tipikusan 128)	CD
	Layer II	32 ; 44.1, 48		32 – 384 32, 48, 56, 64, 80, 96, 112, 128, 160 vagy 192	mono, joint stereo Joint Stereo 4, 8, 12, 16 csat
	Layer III (MP3)	11, 44.1	max.16 kHz	Tipikusan 128	mono, joint stereo-MS (magas hangok) joint stereo-IS (mély hangok: mono)
	(MP3 Pro)			64	
MPEG 2 - 3 (ISO 13818)	Layer I			10 000	HDTV, DVD
	Layer II	16, 22.05, 32, 44.1, 48		8, 16, 24, 32, 40, 48, 56, 64 vagy 80	mono, joint stereo Joint Stereo 4, 8, 12, 16 csat.
	Layer III:				
MPEG 3				Kis sebességű kódolás	Multimédia-tartalom leírása
MPEG 4					Multimédia audiovizuális keresés
LBR Audio		8		8, 9, 10, 11, 12, 13, 14, 15 vagy 16	mono

A kódolási eljárások után az eredményül kapott bitfolyamok az átviendő információmennyiség csökkentése érdekében még külön tömöríthetők. Egyes eljárások azonban valós idejű alkalmazásoknál nem használhatók, mivel a tömörítéshez először az egész hang- és képanyag ismerete szükséges. A kibontásnál esetleg több forrást is egyidejűleg kell használni. [12] A Huffman-eljárások lényege, hogy a bitfolyamban az ismétlődő részeket valamilyen rövidebb sorozattal helyettesítik.

- LZ77 (Lempel-Ziv): olyan tömörítő eljárás, amelynél az egész állományt elemzik, és az előfordulási gyakoriság függvényében egy fa struktúrában helyezik el oly módon, hogy a leggyakoribb bitkombinációk a kiindulási ponthoz legközelebb helyezkedjenek el, miáltal a hozzájuk tartozó kód a legrövidebb. A tömörített jelsorozat mellé ezt a fát mellékelve kapjuk a végeredményt. Az eljárást megfordítva kapjuk vissza az eredeti jelet.
- LZ78: a karaktersorozatban az ismétlődő sorozatrészeket (pl. gyakori szavak) rövidebb kódokkal (pl. egy karakter) helyettesítik. Ehhez a kódtáblázatban külön lapot használnak (szótár). A kódlapok közötti mozgás a szokásos módon történik. A tömörített állomány kicsomagolásához szükség van a szótár meglétére is, melyet a fájlhoz csatolnak.

Összefoglalás

A hangkódolás fejlődése számos szerteágazó eredményt hozott. Ezen elméleti és gyakorlati eredmények azonban akkor használhatók ki hatékonyan, ha az egyes rendszerek közötti együttműködés kérdései tisztázottak. Egyre növekszik annak a jelentősége, hogy egy adott távközlőhálózaton nem két humán beszélő, hanem pl. egy humán használó és egy szerver kerül kapcsolatba, és a hangrögzítési, vagy -átviteli rendszerek között közvetlen kapcsolat létesül. A DAVIC (Digital Audio Visual Council) keretében folyó szabványosítási tevékenység az MPEG specifikációk kidolgozásával jelentős eredményeket ért el. Meghatározó az ITV-t 12 TB, és ezen belül a Speech Quality Expert Group (SQEG) munkája eredményezett sikeres beszédkompressziós eljárásokat. Ezek gyakorlati megvalósítása lehetőséget adhat a fenti célkitűzések megvalósítására.

Irodalom

1. R. V. Cox. „Current Methods of Speech Coding." International Journal of High Speed Electronics & Systems, Vol 8, No 1 (1997) pp 13-68.
2. G.711 - Pulse code modulation (PCM) of voice frequencies 1988
3. G.722 - 7 kHz audio-coding within 64 kbit/s 1988
4. G.723.1 - Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s 1996.
5. G.726 - 40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM) 1990
6. G.728 - Coding of speech at 16 kbit/s using low-delay code excited linear prediction 1992
7. G.729 - Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear-prediction 1996
8. P.800 - Methods for objective and subjective assessment of quality 1996
9. Rosta, G.: „Tömörítés I" Computer Technika, 2000. okt. 17.
10. Dusa, G.: „Tömörítés a gyakorlatban II" Computer Technika, 2000. okt. 24.
11. ETS 300 036 szabvány.
    European Telecommunications Standard Institute
12. Jarkko Ahonen & Arttu Laine: „Realtime speech and voice transmission on the Internet"
    Helsinki University of Technology - Telecommunications Software and Multimedia Laboratory April, 1997 Jarkko.Ahonen@iki.fi & Arttu.Laine@eunet.fi
13. Richard V. Cox & Peter Kroon. Low Bit-Rate Speech Coders for Multimedia Communication, IEEE Communications Magazine, 12(34):34-41, December 1996
14. Federal Standard 1016, Telecommunications: Analog to Digital conversion of Radio Voice by 4800 bps Code Excited Linear Prediction (CELP)
15. http://cips02.physik.uni-bonn.de/~scheller/audio/ Comparison of audio compression techniques.
16. http://fas.sfu.ca/cs/undergrad/CourseMaterials/CMPT365/material/notes/Chap4/Chap4.3/Chap4.3.html Audio compression techniques and human audio perception
17. Procedures for real-time Group 3 facsimile communication over IP networks
    ITU-T Recommendation T.38
18. Procedures for the transfer of facsimile data via store-and-forward on the Internet
    ITU-T Recommendation T.37
20. General Characteristics Of International Telephone Connections And International Telephone Circuits - Echo Cancellers
    ITU-T Recommendation G.165
21. ETS 300 149 (Audio)
22. T.J. Kostas et alii, Real-Time Voice over Packet Switched Networks, IEEE Network, Jan-Feb 1998.
23. Echo Cancellers
    ITU-T Recommendation G.165 ITU Geneva 1993
24. Digital cellular telecommunications system (Phase 2+);
    Full rate speech; Transcoding
    GSM 06.10 version 8.1.0 Release 1999
    European Telecommunications Institute
25. Hersent–O., Gurle–D., Petit–J-P.: „IP Telephony. Packet-based multimedia communications systems"
    Addinson-Wesley 2000, ISBN 0-201-61910-5
26. Brebovszky, J.: A csomagkapcsolt beszédátvitel minősítése, Híradástechnika, Vol LYI, 2001. április 19–22.
27. H. Fletcher: Speeck and Hearing in Communication. D. Van Nostrand. New York, 1953.

A statisztikus sávszélesség általánosítása csomagkapcsolt hálózatokban

LEVENDOVSZKY JÁNOS–DÁVID TAMÁS–VESZTERGOMBI GYÖRGY

Budapesti Műszaki és Gazdaságtudományi Egyetem (BME)
Híradástechnikai Tanszék

L

A cikk a Chernoff-egyenlőtlenségen alapuló statisztikai sávszélesség lehetséges kiterjesztéseit adja meg, amelyek segítségével a hálózatok kihasználtsága növelhető. Ezen új sávszélességek alapján csomagkapcsolt hálózatok forgalmi dimenzionálása, illetve hívásengedélyezése valós idejű algoritmusokkal lehetővé válik. Az eredményeket az elméleti bizonyítás mellett szimulációk is alátámasztják.
Kulcsszavak: hívásengedélyezés, csomagkapcsolt hálózatok, Chernoff-egyenlőtlenség, nagy eltérések elmélete.

Bevezetés

Napjaink egyik alapvető kommunikációs technológiája a csomagkapcsolás, amellyel az áramkörkapcsolásnál nagyobb kihasználtság érhető el [1, 2]. Ezért a gerinchálózati protokollok IP alapúak, amelyhez az előfizetői hozzáférés pl. ATM „gyűjtőhálózatokon" keresztül valósulhat meg [3, 4, 5]. Ráadásul a felhasználók az ADSL technika előretörése miatt korrelált „felfelé" és „lefelé irányú" forgalmakat generálnak, amelyek menedzsmentje, valamint az optimális kihasználtság garantálása nagy kihívásokat jelent a hálózat üzemeltetője számára. Természetesen ezeket a problémákat adott szolgáltatási színvonal (Quality of Service = QoS) biztosítása mellett kell megoldani.

Ezért a csomagkapcsolt technikák körében alapvető szerepet kap a gyors, valós idejű hívásengedélyezési és dimenzionálási algoritmusok fejlesztése, amelyek segítségével biztosítható, hogy a rendelkezésre álló erőforrásigények megfeleljenek a minőségi kommunikáció követelményeinek.

A hívásengedélyezés és dimenzionálási feladatok egyik központi koncepciója a statisztikus sávszélesség fogalma, amely lehetővé teszi a QoS-követelmények gyors ellenőrzését és ez alapján a hálózatba beengedhető forgalmi volumennek (a felhasználók összegzett forgalmának) az optimalizálását. A statisztikus sávszélesség fogalmát – a Chernoff-egyenlőtlenség alapján – először Kelly vezette be [8], majd elterjedten használttá vált a csomagkapcsolt hálózatok forgalmi tervezésében [2, 6, 10, 11, 12]. A Chernoff-egyenlőtlenség a logaritmikus momentumgeneráló függvények használatára épül, amely független forgalmak esetén additív tulajdonságot mutat. Az eredeti koncepció gyenge pontja, hogy a logaritmikus momentumgeneráló függvény adott értékének a megtalálása külön számításokat igényelt minden egyes forgalmi konfiguráció esetén. Ugyanakkor csak egy uniform értékkel számolva a számítási algoritmus valóban egyszerűbb, de a hálózat kihasználtsága sokat csökkenhet.

A fenti problémák leküzdése érdekében a cikk új sávszélesség-fogalmakat vezet be és a hívásengedélyezési algoritmusoknak ezekkel elért teljesítőképességét vizsgálja. Ezen új sávszélességek a következők:

- forgalmi volumen alapján optimalizált sávszélesség;
- vektoriális sávszélesség (egy adott típusú forgalmi folyamhoz egy sávszélesség vektor tartozik);
- korrelált bidirekcionális forgalmi folyamokra vonatkozó statisztikus sávszélesség.

A továbbiakban elméleti bizonyítások, illetve numerikus eredmények is bizonyítják, hogy az új sávszélességek nagyban képesek növelni a hálózat kihasználtságát a minőségi kommunikáció kritériumainak a betartása mellett.

A statisztikus sávszélesség fogalma – modell és jelölések

A következőkben bevezetjük a probléma megfogalmazásához szükséges modellt és jelöléseket. Tételezzük fel, hogy

- Zéró buffer approximációt használunk, azaz a sorban állási késleltetéstől eltekintünk;
- a felhasználói osztályok száma $i = 1,...M$ (pl. hang, video, adat ... stb.);
- $\mathbf{X}m_j^{(i)}$ az i-dik osztály j-dik forrását jelöli;
- minden egyes osztályban a felhasználók On/Off forrással jellemezhetők. Azaz egy adott forrás két állapottal rendelkezik, vagy h_i sebességgel ad, vagy „hallgat". Az átlagos adási sebesség m_i. Ezen két

paraméter segítségével a forgalom eloszlása a következőképpen írható le:

$$P(X_i=0)=1-\frac{m_i}{h_i} \quad P(X_i=h_i)=\frac{m_i}{h_i}, \tag{1}$$

ahol X_i az adott i-dik osztálybeli felhasználó véletlen forgalmát jelöli kBit/sec-ban;

- n_i jelöli az i-dik osztálybeli felhasználók számát;
- $\mathbf{n} = (n_1, n_2, \ldots n_M)$ forgalmiállapot-vektor írja le a rendszer teljes állapotát, amely megadja a felhasználók számát az egyes forgalmi osztályok szerint;
- a csomópont kapacitása C;
- γ jelöli a cellavesztésre vonatkozó QoS-paramétert, aminek teljesülnie kell a C kapacitású linken.

A QoS biztosítása érdekében a következő egyenlőtlenségnek kell teljesülnie:

$$P\left(\sum_{i=1}^{M}\sum_{j=1}^{n_i} X_j^{(i)} > C\right) < e^{-\gamma}, \tag{2}$$

ahol $\sum_{i=1}^{M}\sum_{j=1}^{n_i} X_j^{(i)}$ jelöli az aggregált véletlen forgalmat és $\sum_{i=1}^{M}\sum_{j=1}^{n_i} X_j^{(i)} > C$ pedig a cellavesztés eseményét.

Csomagkapcsolt hálózatokban a QoS-kommunikáció a fenti egyenlőtlenséget két aspektusból vizsgálja:

1. Dimenzionálás

Ilyenkor adott forgalmi osztályok, $\mathbf{n}$ vektor és γQoS-paraméter esetén meg kell találni azt a legkisebb C értéket, amelyre a fenti egyenlőtlenség teljesül. Azaz a dimenzionálás a következő optimalizálási feladat megoldását jelenti.

$$C_{opt} : \min_C P\left(\sum_{i=1}^{M}\sum_{j=1}^{n_i} X_j^{(i)} > C\right) < e^{-\gamma} \tag{3}$$

2. Hívásengedélyezés

Ekkor adott γ és C esetén meg kell adnunk azon $\mathbf{n}$ vektorok halmazát, amelyre az (2) egyenlőtlenség teljesül úgy, hogy a beengedett forgalmi volumen maximális legyen, azaz

$$Vol_{opt} = \max_{\theta} \#\{\mathbf{n}: \mathrm{CAC}(\mathbf{n},\theta) = \mathrm{elfogad}\}, \tag{4}$$

ahol $CAC(\mathbf{n},\theta)$ egy a hívásengedélyezést végző általános algoritmust jelöl, amely vagy elfogadja, vagy elveti az adott forgalmiállapot-vektort, θ pedig a rendszer szabad paramétereinek a halmaza.

A fenti feladatok azért jelentek meg optimalizációs feladat gyanánt, mert az aggregált forgalom farokeloszlása $P\left(\sum_{i=1}^{M}\sum_{j=1}^{n_i} X_j^{(i)} > C\right)$ analitikusan nem számolható, ezért megfelelő közelítésekre van szükség. A következőkben a hívásengedélyezésre összpontosítunk.

A farokeloszlás becslésére az egyik legszélesebb körben elterjedt módszer a Chernoff-egyenlőtlenség:

$$P(Y > C) \le e^{\mu_Y(s)-sC} \tag{5}$$

ahol $\mu_Y(s) = \log E\left(e^{sY}\right)$ a logaritmikus momentumgeneráló függvénye az Y valószínűségi változónak (mely esetünkben a felhasználók aggregált sávszélességigényét jelöli), míg s egy tetszőleges pozitív érték. A fenti egyenlőtlenség akkor a legélesebb, ha az egyenlőtlenség jobb oldala minimális, vagyis

$$s_{opt} : \inf_s \mu_Y(s) - sC. \tag{6}$$

A jelenlegi esetben az aggregált forgalom $Y = \sum_{i=1}^{M}\sum_{j=1}^{n_i} X_j$, ami a források függetlensége miatt azt eredményezi, hogy

$$\mu_y(s) = \sum_{i=1}^{N} n_i \mu_i(s), \tag{7}$$

ahol

$$\mu_i(s) = \log\left(1-\frac{m_i}{h_i}+\frac{m_i}{h_i}e^{sh_i}\right). \tag{8}$$

Így a QoS-kommunikációra érvényes Chernoff-egyenlőtlenség a következőképpen alakul:

$$P\left(\sum_{i=1}^{M}\sum_{j=1}^{n_i} X_j > C\right) \le e^{\sum_{i=1}^{M} n_i\mu_i(s_{opt})-s_{opt}C}, \tag{9}$$

ahol

$$s_{opt} : \inf_s \sum_{i=1}^{M} n_i \mu_i(s) - sC \tag{10}$$

Ennek alapján a QoS-teljesítése a következő formulák alapján ellenőrizhető:

$$P\left(\sum_{i=1}^{M}\sum_{j=1}^{n_i} X_j > C\right) \le e^{\sum_{i=1}^{M} n_i\mu_i(s_{opt})-s_{opt}C} < e^{-\gamma} \tag{11}$$

$$\sum_{i=1}^{M} n_i \mu_i(s_{opt}) < s_{opt}C - \gamma. \tag{12}$$

A fenti eredmény fontossága abban rejlik, hogy viszonylag egyszerű formában adott a QoS-paraméter és a források által nyújtott statisztikai terhelés közti viszony. Ennek megfelelően az $\frac{1}{s}\mu_i(s)$ mennyiséget az i-dik osztály statisztikus sávszélességének is szokták nevezni [8].

Így a klasszikus Chernoff-határ alapján történő dimenzionálás a következő algoritmus alapján történhet:

Adott: γ, és $\mathbf{n}$

1. Válassza a kiindulási kapacitásértéket $C_0 = \sum_{i=1}^{M} n_i m_i$.
2. Határozza meg az $s_{opt} : \inf_s \sum_{i=1}^{M} n_i \mu_i(s) - sC_0$ értéket.
3. Ellenőrizze, hogy $\sum_{i=1}^{M} n_i \mu_i(s_{opt}) < s_{opt} C - \gamma$, teljesül-e.
4. Ha nem, akkor növelje a kapacitás értékét $C_{k+i} = C_k + \Delta$; visszalépés a 3-as pontra.
5. Ha igen, akkor a dimenzionálást megoldottuk C_{opt} megtalálásával.

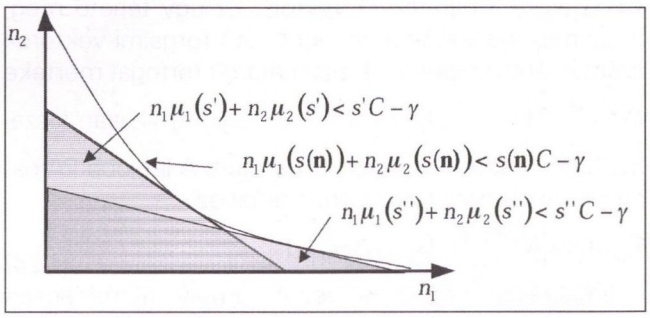
Hívásengedélyezés esetén a következő algoritmus alapján járhatunk el:

1. Adott egy $\mathbf{n} = (n_1,...n_m)$ forgalmiállapot-vektor.
2. Határozzuk meg az egyes forgalmi osztályok $\mu_m(s)$ logaritmikus momentumgeneráló függvényét *(i = 1,...M)*
3. Határozzuk meg az $s_{opt} : \inf_s \sum_{i=1}^{M} n_i \mu_i(s) - sC$ optimális értéket.
4. $\sum_{i=1}^{M} n_i \mu_i(s_{opt}) < s_{opt} C - \gamma$ egyenlőtlenség teljesülése alapján döntsük el, hogy az adott forgalmiállapot-vektor elfogadható-e.

A farokeloszlás becslése új, optimalizált Chernoff-egyenlőtlenségek alapján

Látható, hogy az s paraméter újraoptimalizálása mindkét esetben probléma, hiszen akár a dimenzionálás, akár a hívásengedélyezés esetén (különböző C értékeknél, illetve $\mathbf{n}$ vektoroknál) ez a paraméter újraoptimalizálandó. Ezért felvetődik a kérdés, hogyan lehet a Chernoff-egyenlőtlenséget egyetlenegy univerzális paraméterrel használni, amely nem csökkenti jelentősen a hívásengedélyezés során beengedhető forgalmi volument, ugyanakkor a számításigényt jelentősen redukálja. Ezzel megnyílik az út a valós idejű hívásengedélyezés felé.

Az optimalizálás alapja a következő: fix s esetén a $\sum_{i=1}^{M} n_i \mu_i(s) - sC$ egyenlet egy hipersíkot határoz meg.



1. ábra: Szeparáló felület és a beengedhető forgalmi volumen alakulása különböző s paraméterértékek esetén, két forgalmi osztályt feltételezve.

A beengedhető forgalmi volumen az M dimenziós állapottérben pontosan ezen hipersík és a tengelyek által határolt M dimenziós térrész térfogata:

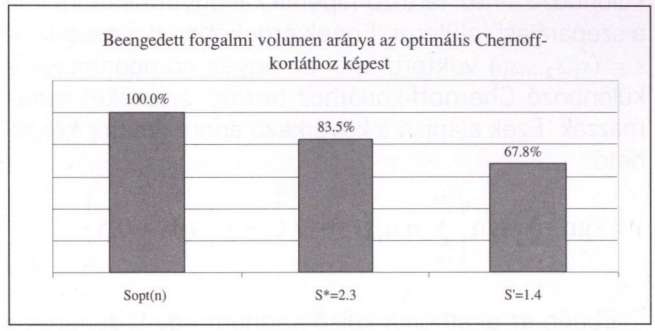
$$\frac{(sC-\gamma)^M}{M!\prod_{i=1}^{M}\mu_i(s)} \tag{13}$$

Ezért azt az s-et kell kiválasztani, amely az ábrán szürkével jelölt térrész térfogatát maximalizálja, tehát a szerzők által javasolt új statisztikus sávszélesség

$$\frac{1}{s^*}\mu_i(s^*),$$

ahol

$$s^* : \max_s \frac{(sC-\gamma)^M}{M!\prod_{i=1}^{M}\mu_i(s)}. \tag{14}$$



2. ábra: A beengedhető forgalmi volumen alakulása különböző s paraméterértékek esetén.

Bár s^* az $s_{opt}(\mathbf{n})$ alapján definiált sávszélességhez képest megközelítőleg 15%-os veszteséget eredményez, előnye viszont a sokkal kisebb számítási komplexitás és a hívásengedélyezés valós idejű implementációja.

A statisztikus sávszélesség további kiterjesztése a hálózatkihasználtság növelése érdekében

Ebben a fejezetben továbbfejlesztjük a statisztikus sávszélesség fogalmát úgy, hogy minden forgalmi osztályhoz egy „sávszélesség vektort" rendelünk hozzá. A sávszélesség vektor bevezetését az indokolja, hogy nemcsak egy, hanem több paraméterrel fogunk dolgozni.

Emlékeztetőül álljon itt a Chernoff-egyenlőtlenség következő formája:

$$P\left(\sum_{i=1}^{M}\sum_{j=1}^{n_i} X_j^{(i)} > C\right) \le e^{\sum_{i=1}^{M} n_i\mu_i(s(\mathbf{n})) - s(\mathbf{n})C}, \tag{15}$$

ahol

$$s(\mathbf{n}) : \sum_{i=1}^{M} n_i \frac{d\mu_i(s(\mathbf{n}))}{ds} = C. \tag{16}$$

A beengedhető forgalmi volument a következő halmazszeparálás adja meg:

$$N^{s_{\text{var}}-elfogad} := \left\{ \mathrm{n} : \sum_{i=1}^{M} n_i \mu_i(s(\mathrm{n})) - s(\mathrm{n}) C + \gamma < 0 \right\}, \tag{17}$$

és

$$N^{s_{\text{var}}-elvet} := \left\{ \mathrm{n} : \sum_{i=1}^{M} n_i \mu_i(s(\mathrm{n})) - s(\mathrm{n}) C + \gamma \geq 0 \right\}. \tag{18}$$

halmazokkal jelöljük. A „var" index arra utal, hogy a formulában használt s paraméter minden forgalmi helyzetben más és más, függvénye az n forgalmiállapot-vektornak. A keletkező felületet az 1. ábra érzékelteti két forgalmi osztály esetén.

Mivel a szeparálási felület $s(\mathrm{n})$ esetén görbült, ezért nem biztos, hogy hatékonyan közelíthető egy darab hipersíkkal. Az illeszkedés pontossága javítható, ha több különböző s-hez tartozó hipersíkkal együttesen írjuk le a szeparálási felületet. Ennek érdekében bevezetjük az $\mathrm{s} = (s_1, s_2, \ldots s_V)$ vektort, ahol az egyes komponensek a különböző Chernoff-korláthoz tartozó értékeket tartalmazzák. Ezek alapján a következő approximátor készíthető:

$$y = \operatorname{sgn}\left\{ \sum_{v=1}^{V} \operatorname{sgn}\left(\sum_{i=1}^{M} n_i \mu_i(s_v) - s_v C + \gamma \right) + V - 0.5 \right\} \tag{19}$$

Ebben az esetben a külső szignum egy V dimenziós vagy kapcsolatot valósít meg, a belső pedig elvégzi a halmazszeparálást különböző hipersíkok segítségével, amelyeket az s paraméterek és a forgalmat leíró véletlen változók logaritmikus momentumgeneráló függvénye határoz meg. Ezáltal az egyes Chernoff-korlátok által meghatározott elfogadási tartományok unióját nyerjük, mint az a 3. ábrán megfigyelhető. Ezt az approximátort poligoniális approximátornak (PA) nevezzük.

A PA által végzett halmazszeparálást a következő halmazokkal jelöljük:

$$N^{PA-elfogad}(s_1, \ldots, s_V) :=$$

$$= \left\{ \mathrm{n} : \operatorname{sgn}\left(\sum_{v=1}^{V} \operatorname{sgn}\left(\sum_{i=1}^{M} n_i \mu_i(s_v) - s_v C + \gamma \right) + V - 0.5 \right) = 1 \right\}$$

$$N^{PA-elvet}(s_1, \ldots, s_V) :=$$

$$= \left\{ \mathrm{n} : \operatorname{sgn}\left(\sum_{v=1}^{V} \operatorname{sgn}\left(\sum_{i=1}^{M} n_i \mu_i(s_v) - s_v C + \gamma \right) + V - 0.5 \right) = 1 \right\}$$

A zárójelben lévő $(s_1, s_2, \ldots s_V)$ vektor utal arra, hogy a közelítés függ az s paraméterek megválasztásától. Mivel minden $s>0$ esetén a Chernoff-korlát konzervatív becslést ad, ezért a PA eljárás is konzervatív, azaz

$$N^{PA-elfogad}(s_1, \ldots, s_V) \subseteq N^{elfogad} \quad \forall s_i > 0,\ i = 0, \ldots, V. \tag{20}$$

Így nem következhet be szerződésszegés PA használatával. Továbbá PA felfogható a $\sum_{i=1}^{M} n_i \nu_i s(\mathrm{n}) = s(\mathrm{n}) - \gamma$ szeparáló felület közelítéseként $(s_1, s_2, \ldots s_V)$ paraméterekkel. Mivel egy kétrétegű neurális háló matematikai leírása

$$y = \varphi\left\{ \sum_{v=1}^{V} w_v^{(2)} \varphi\left\{ \sum_{i=1}^{M} w_{vi}^{(1)} n_i - w_{v0}^{(1)} \right\} - w_0^{(2)} \right\}, \tag{21}$$

ezért PA implementálható ezzel a struktúrával. A paramétereket a következő módon kell beállítani:

$$w_v^{(2)} = 1, \quad v = 1, \ldots, V$$
$$w_0^{(2)} = -V + 0.5$$
$$w_{vi}^{(1)} = \mu_i(s_v), \quad i = 1, \ldots, M \quad v = 1, \ldots, V$$
$$w_{v0}^{(1)} = s_v C - \gamma$$

Említésre méltó, hogy a paraméterek analitikusan felírhatók, ezért nincs szükség hosszadalmas tanítási fázisra a neurális hálózatnál a súlyok beállításához.

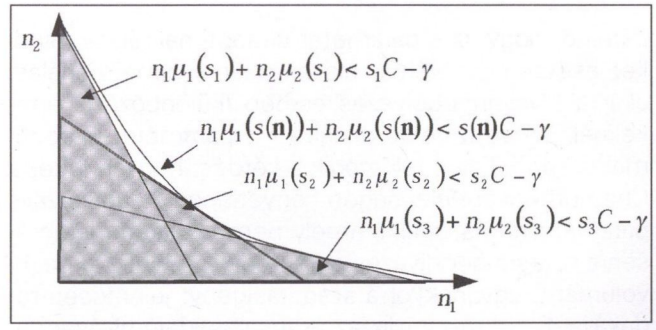
Lévén, hogy V darab Chernoff-korlát uniójaként hoztuk létre a PA algoritmust, ezért hatékonyabb bármely egyszerű egy hipersíkos Chernoff-korlátnál, vagyis

$$N^{PA-elfogad}(s_1, \ldots, s_V) \supseteq N^{s_v-elfogad} \quad \forall v = 1, \ldots, V, \tag{22}$$

amiből következik, hogy

$$\left| N^{PA-elfogad}(s_1, \ldots, s_V) \right| \geq \left| N^{s_v-elfogad} \right| \quad \forall v = 1, \ldots, V. \tag{23}$$

Mivel a kihasználtság arányos $\left| N^{elfogad} \right|$ értékével, ezért PA jobb kihasználtságot tesz lehetővé.



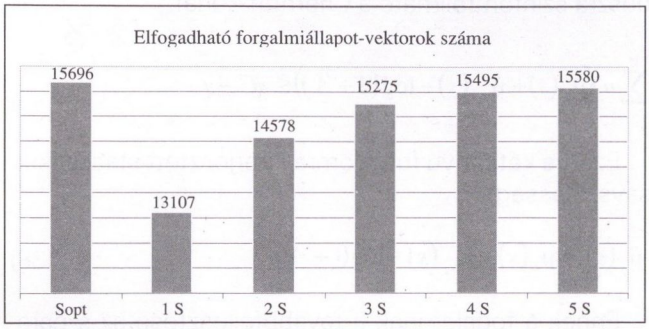
3. ábra: Szeparáló felület három általános s paraméterérték és két forgalmi osztály esetén.

Fennmaradó kérdés, hogyan határozzuk meg az $\mathrm{s} = (s_1, s_2, \ldots s_V)$ paraméter vektort. Ez úgy tehető meg, hogy maximalizáljuk a beengedhető forgalmi vektorok számát, ami a hipersíkok által határolt térfogat mértéke $\left| N^{PA-elfogad}(s_1, \ldots, s_V) \right|$. Ez a terület algoritmikusan kiszámolható, esetén akár analitikus úton. A legjobb PA paraméterek meghatározásához tehát az

$$\mathrm{s}_{opt} : \max_{\mathrm{s}} \left| N^{PA-elfogad}(s_1, \ldots, s_V) \right|, \tag{24}$$

optimalizálási probléma vezet, amely numerikusan egyszerűen megoldható. Ezen paraméterekkel nyerjük a PA hívásengedélyezési algoritmust, amely konzervatív módon működik és nincs szükség tanító halmazra.

Az eredményül kapott struktúra pedig megvalósítható kétrétegű neurális hálózattal.



4. ábra: 5.76 *MBit*/sec kapacitáskorlát mellett az elfogadható forgalmiállapot-vektorok száma a szeparáló felületet alkotó hipersíkok számának függvényében.

A fentiek alapján a statisztikus sávszélesség kiterjesztése megfelel egy $\vec{\mu}(s) = (\mu(s_1),\mu(s_2),\ldots\mu(s_V))$ vektornak.

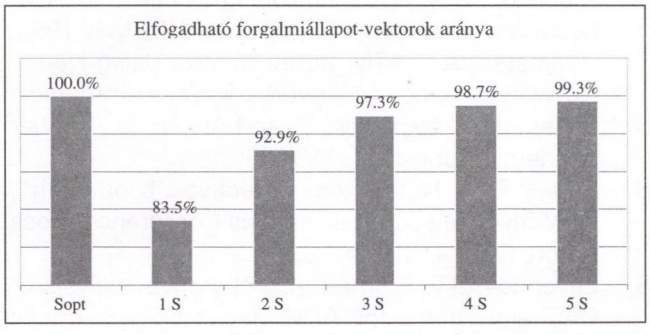
A módszert egy 3 forgalmi osztályból álló modellen teszteltük (V-DSL, Internet Access I, Internet Access II). Az egyes forgalmi osztályok forrásparamétereit a következő táblázat tartalmazza:

	Átlagos adási sebesség (kBit/sec)	Csúcs adási sebesség (kBit/sec)
V-DSL	20	40
Internet Access I	20	384
Internet Access II	24	2048

1. táblázat: Az egyes forgalmi osztályok m_i átlagos és h_i csúcs adási sebességeinek értékei.

A kapacitáskorlátot $C = 5.76\ MBit$/sec-nak tekintettük, míg a QoS-paraméter értéke $\gamma = 8$ volt a tesztelés során. A kísérlet során a szeparáló felületet 1, 2, 3, 4, illetve 5 darab hipersíkot tartalmazó (mely megegyezik a figyelembe vett s_i értékek számával) poligonnal közelítettük. A módszerek hatékonyságát az adott QoS-paraméter mellett elfogadható forgalmiállapot-vektorok számával, vagyis a beengedhető forgalmi volumennel mértük.

A tesztelés során az összehasonlítás alapjául az ábrán „Sopt"-tal jelölt eset szolgált, amikor minden egyes forgalmiállapot-vektor esetén meghatároztuk az optimális $s(\mathrm{n})$ paraméterértéket, és ez alapján döntöttünk, hogy az adott forgalmiállapot-vektor elfogadható-e.



5. ábra: 5.76 *MBit*/sec kapacitáskorlát mellett az elfogadható forgalmiállapot-vektorok számának aránya az optimális érték függvényében.

Az ábrákból látható, hogy míg 1-2 hipersíkot tartalmazó szeparáló felület esetén a módszerrel lényegesen rosszabb kihasználtság érhető el a 3 hipersíkot tartalmazó szeparáló felülethez képest, addig 4-5 hipersík megléte esetén a javulás jóval kisebb mértékű. Tekintettel arra, hogy a módszer komplexitása a hipersíkok számával exponenciálisan növekszik, a kihasználtságot, illetve a futási időt együttesen figyelembe véve a 3 hipersíkot tartalmazó szeparáló felület tűnik optimális megoldásnak. Tekintettel azonban arra, hogy ennek a nagy komplexitású feladatnak az elvégzésére csupán egyszer – a forgalmi paraméterek ismeretében, de még a valós idejű működés megkezdése előtt – van szükség (ilyenkor a futási idő nem jelent korlátot), így ebben az esetben érdemes minél több hipersíkot meghatározni, hiszen annál jobb lesz a közelítés. Mivel a valós idejű működés során egy adott konfiguráció esetén annak eldöntése, hogy az aktuális forgalmiállapot-vektor elfogadható-e, már egyszerűen az előre meghatározott súlyok alapján történik, így itt egyáltalán nem okoz problémát a hipersíkok nagyobb száma.

A kétirányú forgalom hatása

Az előzőekben a statisztikus sávszélességet olyan esetben vizsgáltuk, amikor minden forrás ugyanabba az irányba – a hálózat felé – generál forgalmat. A valóságban azonban előfordulhat, hogy architekturális megoldások miatt a linkenként független lefelé és felfelé irányú forgalom a csomópontokon együttes terhelést jelent a belső kapcsoló működése miatt. Feltételezve, hogy a felfelé irányuló aggregált forgalmat Y-nal, valamint a lefelé irányút Z-vel jelölve a QoS-kommunikáció megvalósításához az alábbi egyenlőtlenség teljesülésére van szükség:

$$P(Y+Z>C) < e^{-\gamma} \tag{25}$$

A probléma az, hogy Z nem független Y-tól, így a Chernoff-egyenlőtlenség használata és a statisztikus sávszélesség ennek megfelelő kiterjesztése nem teljesen egyértelmű.

Az előző fejezettel összhangban, itt is bevezetjük a következő jelöléseket. Feltételezzük, hogy a felfelé irányuló forgalom az $i = 1,\ldots,M$ forgalmi osztályokból tevődik össze. A források On/Off típusú $X^{(i)}$ véletlen változók:

$$P\left(X^{(i)}=0\right)=1-\frac{m_i}{h_i},\quad P\left(X^{(i)}=h_i\right)=\frac{m_i}{h_i} \tag{26}$$

eloszlással, ahol m_i az átlag, h_i pedig a csúcssebesség. Az aggregált felfelé irányuló forgalom felírható

$$Y=\sum_{i=1}^{M}\sum_{j=1}^{n_i}X_j^{(i)} \tag{27}$$

alakban, ahol különböző indexekhez azonos eloszlású független $m_j^{(i)}$ valószínűségi változók tartoznak.

A lefelé irányuló forgalom hasonló módon jellemezhető. Feltételezzük, hogy a források On/Off típusúak

$$P\left(\tilde{X}^{(i)}=0\right)=1-\frac{\tilde{m}_i}{\tilde{h}_i},\quad P\left(\tilde{X}^{(i)}=\tilde{h}_i\right)=\frac{\tilde{m}_i}{\tilde{h}_i} \tag{28}$$

$\tilde{m}_i$ átlag és $\tilde{h}_i$ csúcssebességgel. Továbbá feltételezzük, hogy a felfelé és lefelé irányuló forgalom lineárisan korrelált, vagyis

$$\tilde{X}^{(i)}=A_i X^{(i)}+\nu^{(i)} \tag{29}$$

A forgalmi modell tényezőinek meghatározásához ki kell fejezni a lefelé irányuló forgalom független $\nu^{(i)}$ komponensét. Mostani tárgyalásunkban a független komponenst szintén On/Off típusúnak vesszük. Ha ismertek az $m_i,\tilde{m}_i,h_i,\tilde{h}_i$ paraméterek, akkor $\nu^{(i)}$ csúcssebessége és átlagsebessége kifejezhető az

$$A_i=\frac{E\left(X^{(i)}\tilde{X}^{(i)}\right)}{E\left(X^{(i)2}\right)} \tag{30}$$

$$\tilde{m}_i=A_i m_i+m_{\nu_i} \tag{31}$$

$$\tilde{h}_i=A_i h_i+h_{\nu_i} \tag{32}$$

egyenletekből.
Az aggregált lefelé irányuló forgalom

$$Z=\sum_{i=1}^{M}\sum_{j=1}^{n_i}X_j^{(i)} \tag{33}$$

formában adható meg.

A forgalmiállapot-vektor ebben az esetben is legyen $\mathbf{n}=(n_1,n_2,...n_M)$, ahol az i-dik komponens megadja, hogy hány forrás van jelen az i-dik osztályból mindkét irányban. Ezzel a jelöléssel a következő kritériumot kapjuk:

$$P\left(\sum_{i=1}^{M}\sum_{j=1}^{n_i}\left(X_j^{(i)}+\tilde{X}_j^{(i)}\right)>C\right)<e^{-\gamma}, \tag{34}$$

amelyet tovább írva

$$\begin{aligned}&P\left(\sum_{i=1}^{M}\sum_{j=1}^{n_i}\left(X_j^{(i)}+\tilde{X}_j^{(i)}\right)>C\right)=\\&P\left(\sum_{i=1}^{M}\sum_{j=1}^{n_i}\left(X_j^{(i)}+AX_j^{(i)}+\nu_j^{(i)}\right)>C\right)=\\&P\left(\sum_{i=1}^{M}\sum_{j=1}^{n_i}\left((1+A)X_j^{(i)}+\nu_j^{(i)}\right)>C\right)\end{aligned} \tag{35}$$

a lineáris korrelációs modell használatával.

Külön kiemeljük azt az érdekes tényt, hogy a lefelé irányuló forgalom logaritmikus momentumgeneráló függvénye kifejezhető

$$\begin{aligned}&\tilde{\mu}_i(s):=\log\left(E\left(e^{s\tilde{X}^{(i)}}\right)\right)=\log\left(E\left(e^{s\left(A_iX^{(i)}+\nu^{(i)}\right)}\right)\right)=\\&\qquad\mu(s)+\log A_i+\mu_{\nu_i}(s)\end{aligned} \tag{36}$$

formában, a korrelációs modell segítségével, lévén, hogy $X_j^{(i)}$ és $\nu_j^{(i)}$ függetlenek. Ezek fényében a belső buszra szintén felírható a Chernoff-korlát:

$$\sum_{i=1}^{M}n_i\left(\mu_i(s)+\mu_{\nu_i}(s)+\log(1+A_i)\right)\le sC-\gamma. \tag{37}$$

Ezért a kétirányú forgalomra kiterjesztett statisztikus sávszélesség:

$$\tilde{\mu}_i(s):=\mu_i(s)+\mu_{\nu_i}(s)+\log(1+A_i). \tag{38}$$

Ennek a fogalomnak a továbbfejlesztése az s paraméter optimalizálása szempontjából az előző fejezeteknek megfelelően történhet.

Konklúziók

A cikk a nagy eltérések elmélete segítségével új sávszélesség-fogalmakat vezetett be, amelyek jobb hálózatkihasználtságot eredményeznek hívásengedélyezés és dimenzionálás szempontjából. Az új sávszélességek egyrészt képesek a korrelált lefelé és felfelé irányuló forgalom figyelembevételére, valamint a Chernoff-határ szabad paramétereinek off-line optimalizálására.

Irodalom

1. De Prycker, M.: „Asynchronous Transfer Mode Solution for Broadband ISDN", Ellis Harwood Ltd. 1991.
2. Sohraby, K.: „Flow Admission Control of ON-OFF Sources in High Speed Networks", IEEE, LOBECOM, San Francisco, 1994.
3. Eckberg, A., Dashi, B. and Zoccolilla, R.: „Controlling congestion in B-ISDN/ATM: Issues and Startegies", IEEE Communication Magazine, Vol. 29, No. 9, pp. 64–70, September 1991.
4. Hui, J.: „Resource Allocation for Broadband Networks", IEEE Journal on Selected Area of Communications, Vol. 6, No. 9., pp. 1598–1608, December 1988.
5. Hui, J.: „Switching and Traffic Theory for Integrated Broadband Networks", Kluwer Academic Publishers, 1990.
6. Yasuhiro, M.: „A Dimensioning Scheme in ATM networks", Networks '92, pp. 171–176, May 1992.
7. Hiramatsu, A.: „ATM Traffic Control Using Neural Networks", Neural Networks in Telecommunications, edited by Yuhas, B. and Ansari, N., Kluwer Academic Publishers, 1994.
8. Kelly, F.: „Notes on effective bandwidth", INFORMS Telecommunications Conference, Boca Raton, Florida, March, 1995.
9. Levendovszky, S. Imre: „Comparative analysis of CAC algorithms for ATM networks", Scientific Progress Report, COPP579-SPR-1, EU.
10. Levendovszky, J, E. C. van der Meulen.: „Tail Distribution Estimation for Call Admission in ATM

Networks", Proccedings of IFIP, Third Workshop on Performance Modelling and Evaluation of ATM Networks, Ilkley, West Yorkshire, UK, 2–6th, July 1995.
11. Levendovszky, J.: „Validation of novel CAC algorithms", ICAM- IEEE 1999, pp. 195–211.
12. Levendovszky, J.: „Call admission control of ATM networks based on modulated Markov chains", Journal on Communication dedicated to ATM Networks , Vol. XLVII, pp. 19–24, March 1995.
13. Levendovszky, J.: „Neuron based penalty function classifiers", 19th WIC Conference, Veldhoven, Holland, May, 1998.
14. Levendovszky, J. et al: „Nonparameteric decsison algorithms for CAC in ATM networks", Journal on Performance Evaluation, Elsevier, Vol. 41, 2000, pp. 133–147.

Hírek

AppsWorld, az e-business jelene és jövője

2002. január 15. és 18. között Amsterdamban kerül megrendezésre az Oracle nemzetközi konferenciája, az AppsWorld Europe, amely az Oracle technológiáit használó vállalatok döntéshozóinak évente megrendezésre kerülő legnagyobb összejövetele. Az Oracle AppsNet állandóan elérhető új, on-line szolgáltatása révén az idei évben már azok is bekapcsolódhattak a konferencia munkájába, akik személyesen nem tudtak azon részt venni.

A rendezvény célja az, hogy azok a vállalatok, amelyek működésük részét vagy egészét elektronikus alapokra helyezték, vagy a jövőben ilyen irányba szeretnének elmozdulni, a legújabb e-business stratégiák, technológiák, alkalmazások, illetve mások tapasztalatainak megismerésével a számukra legjobb megoldásokat választhassák ki. A konferencia nemcsak a legújabb lehetőségek megismerésének a fóruma, hanem a gyorsan fejlődő iparág jövőbeli tendenciái áttekintésének és a lehetséges fejlődési irányvonalak kijelölésének egyik eszköze. A részt vevő érdeklődők és a megoldásokat már használó partnerek igényei itt jutnak el leghatékonyabban a vállalathoz, így a három nap alatt lezajló információcsere valóban a jövő fejlesztéseinek egyik alapköve.

A közel 200 előadás során továbbá a szerződés-nyilvántartás, az e-üzlet-technológia, a pénzügy, az emberi erőforrás, a marketing, a termékfejlesztés, a projektkezelés, a szolgáltatási és ellátási lánc, a beszerzés és az értékesítés területek egyedi elvárásainak megfelelően kialakított megoldásait ismerhetik meg a résztvevők testközelből.

❖ ❖ ❖

A Siemens IC Mobile ágazata és a Siemens leányvállalat „designafairs" európai és ázsiai diákok számára tervezési tábort indít márciusban. Itt két tutor segítségével szemeszterenként tíz különböző szakon tanuló diák fogja a távközlés különféle kérdéseit öt hónapon át tanulmányozni és feldolgozni, végül eredményeiket alkotó módon átültetni a gyakorlatba. A tanulmányozható kérdések a „digitális" társadalom tudati változásaira, a kultúraváltásra vonatkoznak, valamint a kommunikáció ebből adódó új koncepcionális modelljére. A 2002. márciustól júliusig, részben Sanghajban megtartandó első szemeszter résztvevőinek kiválasztása megtörtént. A designlab működésének költségeit, beleértve a diákok ösztöndíját, a Siemens IC Mobile fedezi. A szeptemberben induló második szemeszterre pályázni lehet az alábbi címeken:

info@designlab-siemens-mobile.org, vagy

Anke Gebhard, Tölzer Strasse 2c, 81379 München.

Hírek

Az Oktatási Minisztérium, a Nemzeti Szakképzési Intézet és a Cisco Systems együttműködésében kiírt pályázat eredményeként 16 további hazai oktatási intézményben indulhat meg a hálózati szakemberek képzése.

Ez a feladat rendkívül szerteágazó, magában foglalja az alap-, közép- és felső szintű informatikusok képzését, valamint az általános informatikai ismereteket oktatását.

Az együttműködés eredményeképpen az új szakma bevezetésének elősegítésére pályázatot írtak ki 50 millió Ft értékben. A pályázat nyertesei – 16 hazai közép- és felsőoktatási intézmény – 2001. december 18-án írhatták alá a támogatási megállapodást, így még a 2001—2002-es tanévben megkezdhetik a hálózati szakemberképzést.

A kiírt pályázatra 42-en regisztráltak, és 28-an adtak be érvényes pályázatot. A szakmai bizottság döntése alapján a rendelkezésre álló keretből 16 oktatási intézmény számára nyújt támogatást. A támogatás a Cisco Hálózati Akadémia Program beindításához szükséges alapvető laborfelszerelésekre (5 útvonalválasztó, 2 kapcsoló, alapvető kábelezés és egyéves jótállás, illetve karbantartás) vonatkozik.

Felismerte, hogy a hazánkban már ma is jelentős, és a kutatók által 2003-ra mintegy 37%-ra prognosztizált hálózati szakemberhiányt (Európára ugyanekkorra 35%-ot jeleznek) nem lehet kizárólag a hagyományos közoktatás eszközeivel hatékonyan csökkenteni. Követik az Európában és a világon egyre elterjedtebbé váló gyakorlatot, amely szerint a megoldás kidolgozásában szorosan együttműködik a magánszféra a közoktatással, valamint azok szakértőivel.

A képzésből kikerülő szakemberek azonnal tudják hasznosítani szakismereteiket és gyakorlati tapasztalataikat, függetlenül attól, hogy az őket alkalmazó vállalat, vagy más szervezet mely gyártó berendezéseit használja. (Tehát képesítésük nem csupán a Cisco berendezéseinek ismeretéről tanúskodik.)

Hazánkban több éve működnek Cisco hálózati akadémiák, elsősorban felsőoktatási és szakképző intézmények közreműködésével. Eddig 24 intézmény kapcsolódott be a képzési programba, és további mintegy 70 jelezte ez irányú szándékát. Ennek a – nem pusztán elméleti és gyakorlati tananyagot, hanem az oktatás és az oktatóképzés komplett struktúráját is biztosító – képzési formának széles körű hazai alkalmazása hatékony eszközt jelenthet a hálózati szakemberhiány csökkentésére. A képzés maximálisan 2 év tanulás – és az előírt vizsgák sikeres letétele – után azonnal felhasználható, gyakorlati szaktudást ad.

Az Oktatási Minisztérium, az NSZI és a Cisco Systems kezdeményezését követő együttműködés tapasztalatai alapján az OM és az NSZI a közelmúltban több információtechnológiai céggel is tárgyalt, hogy a Cisco Hálózati Akadémia Programhoz hasonló további iparági támogatással rendelkező oktatási lehetőségeket kutasson fel a hazai informatikai szakemberképzés számára.

❖ ❖ ❖

Árokásás helyett szennyvízcsatorna

Költséges az útburkolatok felbontása fényvezető kábelek elhelyezése érdekében. Az Egyesült Államokban működő Citynet nevű szolgáltató hálózatát már 12 városban a szennyvízcsatornában építi ki. Utóbbi használatáért a városok önkormányzata bruttó bevételének bizonyos százalékát fizeti. Ezenkívül videofelvételt bocsát rendelkezésükre a szennyvízalagutak belsejéről, sőt vállalja a szennyvízelvezető hálózat fenntartását és tisztítását azért, hogy az önkormányzat alkalmazottai ne tegyenek kárt a fényvezetőkben.

Alcatel teljes rendszert dolgozott ki a víz-, a gázellátás és a csatornázás meglévő föld alatti hálózatának felhasználására, fénykábelek elhelyezésére. Elméletben a fénykábelek gáz- és vízcsövekre ültetése olcsóbb, mint a szennyvízelvezető hálózatra, de a Citynet műszaki igazgatója szerint a csatorna a legolcsóbb közmű és a leginkább üzembiztos is, mert a legmélyebben fekszik, így ásógépek a legkevésbé sértik meg.

Egy kanadai cég állítása szerint nyolcszor gyorsabban építi ki a távközlőhálózatot a csatornában, mint az e célra ásott árokban. A munkát egy 1,8 m hosszú robot végzi, amely még 20 cm átmérőjű csőben is naponta 800 m kábelt helyez el. Ennek sötét szálait adja el távközlési vállalatoknak, bankoknak és másoknak.

Virtuális magánhálózatok tervezése védelemmel

MALIOSZ MARKOSZ–CINKLER TIBOR

Budapesti Műszaki és Gazdaságtudományi Egyetem (BME)
Távközlési és Telematikai Tanszék

Célunk virtuális magánhálózatok (Virtual Private Network – VPN) útvonaltervezése, adott fizikai hálózatban, védelmi szempontok figyelembevételével. Két, különböző szintű védelmi módszert vizsgáltunk, az egyikben kívülről, a szolgáltató gondoskodik a virtuális utak védelméről, míg a másikban az adott magánhálózaton belül építjük fel a védelmet. A probléma megfogalmazására általános modellt alkottunk, azaz nem korlátozódtunk egy adott hálózati technológiára, így a javasolt módszerek alkalmazhatók különböző SDH, ATM, IP, MPLS, illetve WR-DWDM hálózatokra. A magánhálózatok átviteli követelményeit a végpontok közötti sávszélességigényekkel adjuk meg. Adottak a fizikai hálózat összeköttetéseinek kapacitásai, valamint a magánhálózatok átviteli igényei, keressük azt a védelemmel ellátott hálózati konfigurációt, amelynek költsége a legkisebb. A numerikus eredmények megmutatják a különböző védelmi megoldások jellemzőit.

Bevezető

A virtuális magánhálózatok alkalmazása széles körben elterjedt az utóbbi években. Egyre több felhasználó igényli a titkos kapcsolatot, és emellett a szolgáltatás valamilyen szintű minőségi garanciáit is. Ahelyett, hogy nagy költségekkel saját hálózatot építenénk ki, kézenfekvő megoldás a már létező nyilvános hozzáférésű hálózatokat kihasználni erre a célra. A virtuális magánhálózatok lehetővé teszik egy zárt csoport kommunikációját, különleges tekintettel a titkos és biztonságos átvitelre. Tipikus példák virtuális magánhálózatok alkalmazására: távoli elérés közös munkán dolgozó munkatársak részére, otthoni felhasználó bejelentkezése a munkahelyi intranetre.

A titkosítás és a biztonság védelmét a felsőbb kapcsolati rétegek végzik, azonban az útvonaltervezésnél kulcsfontosságúak az üzemeltetési költségek. A megbízhatóság érdekében a tervezési módszernek figyelembe kell vennie a *hibalehetőségeket* is, ezért a virtuális magánhálózatok redundánsak lesznek, a végpontok között egy elsődleges, üzemi, valamint egy másodlagos, védelmi útvonal szükséges.

A virtuális magánhálózatok megosztva használják a fizikai erőforrásokat, úgymint a szakaszok sávszélességét, vagy a csomópontok puffereit, feldolgozási képességét, így egymással versengenek ezekért az erőforrásokért. Azonban a virtuális hálózatok alkalmazásának van jó néhány előnye. Nem szükséges kiépíteni a fizikai magánhálózatot, mindössze a nyilvános hálózaton kell konfigurálni a virtuális magánhálózatot, ami költségkímélő megoldás az előbbihez képest. Ha egy adott virtuális hálózat éppen használaton kívül van, akkor a többi virtuális magánhálózat fel tudja használni az ily módon felszabadult erőforrásokat, sőt át is konfigurálhatjuk a virtuális hálózatunkat, ami egy fizikai hálózat esetén nem olyan egyszerű.

Virtuális magánhálózatok létrehozhatók különböző típusú hálózatokon, úgymint ATM, IP, vagy Multi-Service hálózatokon. A különböző szolgáltatásminőséget garantáló módszerekkel is társíthatók a virtuális hálózatok, mint például VPN-Diffserv kombinált megoldás [1]. Az általunk megalkotott modellben *statikus sávszélességigényekkel* dolgozunk és a *különféle védelmi eljárásokat* elemezzük. Létezik megoldás, amely szintén statikus igényeket vesz alapul és létesít virtuális magánhálózatot egy nagyobb hálózaton [2]. Megközelítésünk egy időben több virtuális magánhálózatot tervez a fizikai hálózaton. Másik terület a dinamikus igények vizsgálata, mint például [3], ahol az igények újraméretezését megengedik, azonban a védelemmel nem foglalkoznak.

A szakirodalom [4,5,6] vizsgálja az együttes erőforrásfoglalás- és útvonaltervezést is multi-service hálózatokban, azonban a felsoroltak nincsenek tekintettel a virtuális magánhálózatok szempontjaira. A fizikai hálózatok méretezése alapvetően meghatározza a benne elhelyezett virtuális hálózatok számát, kiterjedését. A virtuális magánhálózatok méretének jellemzése, megállapítása szintén fontos kérdés [7].

Védelmi módszerek

Megközelítésünkben több virtuális magánhálózatot tervezünk meg ugyanazon fizikai hálózaton. Két védelmi módszert definiáltunk, nevezetesen az utakat lehet védeni az összeköttetések szintjén, vagy a virtuális magánhálózat szintjén. Az *összeköttetés szintű védelem* azt jelenti, hogy minden végpontpár közötti forgalom

részére két utat biztosítunk, amelyek a virtuális magánhálózathoz tartoznak. A két út lehet élfüggetlen, ha összeköttetés-meghibásodás, vagy csomópontfüggetlen, ha csomópont-meghibásodás elleni védelmet is akarunk nyújtani. A *virtuális hálózat szintű védelem* azt jelenti, hogy a szakaszok, amelyek a virtuális magánhálózatot alkotják, lesznek védve, nem pedig a forgalom. Az 1. ábra illusztrálja, hogy lesz egy üzemi virtuális magánhálózatváz, és egy védelmi váz. Ezeket a vázakat a virtuális szakaszok alkotják, az üzemi és a védelmi utak alapján. Ennél a védelemnél kizárólag az élfüggetlenség értelmezhető, ugyanis csak a virtuális magánhálózatokhoz keresünk védelmet, nem pedig a bennük lévő forgalmi igényekhez. Ezért az üzemi és védelmi váznak mindig több közös pontja lesz, azok a pontok, ahol át lehet kapcsolni a forgalmat hiba esetén.

A két módszer közötti különbség az, hogy ha egy szakasz meghibásodik és összeköttetés szintű védelmet használunk, akkor az összes út valamennyi virtuális hálózatban, ami érintette a meghibásodott szakaszt, át lesz kapcsolva a védelmi útra. A virtuális hálózat szintű védelemnél az összes virtuális hálózat, amelynek része a meghibásodott szakasz, át lesz kapcsolva a védelmi vázra, azaz teljes virtuális hálózatok épülnek ki.

1. ábra Különböző védelmi módszerek

Célkitűzésünk, hogy megtaláljuk a virtuális magánhálózatok azon optimális konfigurációját, ahol a virtuális szakaszok száma a minimális. Ez előnyös, amikor a használt fizikai szakaszok, azaz a virtuális összeköttetések után arányos üzemeltetési, karbantartási költséget számol fel a szolgáltató.

Kiindulásul adottak a forgalmi igények, valamint a fizikai hálózat kapacitásmátrixa. Ezek az adatok statikusnak tekinthetők, mintha egy pillanatfelvételt készítenénk a hálózatról. Ezért a gyakorlatban olyan helyzetekben alkalmazható módszerünk, amikor egy szolgáltató megtervezi a virtuális magánhálózatot saját hálózatában a cégek, ügyfelek heti vagy havi megrendelései alapján. Az eredményül kapott útvonalakat az általános *célalapú* forgalomirányítás helyett *kényszeralapú* forgalomirányítással (Constraint-Based Routing – CR) tudjuk a mai hálózatokban megvalósítani, mint például MPLS (Multiprotocol Label Switching) segítségével [8,9].

A modellek

Összeköttetés szintű védelem

Az élfüggetlen modellben a virtuális élek számát – és ezzel együtt a költségeket is – minimalizáljuk. A hálózat felírható irányítatlan gráfként: $U(N,L,C)$. N a csomópontok halmaza, L az élek halmaza és C a kapacitásmátrix, amely a fizikai szakaszok sávszélességét tartalmazza. Minden virtuális magánhálózathoz adott a forgalommátrix, amelyben a magánhálózat végpontpárjai közötti sávszélességigény szerepel. Az optimalizálásban szereplő változók:

$X1_l^d$ és $X2_l^d$ bináris változók, l a fizikai szakasz azonosítója, d a forgalom sávszélességigényét jelöli két végpont között

$X1_l^d \in \{0,1\}$ $\quad X2_l^d \in \{0,1\}$

Y_l^p bináris változó, l a fizikai szakasz azonosítója, p a virtuális hálózat azonosítója

$Y_l^d \in \{0,1\}$

$X1_l^d$ és $X2_l^d$ fejezi ki, hogy az l szakasz része-e az útvonalnak, amely d igényhez tartozik, $X1_l^d$ az üzemi $X2_l^d$ pedig a védelmi útvonalra vonatkozik. Y_l azt fejezi ki, hogy az l szakasz része-e p virtuális hálózatnak. A „0" érték jelöli, amikor nincs forgalom az l szakaszon, és „1", amikor van. Az l-lel jelölt szakasz tulajdonképpen (i,j) számpár, ahol i és j a csomópontok sorszámai (azonosítói), azaz az l szakasz az i és j pont között helyezkedik el. A d-vel jelölt sávszélességigény pedig (i,j,b,v) számnégyes, ahol i,j számpár az i, j csomópontok sorszámai, b a sávszélességigény, v a virtuális hálózat azonosítója, jelentése: a v-vel jelölt virtuális magánhálózatban b nagyságú a sávszélességigény az i és j csomópont között.

A lehetséges l-ek azok az (i,j) számpárok, ahol az (i,j) elem nem nulla a kapacitásmátrixban, ezeket jelöljük az L halmazzal $(l \in L)$. Ha a b sávszélességigény (i,j) pontok között nem nulla, akkor ez érvényes igénynek tekinthető, ezek alkotják a D halmazt $(d \in D)$.

$l = \{(i,j) \mid (i,j) \in L, L \subset N^2\}$

$X1_l^d$, $X2_l^d$ valamint az Y_l változók fejezik ki a szakaszok kihasználását, csak más megközelítésben. Amíg $X1_l^d$ és $X2_l^d$ az l szakasz használatát a d igény szempontjából tükrözik, addig Y_l azt mutatja, hogy az l szakasz része-e p virtuális magánhálózatnak.

A virtuális magánhálózat költségét a következőképpen definiáljuk:

$$C_{VPN} = \sum_{\forall p} \sum_{l \in L} Y_l^p \qquad (1)$$

A célfüggvény:

$\min(C_{VPN})$

Kényszerfeltételek:

Folyamfolytonossági feltételek:

$$\sum_{\forall (i,j)\in L} X1^d_{(i,j)} - \sum_{\forall (j,k)\in L} X1^d_{(j,k)} = \begin{cases} -1, & \text{ha j forrása d - nek} \\ 1, & \text{ha j nyelője d - nek} \\ 0, & \text{egyébként} \end{cases} \quad \forall j \in N, \forall d \in D \tag{2}$$

$$\sum_{\forall (i,j)\in L} X2^d_{(i,j)} - \sum_{\forall (j,k)\in L} X2^d_{(j,k)} = \begin{cases} -1, & \text{ha j forrása d - nek} \\ 1, & \text{ha j nyelője d - nek} \\ 0, & \text{egyébként} \end{cases} \quad \forall j \in N, \forall d \in D \tag{3}$$

A folyammegmaradási egyenletek biztosítják, hogy a kijelölt forrásokból induló forgalom célba érkezzen. A közbenső csomópontokban a beérkező és kimenő forgalom egyenlő. Mindez az üzemi és a védelmi útvonalakra is érvényes. Az első összeg a j csomópontba beérkező, a második az onnan kimenő forgalmat jelzi.

Kapacitáskorlát:

$$\sum_{\forall d\in D} (X1^d_l + X2^d_l) b^d \le B_l \qquad \forall l \in L \tag{4}$$

B_l jelöli az l szakasz fizikai kapacitását, b^d pedig a d igény sávszélességét. $X1^d_l$, $X2^d_l$ jelzi, hogy az l szakasz az üzemi, illetve védelmi útvonal része-e. Ez a korlát azt fejezi ki, hogy a virtuális hálózatok közt szétosztott összkapacitás nem haladhatja meg a fizikai korlátot.

Függetlenségi feltétel:

$$X1^d_l + X2^d_l \le Y_l^p \qquad \forall l \in L, \forall p, \forall d \in D^p \tag{5}$$

D^p azon igények halmaza, amelyek a p virtuális hálózathoz tartoznak. $Y_l^p \in \{0,1\}$, azaz $X1_l$ és $X2_l$ közül legfeljebb az egyik lehet „1", azaz csak az egyik használhatja az l szakaszt, biztosítva az utak élfüggetlenségét.

Csomópontfüggetlen eset mindössze eggyel több korlátot tartalmaz, mint az előző, ami azt fejezi ki, hogy két útnak nem lehet közös pontja.

Függetlenségi feltétel II

$$\sum_{l(i,j)\text{: i és j sem forrása, sem nyelője } d\text{-nek}} (X1^d_l + X2^d_l) \le 1 \qquad \forall d \in D \tag{6}$$

Ez a korlát azt fejezi ki, hogy nem lehet két út, amely keresztülhalad az i (illetve j) csomóponton, kivéve, ha az utak onnan indulnak, illetve ott találkoznak.

Virtuális hálózat szintű védelem

Ebben az esetben csak az élfüggetlenséget tudjuk értelmezni. Ez a modell szintén a virtuális szakaszok számát minimalizálja, viszont teljes egészként védi a virtuális hálózatot. Az optimalizálásban szereplő változók:

$X1_l$ és $X2_l$ bináris változók, l a fizikai szakasz azonosítója, d a sávszélességigényt fejezi ki két végpont között

$X1^d_l \in \{0,1\}$ $\quad X2^d_l \in \{0,1\}$

$Y1^p_l$ és $Y2^p_l$ bináris változók, l a fizikai szakasz azonosítója, p a virtuális hálózat azonosítója

$Y1^d_l \in \{0,1\}$ $\quad Y2^d_l \in \{0,1\}$

$X1^d_l$ és $X2^d_l$ jelzi, hogy az l szakasz hordoz-e a d igényhez tartozó forgalmat. $X1^d_l$ vonatkozik az üzemi, $X2^d_l$ pedig a védelmi útvonalra. $Y1_l$ és $Y2_l$ jelzi, hogy az l szakasz az üzemi vagy a védelmi virtuális hálózatváz része. Ha ezen változók értéke „0", akkor nincs forgalom az l szakaszon, az „1" érték jelzi, hogy *van forgalom* az adott szakaszon, d pedig ugyanolyan igényt fejez ki, mint a fentebb ismertetett esetben.

$X1^d_l$, $X2^d_l$, $Y1_l$, $Y2_l$ változók itt is ugyanazt a mennyiséget fejezik ki más megközelítésben. Míg $X1^d_l$ és $X2^d_l$ az igények szerint mutatja meg az adott szakasz használatát, addig $Y1_l$, és $Y2_l$, azt mutatja, hogy az adott szakasz az üzemi vagy a védelmi váz része.

A virtuális magánhálózat költségét a következőképpen definiáltuk:

$$C_{VPN} = \sum_{\forall p} \sum_{l\in L} (Y1^p_l + Y2^p_l) \tag{7}$$

A célfüggvény:

min C

A korlátok részben megegyeznek az összeköttetés szintű védelem modelljével, így a (2), (3) és (4) képletek itt is érvényesek.

További kapacitáskorlátok:

$$X1^d_l \le Y1^p_l \qquad \forall l \in L, \forall p, \forall d \in D^p \tag{8}$$

$$X2^d_l \le Y2^p_l \qquad \forall l \in L, \forall p, \forall d \in D^p \tag{9}$$

D azon igények halmaza, amelyek a p azonosítójú virtuális magánhálózathoz tartoznak. Ha $X1^d_l$, $X2^d_l$ értéke „1" (jelezve, hogy l szakasz hordozza a d igény forgalmát), maga után vonja, hogy $Y1_l$, $Y2_l$ értékének szintén „1"-nek kell lennie, jelezvén, hogy az l szakasz a p azonosítójú virtuális magánhálózat vázához tartozik.

A függetlenségi feltétel ebben a modellben:

$$Y1^p_l + Y2^p_l \le 1 \qquad \forall l \in L, \forall p \tag{10}$$

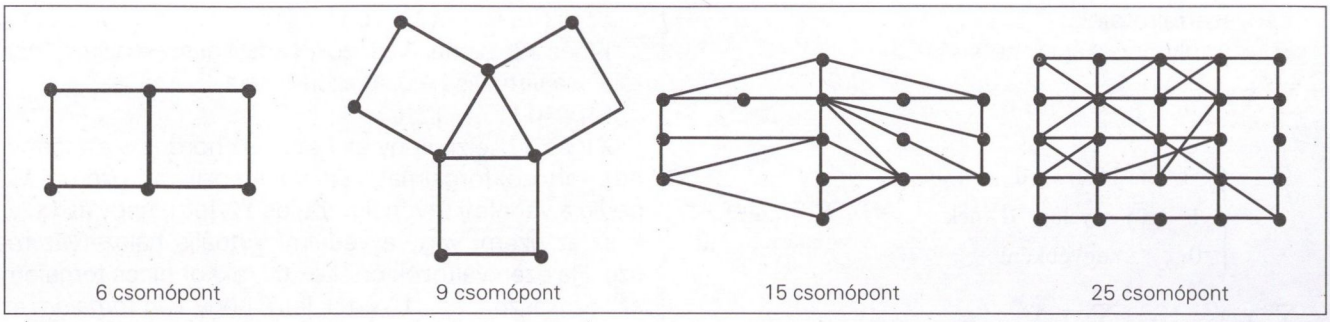
Az élfüggetlenség biztosítása végett a következő egyenlőséget is fel kell írnunk, ellenkező esetben az üzemi és védelmi útvonalak ugyanazt a szakaszt tudnák használni az ellenkező irányokban. Azaz az Y változók által jelölt virtuális hálózatvázak irányítatlanok.

$$Y1^p_{(i,j)} = Y2^p_{(j,i)} \qquad \forall (i,j) \in L, \forall p \tag{11}$$

Az optimalizálási eljárás

Hálózati topológiák

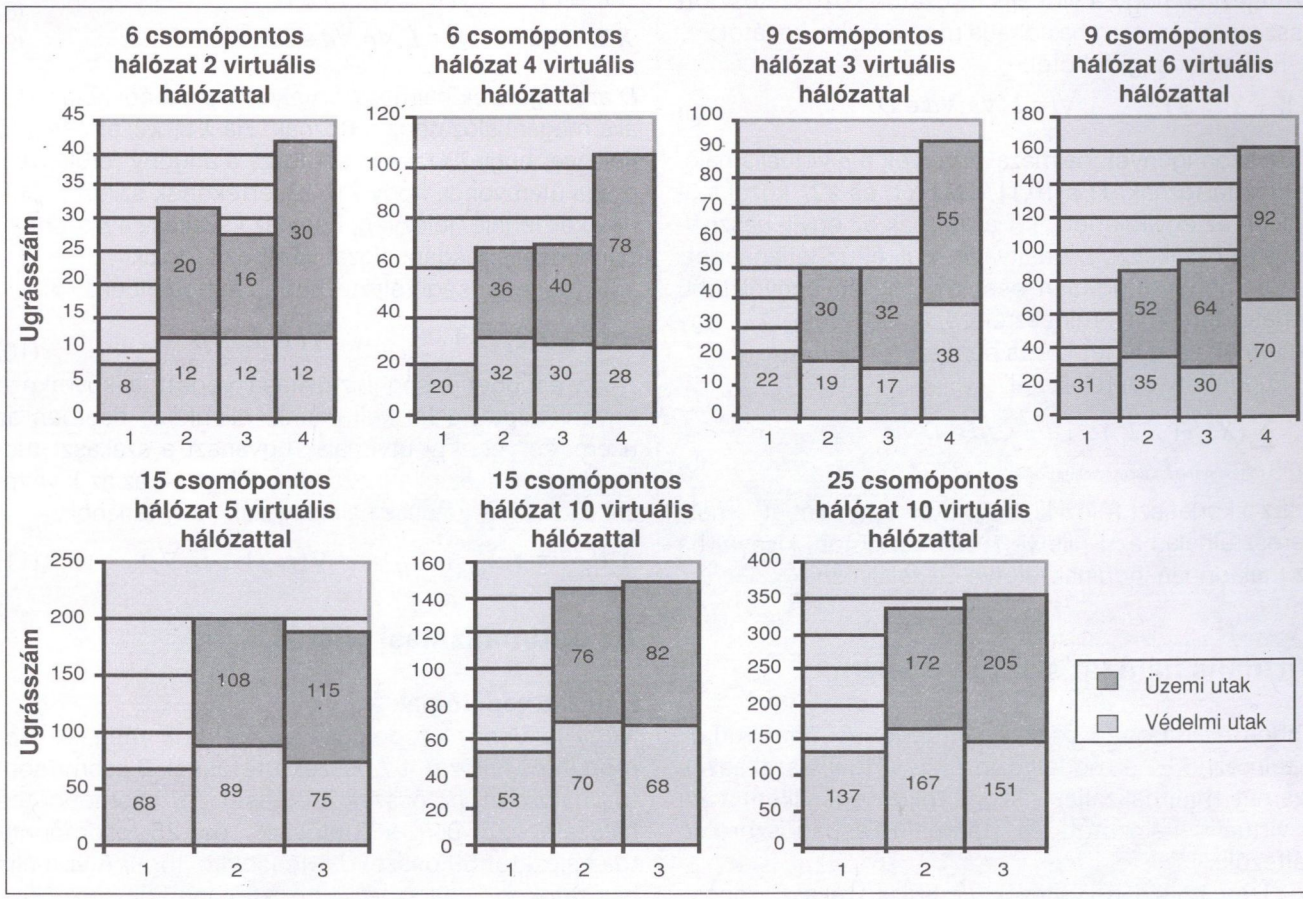
Négy különböző topológiát vizsgáltunk meg, 6 csomópontos hálózatot 7 összeköttetéssel, 9 csomópontos hálózatot 12 összeköttetéssel, 15 csomópontos hálózatot 25 összeköttetéssel, és 25 csomópontos hálózatot 50 összeköttetéssel (2. ábra). A virtuális hálózatokon belül az egyes esetekben különböző forgalmi igényeket generáltunk.



2. ábra Hálózati topológiák

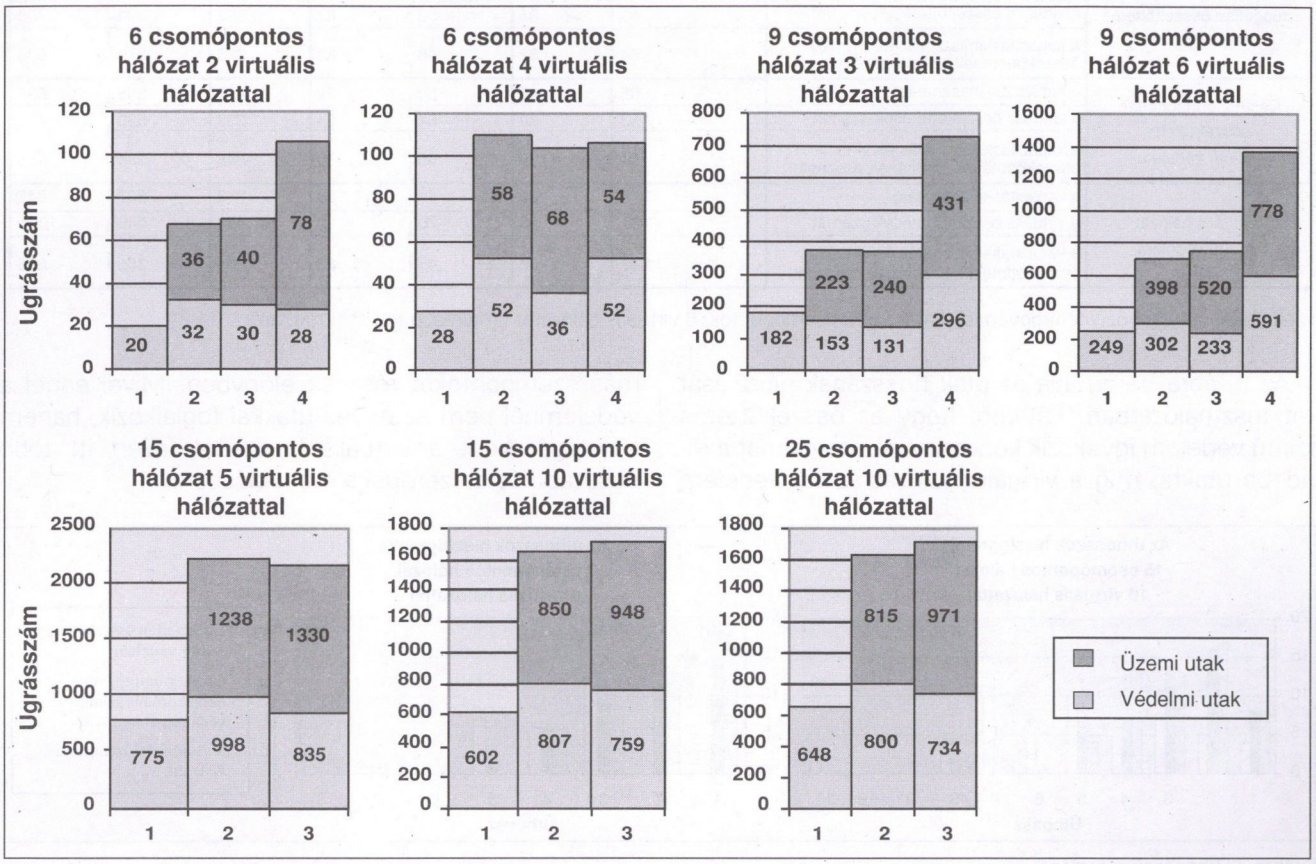
Eredmények

Az ILOG CPLEX optimalizáló [10] szoftvercsomagot alkalmaztuk a felírt ILP (Integer Linear Programming), egész értékű lineáris programozási probléma megoldására. Az útvonaltervezés eredményeit egymással és a védelem nélküli esettel [11] is összehasonlítottuk. A védelem nélküli esetben a megoldások triviálisak, hiszen a rendelkezésre álló kapacitások elég nagyok, hogy a védelmi útvonalak is elférjenek a hálózatban. A 3. ábrán látható diagramok az útvonalak élszámát, a 4. ábra pedig a felhasznált összkapacitást mutatja. $X1_l^d$, illetve $X2_l^d$ kapott értékek közül a kisebbet választottuk az üzemi útvonalnak és a nagyobbat a védelminek. Az útvonalak élszámait és a kapacitás kihasználását összegeztük külön az üzemi, és külön a védelmi útvonalakra. Minden diagramon az első oszlop a *védelem nélküli,* a második oszlop *az összeköttetés szintű védelem élfüggetlen esetét,* a harmadik oszlop *az összeköttetés szintű védelem csomópontfüggetlen esetét,* a negyedik oszlop pedig *a virtuális magánhálózat szintű védelmet* ábrázolja. Amint a diagramon látható, a 15 csomópontos hálózattól kezdve nincs negyedik oszlop, ennek az az oka, hogy ezekben az esetekben a számítások több napig tartottak volna, amit nem tartottunk elfogadhatónak. Az 1. táblázatban a virtuális szakaszok száma, azaz a célfüggvény eredménye és a számításhoz szükséges idő látható. A védelem nélküli esetben ez az idő mindössze néhány századmásodperc, kivéve a 15 csomópontos hálózatot. Az él- és csomópontfüggetlen eseteket összehasonlítva, a csomópontfüggetlen rövidebb idő alatt megoldható, annak ellenére, hogy több korlátot tartalmaz. A virtuális hálózat szintű védelem kiszámítása nyilvánvalóan tovább tart a többinél, mivel már a megfogalmazás is bonyolultabb.



3. ábra Ugrásszámok 4 különböző mintapélda esetén

A virtuális szakaszok száma (a célfüggvény) legalább a kétszeresére növekszik, ha összeköttetés szintű védelmet, és egészen négy-, sőt ötszörösére, ha virtuális hálózat szintű védelmet alkalmazunk. Kis hálózatok esetén nincs lényeges különbség az él- és csomópontfüggetlen esetben a virtuális szakaszok számában. Ezekben a hálózatokban a lehetséges használható összeköttetések is eleve korlátozott számúak, ezért érthető, hogy nem is lehet nagy a különbség.



4. ábra Kapacitáskihasználás 4 különböző teszthálózatra

A 3. ábra szemlélteti, hogy a virtuális magánhálózat szintű védelem nagyobb ugrásszámú, azaz hosszabb útvonalakat igényel. Az él- és csomópontfüggetlen megoldás ebben a tekintetben sem különbözik számottevően. Nagyobb hálózatokban nagyszámú virtuális magánhálózat esetén megfigyelhető az a tendencia, hogy a csomópontfüggetlen megoldás némileg nagyobb ugrásszámot igényel. A 4. ábrán látható eredmények hasonlók a 3. ábrán láthatókhoz, ugyanis hosszabb útvonalak több kapacitást használnak összességében. Ugyanaz figyelhető meg, mint a 3. ábrán, kapacitás tekintetében az összeköttetés szintű védelem körülbelül kétszeres, a virtuális magánhálózat szintű védelem esetén pedig körülbelül négyszeres az igény.

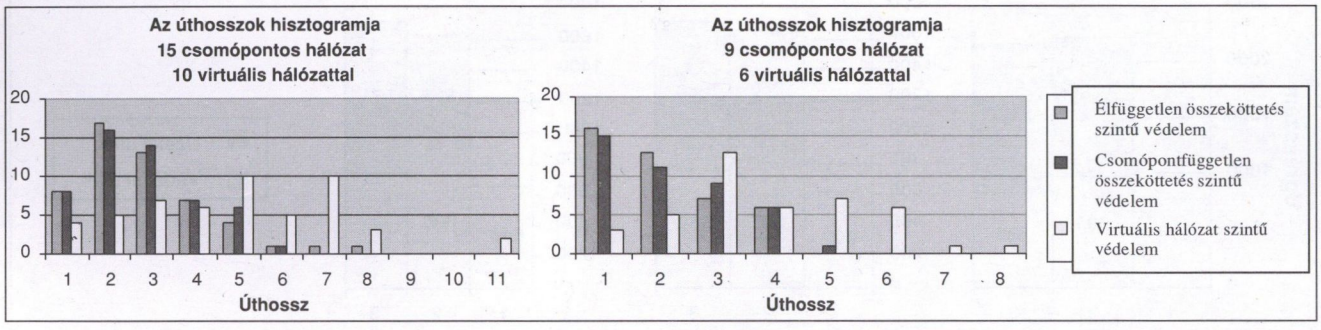
Megfigyelhető, hogy egyes konfigurációknál az üzemi útvonal rövidebb (vagy kevesebb kapacitást használ), mint a védelem nélküli esetben. Ennek az a magyarázata, hogy célfüggvény a virtuális utak száma volt (ami megegyezik ezekben az esetekben, ld. 1. táblázat), nem pedig az utak hossza. Ha átlagoljuk az üzemi és védelmi útvonalakra kapott értékeket, akkor mindig nagyobbat kapunk, mint a védelem nélküli esetben. Az ábrákról az is látszik, hogy legnagyobb az eltérés az üzemi és védelmi utak között a csomópontfüggetlen esetben.

Az általánosan alkalmazott költségalapú (azaz a mi esetünkben a használt kapacitás) optimalizálás és a modellünk (a virtuális élek számának minimalizálása) közötti különbség megvilágítására egy példán keresztül a 2. táblázatban bemutatjuk a különbségeket. Három különböző célfüggvényt számítottunk ki a 9 csomópontos hálózaton, amelyben 6 virtuális hálózatot helyeztünk el. Az első esetben csak a kapacitáskihasználtságot minimalizáltuk, azaz nem vagyunk tekintettel a virtuális magánhálózatokra, minden igény egymástól és virtuális hálózathoz való tartozásától független. A második esetben csak a virtuális szakaszok számát minimalizáljuk, míg a harmadik az előző kettő kombinációja. Az eredmények azt mutatják, hogy ha csak a kapacitáskihasználást minimalizáljuk, az megnöveli a virtuális szakaszok számát. Ha kizárólag a virtuális szakaszok számát minimalizáljuk, akkor hosszabb utakat és nagyobb kapacitáskihasználtságot kapunk. A kombinált megoldás eredménye közelebb áll a második módszerhez a virtuális szakaszok számát tekintve. Kapacitáskihasználtságban jobb, mint a második, de még ez is rosszabb, mint az első.

	Minimalizáljuk	Virtuális összeköttetések száma	Ugrásszám			Használt kapacitás		
			Üzemi	Védelmi	Összesen	Üzemi	Védelmi	Összesen
Védelem nélkül	a kapacitáskihasználást	24	29		29	226		226
	a virtuális összeköttetések számát	22	31		31	249		249
	a kapacitáskihasználás és virtuális összeköttetések számának összegét	24	29		29	226		226
Élfüggetlen összeköttetés szintű védelem	a kapacitáskihasználást	67	29	50	79	238	395	633
	a virtuális összeköttetések számát	53	35	52	87	302	398	700
	a kapacitáskihasználás és virtuális összeköttetések számának összegét	54	32	48	80	266	370	636
Csomópontfüggetlen összeköttetés szintű védelem	a kapacitáskihasználást	65	29	50	79	238	395	633
	a virtuális összeköttetések számát	53	30	64	94	233	520	753
	a kapacitáskihasználás és virtuális összeköttetések számának összegét	54	30	50	80	248	388	636
Virtuális hálózat szintű védelem	a kapacitáskihasználást	108	39	41	80	313	332	645
	a virtuális összeköttetések számát	102	55	70	12	458	546	1004
	a kapacitáskihasználás és virtuális összeköttetések számának összegét	102	38	45	83	301	365	666

1. táblázat Különböző célfüggvények hatása a 9 csomópontos, 6 virtuális hálózatot tartalmazó teszthálózatban

Az 5. ábra bemutatja az utak hosszának eloszlását két teszthálózatban. Látható, hogy az összeköttetés szintű védelem igyekszik koncentrálni a forgalmat a rövidebb utakra, míg a virtuális hálózat szintű védelem más szempontokat részesít előnyben. Mivel ennél a védelemnél nem az egyes utakkal foglalkozik, hanem egy egészként a virtuális hálózattal, ezért itt több hosszabb út is szerepel a megoldásban.



5. ábra Úthosszok eloszlása

Összefoglalás

A virtuális magánhálózatokra vonatkozó együttes útvonaltervezés és minőségigarancia-nyújtás különböző védelmi módszereit mutattuk be. Különböző szintű védelmi módszereink az optimális üzemi és védelmi útvonalak kiválasztására alkalmasak. Célunk a virtuális szakaszok minimalizálása volt a hozzárendelt védelem figyelembevételével. Módszereink igyekeznek a forgalmat kevesebb szakaszra összpontosítani, ami ugyan rosszabb kapacitáskihasználást eredményez, de ily módon a virtuális hálózatok kiterjedése kisebb lesz, azaz kevesebb virtuális szakaszt fognak használni. Nagyobb hálózatok nagyobb számítási kapacitást igényelnek, ezekben az esetekben heurisztikával kellene gyorsítani az eljárást. A virtuális hálózat szintű védelem bonyolultabb probléma, mint az összeköttetés szintű, viszont teljes virtuális hálózatra fejti ki a védelmet. Kétszer annyi kapacitást igényel, mint az összeköttetés szintű védelem, ami kétszer annyit igényel, mint a védelem nélküli. Az él-, illetve csomópontfüggetlen védelem különböző fokozatú hibák ellen nyújt védelmet. Az eredményekre alapozva egy távközlési szolgáltató választhat a különböző védelmi módszerek közül, ami saját maga és felhasználói számára a legelőnyösebb.

Irodalom

1. Ibrahim Khalil–Torsten Braun: Edge Provisioning and Fairness in VPN-Diffserv Networks, The 9th International Conference on Computer Communication and Network (ICCCN 2000), October 16–18., 2000, Las Vegas, USA.
2. Martin Oellrich: Minimum-Cost Disjoint Virtual Private Networks under Edge Dependences, Boca 2000 – Fifth INFORMS Telecommunications Conference, March 5–8., 2000, Boca Raton, Florida
3. Rahul Garg–Huzur Saran: Fair Bandwidth Sharing Among Virtual Networks: A Capacity Resizing Approach, INFOCOM 2000, Tel-Aviv
4. D. Mitra and K. G. Ramakrishnan: A Case Study of Multiservice, Multipriority Traffic Engineering Design for Data Networks, Proc. IEEE GLOBECOM 99, pp. 1077–1083, Dec. 1999
5. D. Mitra–J. A. Morrison and K. G. Ramakrishnan: Optimization and Design of Network Routing using Refined Asymptotic Approximations, Performance Evaluation, vol. 36–37, pp. 267–288, 1999
6. D. Mitra–J. A. Morrison and K. G. Ramakrishnan: Virtual Private Networks: Joint Resource Allocation and Routing Design, Proc. IEEE INFOCOM 99

7. N. Anerousis: „Dynamic Virtual Private Network Dimensioning in Cost-Sensitive Environments", IEEE Globecom, Rio de Janeiro, Brazil, December 1999
8. B. Davie–Y. Rekhter: MPLS – Technology and Applications, Academic Press, 2000
9. I. Pepelnjak–J. Guichard: MPLS and VPN Architectures, Cisco Press
10. ILOG CPLEX 6.5 Documentation
11. M. Maliosz–T. Cinkler: Optimizing Configuration of Virtual Private Networks, Polish-Czech-Hungarian Workshop on Circuit Theory, Signal Processing, and Telecommunication Networks, Budapest, Hungary, 14–17. September 2001

Hírek

A 700 főt foglalkoztató Ericsson Magyarország 450 fős K+F részlege a BME és az ELTE tőszomszédságába, a tervek szerint 2002 májusában az Info Parkba költözik.

Az Ericsson Magyarország munkatársai jelenleg több irodaépületben dolgoznak: a Laborc utcai központi irodaházban, a Bécsi út 269. szám alatti bérleményben, az Árpád fejedelem útja 79.-ben, valamint a Hungária krt. 162.-ben található Ericsson Oktatóközpontban.

A jövő májusban esedékes költözés két szempontból is fontos lépés az Ericsson Magyarország életében. Egyrészt azért, mert a város különböző pontjain dolgozó munkatársaink ettől kezdve két korszerű, munkájuk természetéhez alkalmazkodó, egymással jól kapcsolódó munkahelyre kerülnek. Másrészt a kutatás-fejlesztés fizikailag közelebb kerül az egyetemekhez.

❖ ❖ ❖

Jelenleg közel százezer diák tanul a hazai felsőoktatási intézmények valamelyikében. A magas szintű elméleti képzés mellett – az informatika terén különösen – elengedhetetlen a naprakész gyakorlati ismeretek megszerzése, amivel a kikerülő diákok a munkaerőpiacon lényegesen jobb pozíciót szerezhetnek meg. Nagyrészt az anyagi erőforrások hiánya következtében a különféle ügyviteli és egyéb rendszerek beillesztése az oktatási programokba ma még viszonylag gyermekcipőben jár, így különösen figyelemre méltók azok a sikeres kezdeményezések, amelyek megteremtik a feltételeit a minőségi oktatásnak.

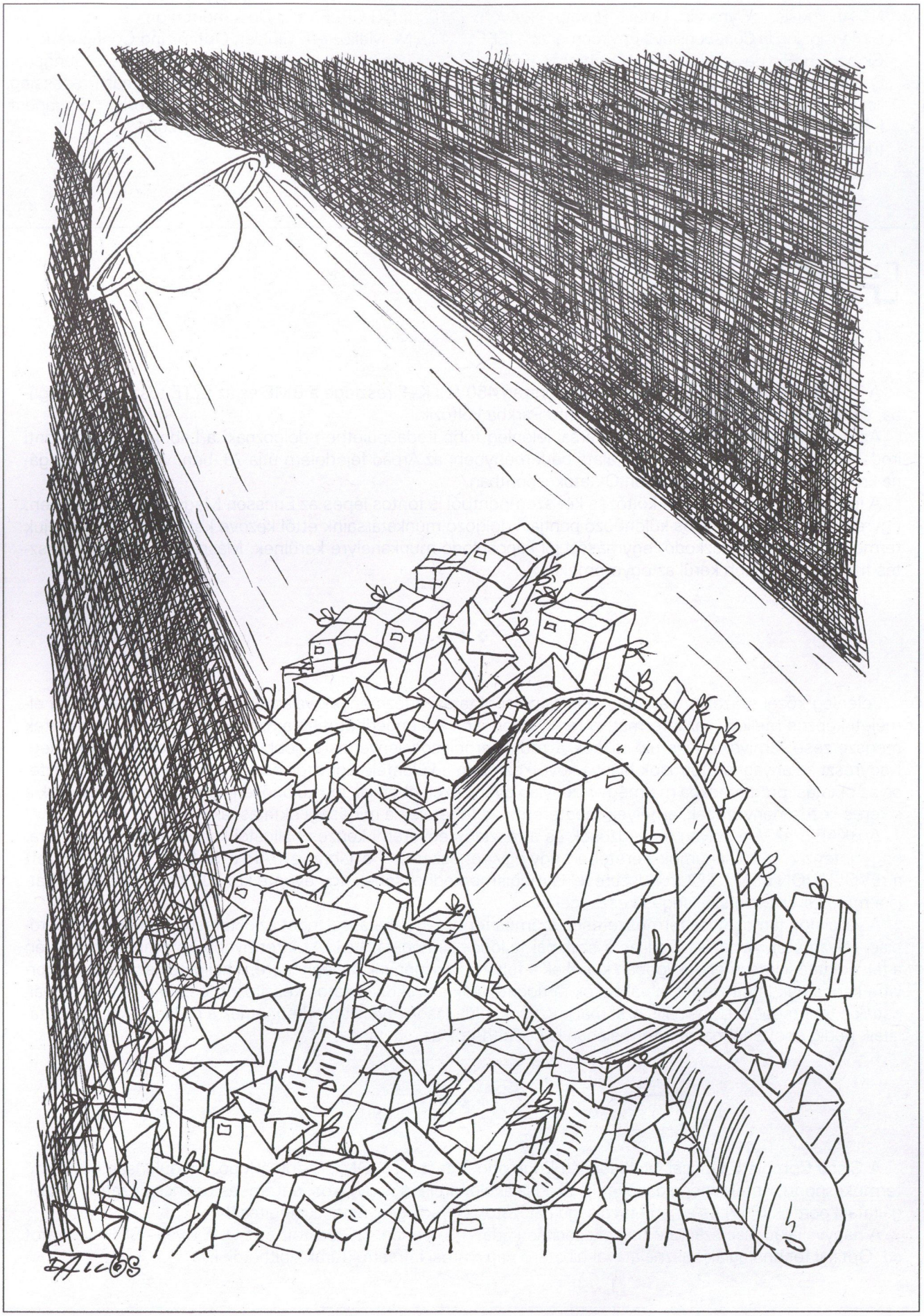
A BKÁE-n az V. évfolyamos végzősök és a részidős egyetemi képzés hallgatói kapnak lehetőséget arra, hogy intenzív szemináriumok keretében egy-egy rendszerrel – a Libra, a SAP, a SAS és a Scala mellett a rEVOLUTION ZENIT SQL rendszerével is megismerkedhessenek. Így évente kb. 700 hallgató elsajátíthatja a munkaerőpiacon szükséges készségeket.

A vállalatok támogatása természetesen számos területen jó hatással lehet az oktatásra, főleg a munkaerőpiaci folyamatok katalizálásával és a szakmai fejlődés támogatásával. Az intenzívebb kommunikáció révén a felsőoktatási intézmények jobban képesek a feltárt piaci igények kielégítésére, a hallgatók szakmai gyakorlatra kaphatnak lehetőséget, a vállalatok támogathatják a szakdolgozatok készítését, ösztöndíjakkal motiválhatják a tehetségeket, speciális szakmai kurzusok, előadások révén ismerkedhetnek a hallgatókkal, tapasztalataik pedig esettanulmányok formájában is beépíthetők az oktatásba.

❖ ❖ ❖

A Cisco Complete Optical Multiservice Edge and Transport (COMET) egy átfogó, modulárisan bővíthető termékcsoport, amely megoldásokat kínál a kialakulóban levő nagyvárosi perem- és gerinchálózatok, a szolgáltatási pontok (PoP) és a nagy távolságú hálózatok egyedi igényeinek kielégítéséhez.

A nagyvállalati piac számára nagy kapacitású adat-, illetve tárolóhálózatot, és SONET vagy SDH hálózatot ad. Optikai technológiák használatával hibatűrő nagyvárosi infrastruktúrák építhetők ki.



Tájkép csata után

BŐGEL GYÖRGY

stratégiai tanácsadó
KFKI Számítástechnikai Rt.

A tőkés gazdaság fejlődését kezdettől fogva a ciklikusság jellemezte: a fellendülések és a hanyatlások ritmikusan váltották egymást. A 2001. év végén ismét recesszió van, ami önmagában nem meglepő, a mögöttünk álló évtized fellendülésének, majd az új évezred legelején bekövetkezett visszaesésnek azonban van néhány, a távközlési és az informatikai szektorhoz kötődő érdekessége is.

Vissza a klasszikusokhoz

Joseph Alois Schumpeter a XX. század első felének kiváló közgazdásza volt. Több könyvet is írt, de ezek közül talán a *gazdasági ciklusokról* szóló a legismertebb és a legnépszerűbb.

Schumpeter szerint a gazdaság nagy ciklusai a nagy *innovációk* okozta „kreatív rombolásra" vezethetők vissza. A „rombolás" szó egy korszak végét jelzi, a „kreatív" pedig azt, hogy a régi helyett valami új születik. Nagyjából az 1780-as évektől kezdődően a textilipar, a vasgyártás és a gőzgép jelentették a „kreativitást". A technikai innovációk nyomán egész iparágak újultak meg, a technikai változásokat pedig mélyreható társadalmi átalakulások kísérték. A XIX. század közepén az acélgyártás és a vasútépítés korszaka következett, a vaspályák rövidesen behálózták az egész civilizált világot. A XX. század az elektromosság és a robbanómotor jegyében indult, ekkor ringott a mai legismertebb autóipari óriások bölcsője is; velük jött Taylor és a fordizmus, a modern tömegtermelés és gyárszervezés, ekkor kezdték összefoglalni a vállalatvezetés jórészt ma is használatos szabályait és módszereit. Az ötvenes években beköszöntött a petrolkémia, az elek-tronika, a számítástechnika és a repülés korszaka: a boltokat elárasztották a műanyagból készült termékek, tömegcikk lett a televízióból, gépesítették a háztartásokat, hétköznapi közlekedési móddá vált a repülés.

Schumpeter megfigyelése szerint az innovációs ciklusok első szakaszára az új iparágak *felfutása* a jellemző. A technikai újításokat meglovagolva tömegével születnek az új vállalkozások, a gazdaság gyorsan növekszik, az új technológia képviselői nagy nyereségre tesznek szert. A második szakaszban *tetőzik* a ciklus: a piac beérik, a kereslet stabilizálódik, sok új vállalkozás már nem jelenik meg a porondon, a verseny viszont egyre jobban kiéleződik, a gyengék elhullanak; a piac konszolidálódik és néhány nagy játékos kezébe kerül. A tetőzés után a *hanyatlás* következik: új technológiák születnek, amelyek új igényeket gerjesztenek; új piacokon, új iparágakban indul meg a nyüzsgés, a régiek pedig a „kreatív rombolás" hatására visszaesnek; a váltani nem tudó régi cégek pozíciója gyengül, sokan örökre eltűnnek közülük.

Tegyünk még valamit hozzá a ciklusok leírásához. Ha alaposabban tanulmányozzuk az időbeli lefutásukat, láthatjuk, hogy rövidülnek: két évszázaddal ezelőtt akár 50 évig is várni kellett, a modern kor innovációs ciklusainak azonban jóval rövidebb idő is elegendő, egyszóval – ahogy azt sokan állítják – a világ gyorsul.

Ha Schumpeternek igaza van, az elmúlt évtizedben egy ilyen *innovációs ciklust* élhettünk át, annak minden jellemzőjével és tünetével. Ez a tíz év az informatikáé, a távközlésé és az interneté volt: ezekben az ágazatokban született a legtöbb innováció, ezek növekedése volt a leggyorsabb, ők szívták fel a rendelkezésre álló munkaerőt. Ha egy kicsit közelebb megyünk a képhez, láthatjuk a részleteket is: e periódusban három „technológiai boom" követte egymást, és rakódott egymásra. Az első a távközlés deregulációjához kapcsolódott, a hatása hosszú távú. A második a 2000. év mesterségesen gerjesztett problémája volt, ami 1998–99-ben időleges keresleti csúcsot idézett elő az informatikai piacon. A harmadik „internetes lufi" néven került be a gazdaságtörténetbe: a tőzsdei léggömb 1995-ben kezdett felfúvódni, amikor a Netscape-et kivitték a börzére, és aki reggel bevásárolt a papírokból, az estére gazdag embernek mondhatta magát.

A három „boom" alatt folyamatosan működtek az elektronikus világ közismert törvényei: azok például, amelyek a csipek és a tárolók kapacitásának gyors ütemű növekedését jósolják, vagy a hálózati gazdaság exponenciális növekedési jelenségeit igyekeznek magyarázni.

Majd 2000-ben bekövetkezett a nagy kiábrándulás, az árfolyamok lezuhantak, egy csomó dotcom cég csődbe ment, a nagy távközlési és informatikai vállalatok egymás után jelezték, hogy mutatóik romlani fognak, keresleti előrejelzéseik nem jönnek be, nyereségterveiket nem tudják teljesíteni.

Pozitív és negatív spirál

A *felfutás,* majd az azt követő *konszolidáció* jól követte Schumpeter leírását. A kilencvenes évek „hosszú fellendülését" (az amerikai gazdaságban az utolsó recesszió 1991–92 körül volt) egyfajta pozitív spirálként is leírhatjuk, amelynek kiindulópontja a technológia fejlődése. A gazdaság egyéb szektorai élénk érdeklődést mutattak az informatika és a távközlés újdonságai iránt: a statisztikákból jól látható, hogy a vállalati beruházásokat az információtechnológiai bevásárlások uralták. Ez szép jövedelmet hozott a szállítóknak és a hozzájuk kapcsolódó integrátor-tanácsadó-szolgáltató holdudvarnak. A munkanélküliség csökkent (főleg az Egyesült Államokban), a vállalatok és az emberek egyaránt jól kerestek. A jövedelmek befektetési lehetőségek után kutatva megjelentek a tőkepiacon, jelentős részben kockázati tőke formájában; ez utóbbi növekedési grafikonja 1995-től kezdődően feltűnően meredek. A tőkepiac természetesen már elektronizált, a tranzakciók rendkívül gyorsak: a befektetők reggel vesznek, délután eladnak; a cél a gyors meggazdagodás, és nem az, hogy néhány biztonságos, jó részvényt hagyjunk örökbe az unokáknak.

Az árfolyamokat figyelő átlagpolgár egyre gazdagabbnak érezte magát, egyre nagyobb kosárral indult bevásárolni, a biztos jövő reményében az eladósodástól sem riadt vissza. Egy egész generáció nőtt fel abban a tudatban, hogy ha jól tanul, nem lesznek állásgondjai, az áruházak pedig tárt karokkal várják, és hitelkártyával mindent ki lehet fizetni. Ez a generáció a fejlett országokban már számítógép mellett nőtt fel, sokan előbb tanultak meg billentyűzeten dolgozni, mint tollal írni. Fiatalok és idősebbek egyaránt gond nélkül költekeztek, amivel tovább gerjesztették a gazdaságot.

A szárnyaló tőzsde óriási vonzerőt jelentett. A *meggazdagodás receptje* a következőképpen hangzott: alapíts egy csúcstechnológiai céget, szerezz hozzá kockázati tőkét, ígérj a munkatársaidnak részvényvásárlási opciókat; aztán kis idő múltán vidd ki az egészet a tőzsdére, következzen a nyilvános részvénykibocsátás; a brókerek világgá kürtölik, hogy íme, itt egy új, különleges vállalkozás, most tessék vásárolni, mert holnap már nem lesz, minden el fog kelni pillanatok alatt. Az sem baj, ha a cég terveiben még hosszú időre veszteség szerepel: üzleti tervre tulajdonképpen nincs is szükség, a hagyományos gazdaságossági számítások elavultak; a legfontosabb dolog elsőnek lenni a piacon, nagy piaci részesedést szerezni, gyorsan növekedni, a nyereség pedig majd megjön magától. A tülekedés óriási, a lehetőségeket meg kell ragadni, el kell halászni a többiek orra elől, kerül, amibe kerül.

A nyereség néha megjött, sokszor viszont nem. A gombamód szaporodó internetes cégek (az „új gazdaság" legismertebb képviselői) közül feltűnően sokan soha nem termeltek semmiféle nyereséget, sőt, üzleti modelljük alapján erre esélyük sem volt. A befektetők türelme egy idő után elfogyott, az árfolyamok egyik napról a másikra esni kezdtek, a korábbi nagy piaci értékek elolvadtak. A pozitív spirál negatívba váltott át, majd végül recesszióba torkollt.

Az infokommunikációs szektor egyre határozottabban felöltötte Schumpeter cikluselmélete *telítődési* szakaszának jegyeit. A fejlett országok távközlési piacán általánossá vált a túlkínálat, a fellendülés idején kiépített kapacitások kihasználatlanok maradtak, az óriási, gyakran hitelből finanszírozott technikai és koncessziószerzési befektetések nem térültek meg. A telefontársaságok beruházási kereslete látványosan visszaesett, ami persze rosszul érintette a berendezések gyártóit és közvetítőit, akik a korábbi szép időkre alapozva alakították ki a kapacitásaikat, és akiknél most eladatlan árukészletek halmozódtak fel. A csődbe ment internetes cégek felszámolói árulni kezdték a használt, vagy használatba sem vett eszközöket. Az ellátási dominósorok borulni kezdtek.

A számítógépek gyártói megtapasztalták, milyen az, amikor egy korábbi piacvezető termék *tömegcikké* válik. Az asztali gépek nyereséghányada napról napra kisebb lett, állandó költségcsökkentési kényszert idézve elő, a piac növekedése pedig megállt, sőt, az Egyesült Államokban az eladások visszaestek. Ugyanez történt a mobiltelefonokkal is, a harmadik generációs rendszerek terjedése lényegesen lassúbb a vártnál. A kockázati tőke forrásai jóval szerényebben bugyognak a korábbinál.

A recesszió közeledtével elsőként a vállalatok fogták vissza beruházási kiadásaikat. Informatikai vonalon – ahogy a nagy könyvben meg van írva – először a hardverbeszerzéseket csökkentették. Időnként szélsőséges hangok is megszólalnak, amelyek szerint az informatika ablakon kidobott pénz, az internet pedig egyszerűen kimegy a divatból. Mindenesetre kétségtelen tény, hogy 2001-ben a nyereségesség és növekedés tekintetében néhány hagyományos iparág – például olajipar, gyógyszeripar, üdítőitalok – vezető képviselői sokkal jobban állnak, mint az „új gazdaság" számos vezérhajója.

A gazdasági elemzők érdekes módon a legtöbbet talán a fogyasztók magatartásával foglalkoznak. Ők ugyanis egy darabig változatlan lendülettel költekeztek tovább, az elmúlt tíz év általános fellendülése bizonyára mély nyomokat hagyott bennük. Amikor ez a cikk készült, mindenki arra volt kíváncsi, vajon milyen lesz a karácsonyi forgalom, visszazökken-e a fogyasztói bizalom a normális kerékvágásba. A mérséklődő fogyasztási kedv keresletkiesést jelent a vállalatoknak, azok ennek hatására leépítésekbe kezdenek, a növekvő munkanélküliség negatívan hat a fogyasztásra – a negatív spirál beindul.

A helyzet értékelésénél nem szabad megfeledkeznünk a szeptember 11-i New York-i terrortámadásról sem. Ha valaki ránéz az amerikai GDP alakulását mutató statisztikákra, jól láthatja, hogy az amerikai recessziót nem a felhőkarcolókba becsapódó repülőgépek idézték elő: a 2001. év második negyedévében már csak néhány tizedszázalékos volt a növekedés, ami aztán a harmadik negyedévben csökkenésbe csapott át. A politikai feszültségek azonban károsan hatnak a gazdasági együttműködésre, a növekvő katonai és más biztonsági kiadások erőforrásokat vonhatnak el más területekről, bár távlatban a honvédelmi fejlesztések fellendíthetik a polgári piacot is. Azok, miután az új technológiák már nem titkosak, új üzletágak kifejlődését segítik.

Időközben azt is meg kellett tanulnunk, hogy a gazdaság valóban *globalizálódott*. A közgazdászok még bizonyára sokat fognak vitatkozni arról, hogy a mostani recessziónak milyen különleges sajátosságai vannak, mennyiben különbözik az előbbiektől. Egy fontos jellemzője mindenesetre van: a világ három nagy gazdasági központjában, az Egyesült Államokban, Japánban és Nyugat-Európában egyszerre következett be. Egyszerre, de nem azonos okból: Amerikában az individualista, ambiciózus vállalkozói kultúra alapjain túlfűtött várakozások vezettek a tőzsde kipukkanásához, Japánban és Nyugat-Európában viszont az alkalmazkodás lassúsága okoz nehézségeket, a biztonság vágya áll szemben a változás kényszerével.

A *japánok* egyes szektorokban (pl. mezőgazdaság, lakás, egészségügy, kiskereskedelmi vállalkozások) változatlanul korlátozzák a versenyt, a munkaerőpiac merev, a kormányzati szektor összefonódik a vállalatokkal, a vállalatok összefonódnak a bankokkal; a csoportlojalitásnak vannak előnyei, de a „kreatív rombolás" időszakában a hátrányai is kiütköznek.

Nyugat-Európában a sűrű szövésű szociális háló akadályozza a hanyatló szektorok leépítését és új munkahelyek teremtését. A béreket terhelő magas adók drágává teszik a toborzást, a bőkezű ellátásban részesülő munkanélküliek nem igyekeznek minél előbb álláshoz jutni. Belgiumban, Franciaországban, Németországban, Ausztriában a 15 és 64 életév közöttiek mintegy fele kap különböző címeken valamilyen kormányzati támogatást.

A kiterjedt kereskedelmi kapcsolatok miatt a világ nagyon érzékeny lett az amerikai gazdaság ingadozásaira. Amíg az USA mozdonya meghúzta az egész világgazdaságot, a másik két nagy központ is jól teljesített. Most azonban éppen fordított a helyzet. A Világbank 1,3%-os általános gazdasági növekedést jósol 2001-re, és 1,6-et 2002-re. Ilyen rossz mutatószámok csak 1982-ben és 1991-ben voltak.

Milyen lesz a fellendülés?

2001 decemberében már nem az a kérdés, hogy lesz-e recesszió, hanem hogy mikor lesz vége – eddig mindegyik befejeződött egyszer –, és milyen lesz a fellendülés. Térjünk vissza ismét *Schumpeterhez*. Ha a neves tudósnak igaza van, és valóban lefutott egy technológiai ciklus fellendülési és tetőzési szakasza, akkor most ismét a kreatív rombolásnak kell következnie: fel kell bukkanniuk azoknak az innovációknak, amelyek élvonalba repítenek egyes iparágakat, és ezek majd meghúzzák a gazdaságot, miközben leszorítanak másokat a porondról. De vajon melyek lesznek ezek az innovációk, és mely iparágak lesznek a következő időszak mozdonyai? E tekintetben a helyzet még többesélyes, a képnek még tisztulnia kell, egyértelmű jövendölések helyett egyelőre jobb forgatókönyvekben gondolkodni.

A tapasztalatok azt mutatják, hogy az a szektor, amely a fellendülés motorja volt az egyik ciklusban, általában gyengébb teljesítményt mutat a következőben. A jövendőmondás hüvelykujjszabálya a következőképpen szól: ha tudni akarod, kik fogják vezetni a következő fellendülést, nézd meg, hogy kik teljesítettek legjobban a megelőző hanyatlás idején. Ha elfogadjuk ezt a gondolkodást, akkor leginkább a *biotechnológiát* és az *egészségügyi* szektort jósolhatjuk befutónak: a szektor vezető szervezetei, innovátorai a mostani recesszió idején is szép eredményeket tudnak felmutatni. A genetika fejlődése új alapokra helyezheti a diagnosztikát és a gyógyszergyártást, Amerikában a menedzselt egészségügyi szolgáltatások környékén igencsak pezseg az élet. Az előző két recesszió idején az egészségügyi kiadások növekedése erősen lelassult, most viszont egészen mást mutatnak a statisztikák. (Emlékeztetőül: az 1990–91-es hanyatlás idején az információs szektor mutatott hasonló erényeket, a hozzá kapcsolódó vállalati beruházások alig csökkentek.) Az egészségügyi szektor által vezérelt fellendülésnek – mint egy lehetséges forgatókönyvnek – érdekes következményei lehetnek. Az információs ipar közvetlen hatást gyakorol a termelékenységre – ezzel szemben az egészségügy fejlődése a várható élettartamot hosszabbítja meg, és az élet minőségének javulásához járul hozzá, ráadásul a kapcsolódó kiadások nagy része felett a kormányzat rendelkezik.

Az infokommunikációs szektor egyelőre – 2001 végén – a gyengélkedés jeleit mutatja. A hivatalos statisztikák szerint az információtechnológiai berendezésekre vonatkozó új megrendelések nagysága az Egyesült Államokban a 2000. júniusi 40 milliárd dollárról 2001 szeptemberére 24 milliárd alá csökkent. A félvezetők gyártásához szükséges berendezések iránti kereslet 2001 harmadik negyedévében további 12%-kal esett vissza. A távközlési ipar lendületét tartósan fékezik a kihasználatlan kapacitások.

Vannak olyan vélemények, amelyek szerint a kilencvenes évtized az infokommunikációs szektoré volt – és a következő is azé lesz. Vezető szerepe megmarad, legfeljebb átalakul egy kissé. Az információs technológiában még rengeteg fejlődési potenciál van, a „kreatív rombolás" e szektoron belül fog lezajlani. A csipek kapacitása még hosszú évekig növekedni fog, ahogy azt Gordon Moore megjósolta, és a merevlemezes tárolók kapacitása is nagyjából évente megduplázódik. A mobil korszaknak még csak a küszöbénél tartunk, a nagy újítá-

sok még csak most következnek. A mobilitás rengeteg új szolgáltatást hoz majd magával, és az internet használatát tekintve is még csak az elemi iskolába járunk.

Bizonyos értelemben a recesszió is az infokommunikációs szektornak dolgozik. Vessünk egy pillantást a termelékenység alakulását mutató amerikai táblázatra. Ebből arra a figyelemre méltó következtetésre juthatunk, hogy míg a korábbi recessziók idején a termelékenység csökkent, addig a 2001. év első két recessziós negyedévében szépen növekedett.

RECESSZIÓ		FELLENDÜLÉS	
1973–75	0,2%	1975–80	1,6%
1980	-1,2%	1980–81	2,1%
1981–82	-0,2%	1982–90	1,8%
1990–91	-0,6%	1991–2001	2,1%
2001	**2,4%**		

1. táblázat Az üzleti szervezetek termelékenységének növekedési rátája (USA, a farmgazdaságok nélkül)

Recesszió idején a vállalatok legtermészetesebb reakciója a *takarékoskodás*. A legutóbbi (1990–91-es) visszaesés idején a vállalatok nagyarányú elbocsátásokba kezdtek, és az infláció alatt tartották a bérek növekedését. A bérköltségek tekintetében még a nehéz idők elmúltával is szorosan fogták a gyeplőt mindaddig, amíg egészséges nyereség nem mutatkozott a könyvekben. A recesszió 1991 márciusában véget ért, de Amerikában a munkanélküliség még 15 hónapig emelkedett, a reálbérek pedig egészen 1995-ig csökkentek. Nem csoda, hogy a kilencvenes évek első felének nagy menedzsmentslágere az üzleti folyamatok radikális újraszervezése, a Business Process Reengineering volt.

Valószínű, hogy a minden bizonnyal előttünk álló fellendülés idején hasonló jelenségnek lehetünk tanúi. A profitjuk után futó vállalatok óvatosan bánnak majd a toborzással és a bérekkel, és mindent elkövetnek a *termelékenység* további növelése érdekében. Eközben egyre kreatívabb módon hasznosítják majd az infokommunikációs eszközöket. Az „új gazdaság" erőre kap, de nem a „régi gazdaság" mellett, hanem abba beágyazva. Számos példa mutatja, hogy miközben kipukkant a dotcom-léggömb, az informatikai és távközlési cégek gyengélkednek, a „régi gazdaság" egyes képviselői (az úgynevezett „tégla-és-habarcs" vállalatok) sokszor különösebb felhajtás és látványosságok nélkül igen jó eredményeket érnek el az elektronizálás terén: gyorsítják és áramvonalasítják a folyamataikat, javítják az ügyfeleik kiszolgálását, automatizálják az irodai munkát, okosabban gazdálkodnak a tudástőkéjükkel, e-business megoldásokkal mozgósítják a tartalékokat az ellátási láncaikban, logisztikai rendszereikben. Információtechnológiai kiadásaikat a recesszió miatt egyelőre visszafogták, de ha a nyereségük ismét emelkedni kezd, a megrendelések is szaporodásnak indulnak. (A növekvő munkanélküliség persze fejfájást okozhat a kormányzatoknak, a lemaradó bérek miatt kieső keresletet valahogyan pótolni kell.)

Termelékenységi verseny

Lehetséges tehát, hogy az infokommunikációs szektor az elkövetkező fellendülésben nem fog olyan vezető szerepet játszani, mint a mögöttünk álló „long boom" idején, de fontos tényező lesz a vezériparágak fejlődésében, a termelékenység általános növelésében. Ne feledjük például, hogy a modern biológia, a genetika, a menedzselt egészségügyi ellátás semmire se menne fejlett informatikai megoldások nélkül. Legjobb esélyeik azoknak a technikai eszközöknek és alkalmazásoknak vannak, amelyek *költségcsökkentő*, *hatékonyságnövelő* hatása gyorsan és közvetlenül érzékelhető, vagy legalábbis az alkalmazók bíznak e képességeikben. Beigazolódhat az a tétel, hogy ami technikailag lehetséges, és van hozzá gazdasági kényszer, annak előbb-utóbb meg kell valósulnia. Ettől az impulzustól kaphat újabb lendületet például az *outsourcing*-hullám: a vezető piaci elemzők mind azt jósolják, hogy a kiszervezési akciókból származó jövedelmek határozottan növekedni fognak az informatikai szektorban. Erre várnak azok az országok – köztük első helyen India, de valljuk be, mi is –, amelyek úgy gondolják, hogy a recesszió nekik dolgozik, hiszen a fejlett országok költségcsökkentésre kényszerített cégei a képzett, de olcsó munkaerővel rendelkező vidékekre fogják kiszervezni távolról is végezhető tevékenységeik egész sorát.

Mindezek következményeképpen sajátos termelékenységi verseny bontakozhat ki a három nagy gazdasági centrum között. A legjobb esélyei Amerikának vannak: a vállalati racionalizálásnak nincs akadálya, a munkaerő mobil, a munkanélküliek ellátása nem túlságosan bőkezű, és a szabadalmi statisztikák szerint az újítási kedv egyáltalán nem mérséklődött. Nyugat-Európa és Japán fölött viszont egyre többen kongatják a vészharangot – az okokat fentebb már elemeztük.

Érdekes kérdés, hogy a termelékenység növekedéséből (és az alapját jelentő technikai fejlődésből) kik és milyen arányban fognak profitálni. A dotcom-korszakban megtanultuk, hogy ahol élénk a verseny és alacsonyak a belépési korlátok, a konkurenciaharc gyorsan lefelé nyomja a nyereséghányadokat, és a végső felhasználó, a fogyasztó lesz az, aki igazából nyerni fog. Újabb tanulság: az infokommunikációs technológiát lehetőleg *tartós versenyelőnyök* megszerzésére, védhető pozíciók kiépítésére kell felhasználni. Kérdés, hogy sikerül-e ez a következő fellendülés zászlóshajóinak.

Internetkapcsolatok minősége BellResearch

ANDRÁSI TAMÁS

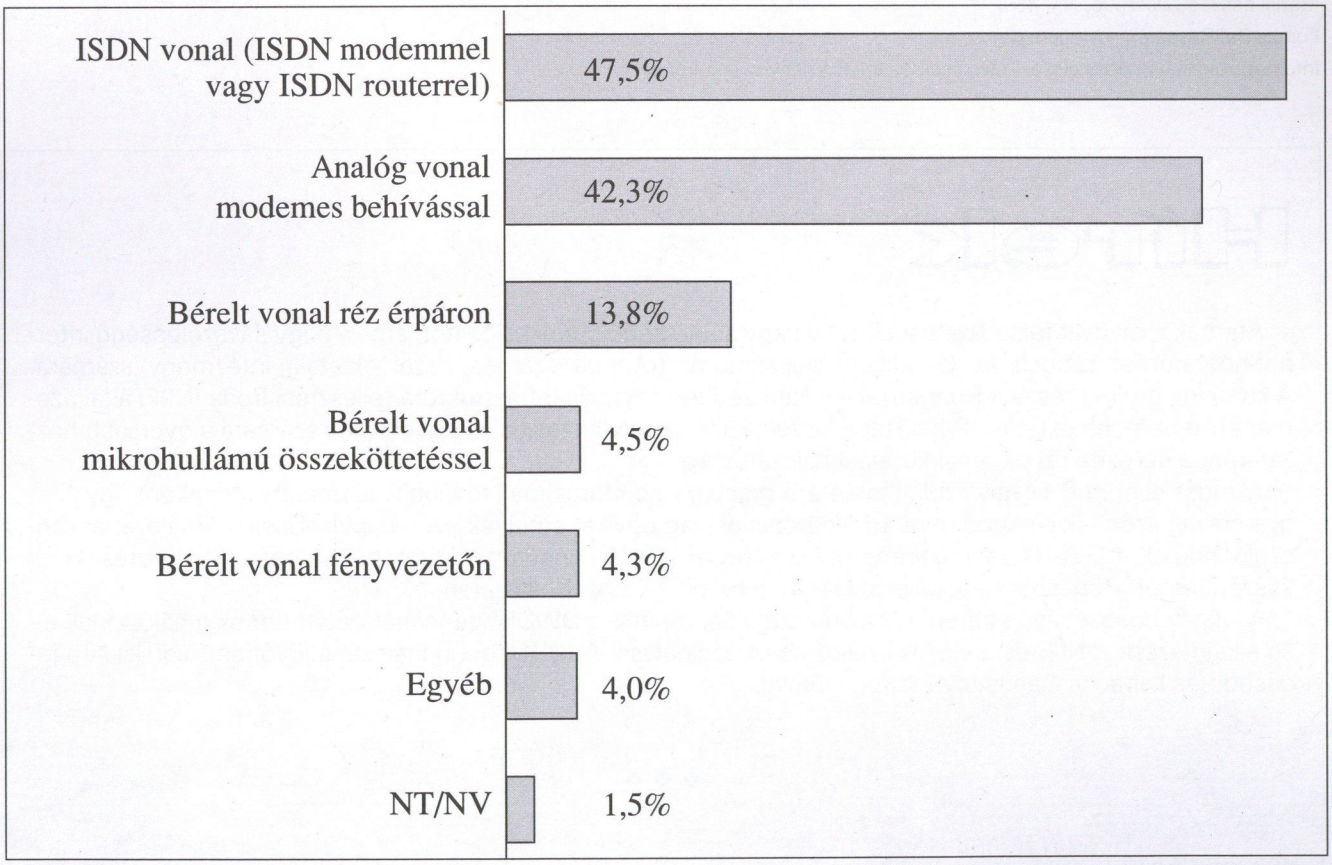
üzletfejlesztési igazgató
BellResearch

Már az ISDN a vezető hozzáférési mód

A hazai közép- és nagyvállalatok körében már az ISDN a legelterjedtebb kapcsolási mód a BellResearch és a Modem Kor legutóbbi közös felmérése szerint.

Míg a vállalatok 42%-a analóg vonalon, modemes behívással kapcsolódik a világhálóhoz, addig az ISDN vonalon keresztüli internet-hozzáférési móddal már közel minden második cégnél találkozhatunk [48%]. A bérelt vonali hozzáférés aránya (réz érpáron, vagy mikrohullámú összeköttetésen keresztül) a vállalatok egynegyedére jellemző [23%], amelyhez hozzájárult az idei évben a szolgáltatók között kibontakozott árverseny.

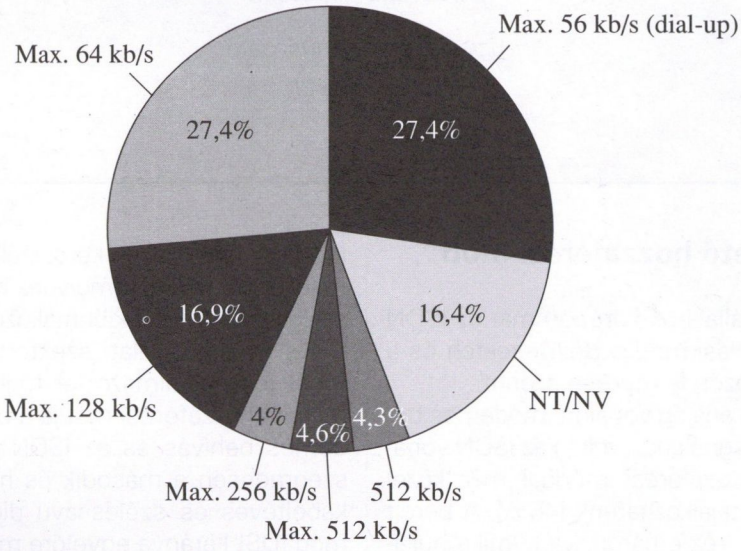
Ha a nagyvállalati szektort külön vizsgáljuk, a 300 főnél több alkalmazottat foglalkoztató társaságok domináns hozzáférési módja a bérelt vonal [60%]. A modemes behívás és az ISDN kapcsolat a nagyvállalati szegmensen a második és harmadik helyre szorul. A kábeltévés és szélessávú digitális vonali hozzáférési mód [DSL] aránya egyelőre még elhanyagolható [3%].



Az 50 fő fölötti vállalkozások internet-hozzáférési módjai (Bázis: összes válaszadó, N = 459)
Forrás: BellResearch – Modern Kor /
Internetszolgáltatók értékelése – elvárások és teljesítmény c. tanulmány

A kapcsolatok 30%-a már 64 kb/s feletti

Az 50 fő feletti internet-hozzáféréssel rendelkező vállalkozások 27%-ának maximális internetkapcsolati sávszélessége 56 kb/s, ami lényegesen alacsonyabb a hagyományos kapcsolt vonali hozzáféréssel rendelkezők arányánál, amely arról tanúskodik, hogy a cégeknél párhuzamosan jelennek meg a fejlettebb kapcsolási módok. A nagyvállalati szegmensben a cégek kétötöde [42%-a] már 64 kb/s feletti sebességgel internetezik, míg ez az arány a középvállalatoknál csak 27%.



Az 50 fő fölötti vállalkozások megoszlása az internetkapcsolat sávszélessége alapján
(Bázis: összes válaszadó, N = 459)
Forrás: BellResearch – Modern Kor /
Internetszolgáltatók értékelése – elvárások és teljesítmény c. tanulmány

Hírek

Átadták a magyar felsőoktatásnak azt a nagy sebességű gerinchálózatot, amely nagy sávszélességű internet-hozzáférést biztosít az Oktatási Minisztérium, továbbá számos hazai oktatási intézmény számára. A komplex projekt része a Hungarnet – a Nemzeti Információs Infrastruktúra-fejlesztési Iroda (NIIF) által üzemeltetett nemzeti oktatási IP-hálózat – kiszolgálása, amely biztosítja az egyetemek számára a gyorsabb hozzáférést a nemzetközi oktatási-kutatási hálózatokhoz.

A most elindított Matáv-szolgáltatás 2,5 gigabit/s adatforgalmat továbbít összeköttetésenként, így Magyarország azon – kevesebb mint 10 – európai ország egyike, amelyek ilyen nagy sebességű hálózattal kapcsolódhatnak a GEANT rendszerébe, 27 országot felölelő páneurópai kutatóhálózathoz. A fejlesztéseknek köszönhetően Budapest regionális szerepet is betölt a GEANT hálózatán.

A Matáv hosszú távú stratégiájának megfelelően építi ki a DWDM gerinchálózatát. Ennek a hálózatnak első alkalmazása a NIIF és a GEANT hálózatok kiszolgálása. A WDM gerinchálózat a jövőben földrajzi kiterjedésben és kapacitásban is tovább fog bővülni.

❖ ❖ ❖

A Cisco Systems az optika, a csomagkezelés, a protokollok és a szolgáltatásbiztosításra alapozva fejlesztette ki a COMET portfóliót, amely biztosítja a hálózat kínálta új lehetőségek költséghatékony kihasználását. A COMET egy modulárisan bővíthető termékcsoport, amely a kialakulóban levő nagyvárosi perem- és gerinchálózatok, a szolgáltatási pontok (PoP) és a nagy távolságú hálózatok egyedi igényeit elégíti ki. A szolgáltatások teljes körének biztosítását teszi lehetővé.

Új eredmények az RSA-kulcsok megfejtéséhez

DÉNES TAMÁS

matematikus

A Ron Rivest, Adi Shamir és Len Adleman szerzőhármas az 1970-es évek közepén megalkotott egy titkosítási eljárást, melynek RSA elnevezése (neveik kezdőbetűiből), azóta ismertté vált az egész világon [1], [2]. Napjainkban az RSA-algoritmus szinte minden informatikai, számítógépes, kommunikációs rendszerben jelentős szerepet játszik, ahol a digitális adatok biztonságáról gondoskodni szeretnének. Ilyenek például az e-kereskedelem, az e-bank-rendszerek, ezzel biztosítják a webszerverek és a kliensek közti biztonságos kapcsolatot, az e-mailek hitelességét és titkosságát, ezt használják a távoli terminálokról bejelentkező felhasználók és az elektronikus hitelkártyás rendszerek.

Az első publikációk óta sok kutató, köztük maguk a szerzők is keresték az RSA-algoritmus gyenge pontjait. Az eltelt huszonöt év vizsgálódásai egy sor nagyon érdekes elméleti és gyakorlati támadási módszert eredményeztek, azonban eddig egyik sem oldotta meg az RSA általános megfejthetőségét, mivel a számítástechnika ezeket a támadásokat kompenzálta. Jelen dolgozat rámutat arra, hogy bár a támadások egyenként nem rendítik meg az RSA biztonságát, összességükben olyan arzenált képviselnek, amelyek szem előtt tartása óvatosságra int az RSA alkalmazásakor.

Itt mutatjuk be azokat a támadási lehetőségeket, amelyek nem az RSA-modulus faktorizációját célozzák, és amelyek érdekessége, hogy részben éppen annak a P. Fermatnak az eredményeiből vezethetők le, akinek a „kis Fermat-tételére" alap maga az RSA-algoritmus.

Az RSA titkosító algoritmus rövid összefoglalása

- Legyen N = pq, két nagy prímszám szorzata (n/2 bit hosszú mindkettő), ezt nevezzük RSA-modulusnak. Napjainkban N tipikus hosszúsága n = 1024 bit, ami 309 decimális jegyet jelent. A két prímtényező pedig 512 bit hosszú. Kezdetben az n = 128 bites modulus is biztonságosnak bizonyult, majd a támadások és a technika fejlődése hatására a biztonságot a számok nagyságának emelésével biztosították. Így lett az RSA-modulus hossza 256, 512, majd 1024 bit.
- Legyen továbbá e, d két egész szám úgy, hogy $ed \equiv 1$, ahol $\varphi(N) = (p-1)(q-1)$ e-t nyilvános (publikus) exponensnek, míg d-t privát (titkos) exponensnek nevezzük.
- Az (N,e) páros a publikus kulcs, amely mindenki számára hozzáférhető, ezzel titkosítják az üzeneteket.
- Az (N,d) páros pedig a privát vagy másképp a titkos kulcs, ezt csak a célszemély ismeri, és arra használja, hogy dekódolja a titkos üzeneteket.
- Az üzenetet minden korlátozás nélkül tekinthetjük egy egész számnak, jelöljük M-mel, amelyre teljesül, hogy $0<M<N$. Ha a tényleges üzenet ennél hosszabb, akkor úgynevezett blokkokra osztjuk, amelyek teljesítik e feltételt.
- A titkosított szöveg: $C = M^e \bmod N$.
- A dekódolt szöveg: $C = M^d \bmod N$, mivel az Euler-Fermat-tétel alapján: $C^d = M^{ed} = M \bmod N$

Az RSA egyirányú függvény, amely adott d esetén könnyen invertálható az előzők alapján, azonban a privát kulcs ismerete nélkül ez nagyon nehéz. Az RSA feltörése pontosan arra irányul, hogy d ismerete nélkül kell invertálni az RSA-függvényt. Pontosabban fogalmazva, ha csupán az (N, e, C) hármas adott, akkor képesek vagyunk-e az eredeti üzenetet, M-et előállítani?

Az RSA-támadások csoportosítása

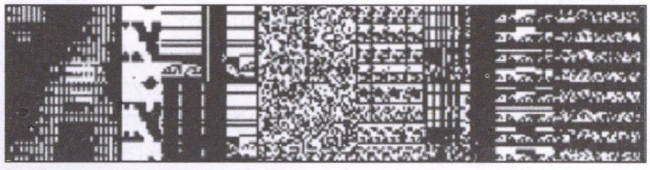
Implementációfüggő támadások

Az RSA-támadásoknak ez a típusa csak az adott helyzetben alkalmazható, viszont ott és akkor hatékony fegyvert ad a támadó kezébe. Ilyen támadási lehetőség például a tárolt kulcsok elleni támadás (a szerver azon területének behatárolása, amelyen a kulcsokat, akár kódolt formában, tárolják), vagy például a smartcardok számítási idejének és áramfelvételének időbeni mérésén alapuló támadás. Ezek a támadások már nem csupán elméleti megfontolásokat, hanem technikát is igényelnek.

Kulcskereséses támadás

Nicko van Sommeren és Adi Shamir [7] kidolgoztak egy olyan technikát, ami hatékony módszert ad a kulcsok memóriában való megkeresésére. A legtöbb al-

kalmazás ugyanis a szerver kulcsait a merevlemezen olyan fájlokban tárolja, amihez csak kevés felhasználónak van hozzáférési joga, sőt ezen felhasználók számára is olvashatatlan ez az állomány, mivel általában ez is titkosítva van. A célalkalmazás tudja csak olvasni és értelmezni, dekódolni a kulcsokat, viszont ahhoz a kulcsot ki kell bontania és ekkor a kulcs a rendszer memóriájában lesz kódolatlan formában. Ha a támadó eléri, hogy a rendszer összeomoljon, akkor valószínűleg ott lesz a memóriadumpban is kulcs, vagy ha hozzáfér a rendszer memóriájához, akkor is megszerezheti azokat. Viszont a feladat még így sem egyszerű, mivel egy-egy memóriadump több száz megabyte is lehet, a keresendő kulcs 1024 bites RSA-kulcsot feltételezve is csak néhány száz byte. A kulcsokat általában álvéletlenszám-generátorral generálják, így nagy entrópiájú adatokként detektálhatók a tárolóban. Tehát ha a keresés során olyan részadatokat találunk, melyeknek nagy az entrópiája, akkor azok jó eséllyel lehetnek a keresett kulcsok. Az 1. ábrán látható, hogy középen helyezkedik el a keresett kulcs.



1. ábra

Az RSA privát kulcsok keresésénél különösen jól alkalmazható ez az eljárás, hiszen nyilvános kulcsú titkosítás lévén, könnyen megszerezhetjük a publikus kulcsot. A modulus a privát kulcsban és a publikus kulcsban megegyezik, így tehát rendelkezünk a privát kulcs felével. Nicko van Sommeren egy webszerveren mutatta be a támadást. Védekezésképpen be lehet vezetni néhány nagyon szigorú biztonsági intézkedést. Az igazi védekezés ez ellen a támadás ellen, ha a kulcsokat nem a rendszer memóriájában tároljuk, hanem egy úgynevezett hardver kripto egységen. Ezek alkalmazása elég költséges, viszont magas fokú biztonságot nyújtanak.

Számítási idő mérése

Napjainkban egyre inkább teret hódítanak a smartcardok és a smartcardokra épülő alkalmazások. A smartcardok képesek a privát kulcs tárolására és az RSA aláírási és titkosítási műveletek elvégzésére anélkül, hogy a privát kulcs kikerülne a kártyából. Kocher módszerének [8] köszönhetően mégis aránylag gyorsan megszerezhetjük a privát kulcsot. A támadás azon alapszik, hogy pontosan kimérjük, mennyi ideig tart a smartcardnak az RSA-dekódolás, vagy RSA-aláírás.

A támadás során a smartcardot arra használjuk, hogy generáljuk néhány véletlen üzenetnek a digitális aláírását, $M_1,...,M_k \in Z_N^*$ és rendre lemérjük, hogy az aktuális művelet elvégzése a smartcardnak mennyi időbe telik (T_i). Ezzel a módszerrel ki lehet nyomozni bitről bitre a d értéket. Legyen t_i az az idő, amit a kártya igénnyel az $M_i \cdot M_i^2 \bmod N$ számítás elvégzésére. Ezek a t_i-k különböznek egymástól, $M_i \cdot M_i^2$, mivel az egyszerű moduláris egyszerűsítés művelet számítási igénye függ a konkrét értéktől. Kocher azt állapította meg, hogy a két sorozat $\{t_i\}$ és $\{T_i\}$ korrelál egymással, ha $d_1 = 1$, ha viszont $d_1 = 0$, akkor a két sorozat $\{t_i\}$ és $\{T_i\}$ úgy viselkedik, mint két független valószínűségi változó.

Kochen egy ehhez hasonló támadási módszert is felvázolt, ezt „power cryptanalysis"-nak nevezte el. Azt figyelte meg, hogy a smartcard áramfelvétele nagyobb olyankor, mikor a nagy pontosságú szorzásokat végzi, mint általában. Így ha azt mérjük, hogy az aláírás generálása közben hogyan változik a kártya energiafelvétele, akkor az előzőhöz hasonló támadáshoz jutunk. Meg kell mérni a nagy áramfelvételű szakaszok hosszát. Ezen szakaszok hosszából megállapítható, hogy egy-egy iteráción belül a kártya egy vagy két szorzást végzett. Ezáltal megfejthető a privát kulcs.

Helytelen alkalmazáson alapuló támadások

A helytelen alkalmazás alatt azt kell érteni, hogy az RSA-algoritmus fentiekben ismertetett feltételei mellett a választható kulcsok száma elképzelhetetlenül nagy, azonban a feltörhetőség szempontjából nem mindegyik kulcs egyformán biztonságos. Egy példa a helytelen alkalmazásra, ha p és q ikerprímek, azaz $N=p(p+2)$, amelyből p pillanatok alatt kiszámítható, és ezzel egy időben megkapjuk N faktorizációját. Ez nagyon speciális eset, de nem elhanyagolható. Még számtalan alkalmazást találtak, amit nem tilt meg az RSA-algoritmus, viszont használatuk esetén igen széles biztonsági rések keletkeznek. Ilyen például a kis privát exponens használata, a közös modulusú üzenetek gyűjtése, vagy éppen a semleges üzenetek digitális aláírása. Az RSA körültekintő használata tehát kulcskérdés az üzenetek biztonsága szempontjából, mivel a matematika mai ismeretei szerint az RSA feltörhetetlensége elméletileg nem garantálható (ezt maguk a szerzők is elismerik).

Közös modulus

Néhány rendszer nem generál minden felhasználónak külön modulust, és ezzel sok számítást takarít meg. Rögzítenek egy $N = pq$ modulust és a központi Certificate Authority mindenkinek ezt a modulust osztja ki, és ehhez mindenkinek generál egy saját e és d értéket.

Az alábbi tétel szerint (melynek bizonyításától itt eltekintek) a privát kulcs leleplezése és N faktorizációja egyenértékű. Ezért nincs értelme elrejteni N faktorizációját azok elől, akik amúgy is ismerik a privát kulcsot.

Simmons tétele

Legyen (N, e) egy RSA nyilvános kulcs. Ha adott a privát kulcs d, akkor N faktorizációja hatékonyan elvégezhető. Ha N faktorizációja ismert, akkor hatékonyan kiszámítható d.

Így a rejtjelezett $C = M^{e_a} \bmod N$ üzenet nincs biztonságban, ha az A és B felhasználó ugyanazt a modulust

használja. Bár B nem rendelkezik a d_a-val (A privát exponense), ugyanakkor rendelkezik egy saját kulccsal, aminek ugyanaz a modulusa. A fenti tétel alapján a saját exponensei e_b, d_b segítségével faktorizálhatja N-t, majd N osztóinak birtokában könnyen kiszámíthatja A privát exponensét, d_a-t.

Kis privát exponens

Az alkalmazások egy részében, hogy gyorsabb legyen a dekódolás, véletlenszerű d privát exponens helyett inkább egy kis d-t választanak. Mivel a modulo hatványozás művelet igénye $\log_2 d$, ezért egy jól megválasztott d segítségével akár tízszeres gyorsítás is elérhető (pl. ha 1024 bit hosszú a modulus). Azonban az M. Wiener [2] által bizonyított alábbi tétel mutatja, hogy ha d egy magadott értéknél kisebb, akkor a kód megfejthetővé válik.

M. Wiener tétele

Legyen $N = pq$ úgy, hogy $q>p>2q$ és legyen $d<\frac{1}{3}N^{1/4}$. Ha adott (N, e) úgy, hogy $ed = 1 \bmod \varphi(N)$, akkor d hatékonyan megfejthető. Mivel N általában 1024 bit hosszú, e tétel következményeként adódik, hogy d-nek legalább 256 bit hosszúnak kell lennie, hogy ez a támadás ne jelentsen veszélyt. Ez a feltétel megnehezíti az alkalmazásokat a gyenge számítási kapacitású hardvereken, ahol a kis d használata nagy előny lenne.

A Wiener-tételt Boneh és Durfee [3] élesítették, így most már a d (N, e)-ből való megfejtésének korlátja $d<N^{0.292}$. Valószínűnek látszik, hogy az igazi korlát valahol $d<N^{0.5}$ körül lehet, azonban ez még nyitott kérdés.

A modulus faktorizációján alapuló támadások

Az elméleti RSA-támadások legelterjedtebb csoportja az, amelyben a támadás a nyilvános kulcs ismeretében (N, e) a modulus N faktorizálására irányul. N osztóinak ismeretében a támadó könnyen kiszámíthatja $\varphi(N)$-t, és ettől a privát kulcs is adódik: $d = e^{-1} \bmod \varphi(N)$. A modulus faktorizációján alapuló támadások műveletigénye a modulus hosszának exponenciális függvénye, így a gyakorlati feltörés irreális időigényű lehet. A jelenlegi leggyorsabb faktorizációs algoritmus az 1993-ban A. K. Lenstra, H. W. Lenstra, M. S. Mantasse és J. M. Pollard által publikált Number Field Sieve-algoritmus, amelynek műveleti igénye egy n-bites szám esetén $e^{(c+o(1))n^{1/3}\log^{2/3}n}$ egy alkalmas $c<2$ konstanssal.

Az RSA Security által meghirdetett faktorizációs versenyen is ezzel az algoritmussal érték el a rekordot, ami egy 512 bites szám osztóinak a megkeresése volt. Érdemes felidézni Martin Gardner 1977-es gondolatait [19]: „Ha a ma ismert legjobb algoritmust és a leggyorsabb számítógépeket használjuk egy ilyen 125 jegyű RSA-kulcs megfejtésére, Rivest becslése szerint a szükséges megfejtési idő körülbelül 40 quadrillió év!"

Az NFS-algoritmusnak a lépésszáma elég lassan nő a bemenet bináris hosszának a függvényében. Tegyük fel, hogy az 512 bites szám faktorizációja X lépést, időt vett igénybe, ha egy ennél 100 bittel hosszabb számot szeretnénk faktorizálni, akkor 40X lépésre lesz szükségünk, ha 150 bittel hosszabbat, akkor kb. 220X, ha 200 bittel növeljük a bemenetet, akkor 1100X-re nő a szükséges lépések száma.

Adi Shamir 2000-ben, az éves RSA-konferencián bemutatott egy gépezetet, amit TWINKLE [12] névre keresztelt, a gépezet egy érdekes optikai technikát alkalmaz, aminek segítségével az NFS-algoritmus sebességét képes két-három nagyságrenddel felgyorsítani, ezáltal képes az algoritmusok által belátható időn belül faktorizálható számok halmazát kitolni 100, esetleg 200 bittel. Így az 512 bites RSA-kulcsok igen komoly támadásnak lesznek kitéve. Ezt különösen fontos kiemelni, mivel az aktuális statisztikák szerint 512 bites RSA-kulcsokat használnak az interneten és az e-kereskedelemben részt vevő szerverek 95%-ánál.

S. W. Golomb algoritmusa

Adott $N = pq$. Írjuk fel N-t mint két négyzet különbségét

$$N = pq = a^2 - b^2 = (a+b)(a-b),$$

ahol a és b természetes számok, p és q pedig prímszámok. Az összefüggésből könnyen látható, hogy ha sikerül két ilyen négyzetszámot találnunk, akkor megvannak N prímtényezői.

Az algoritmus lépései:

- Képezzük az $a_0 = [\sqrt{N}]$ kezdőértéket
- Legyen $a_k = a_0 + k$, ahol $k = 1,2,...$
- Nézzük meg, hogy a_k^2 egy teljes négyzet-e, ha nem, akkor továbblépünk, ha igen, akkor azt kaptuk, hogy: $a_k^2 - N = b_k^2$ és így $N = (a_k+b_k)(a_k-b_k)$.

S. W. Golomb az 1870-ben még megoldhatatlannak vélt Jevons-szám (8.616.460.799) prímfaktorizációjának megkeresésével demonstrálta, hogy ez a módszer egyszerűen alkalmazható és $N = 56$ lépésben meghatározhatók a Jevons-szám prímtényezői: $p = 96079$ és $q = 89681$. A lépések száma a prímtényezők távolságától is függ. Kisebb számok esetében hatékonyabb, mint az NFS-algoritmus, mivel az iterációban szereplő műveletek nagyon egyszerűek. Az egymást követő teljes négyzetek, a_k^2-ek meghatározására ugyanis az $a_{k+1}^2 = a_k^2 + 2a_k + 1$ képletből jól láthatóan egy shiftelésből és egy összeadásból áll. A négyzetgyökvonásra pedig szintén nincs szükség, hiszen az egyenlőség túloldalát is léptethetjük hasonló módszerrel.

A komplementer prímszita

Az algoritmus [14] arra épül, hogy az összes 3-nál nagyobb prímszám $6k+1$ vagy $6k-1$ alakú, ahol $k = 1, 2, 3,...$ természetes szám. Az alábbi tételre alapuló algoritmus a komplementer prímszita.

Dénes T. tétele

Legyenek N, k, u, v természetes számok, valamint $u,v \geq 1$. $N = 6k+1$, akkor és csak akkor összetett szám, ha $k = 6uv+u+v$, vagy $k = 6uv-u-v$,

$N = 6k–1$, akkor és csak akkor összetett szám, ha $k = 6uv–u+v$, vagy $k = 6uv+u–v$.

Ennek a tételnek a következményeként kapjuk N kéttényezős felbontását, azaz
$N = 6k+1 \Rightarrow N = (6u+1)(6v+1)$, vagy $N = (6u–1)(6v–1)$
$N = 6k–1 \Rightarrow N = (6u+1)(6v–1)$, vagy $N = (6u–1)(6v+1)$

A tétel következményeként konstruálható algoritmus:

- Adott N-re eldönti, hogy $N = 6k+1$ vagy $N = 6k–1$ alakú, ennek függvényében két ágra szakad az eljárás, azaz kijelöli, hogy milyen alakú prímekkel érdemes próbálkozni.
- Ha $N = 6k+1$ alakú
  – Legyen $C_0 = (N–1)/6$
  – Ha $C_0–k \equiv 0 \bmod 6k–1$, akkor megvan a megoldás
  – $p = 6k+1$
  – $q = 6\dfrac{C_0+i}{6i+1}-1$
- Ha $C_0+i \equiv 0 \bmod 6k–1$, akkor megvan a megoldás
  – $p = 6i–1$
  – $q = 6\dfrac{C_0-i}{6i-1}+1$

  Ugyanez elvégezhető $N = 6k–1$-re is.

A Golomb-algoritmushoz hasonlóan, könnyen implementálható, nagyon gyorsan elvégezhetővé válik egy iteráció. Az algoritmus nagyon jól párhuzamosítható.

Új támadási lehetőség $\varphi(N)$ becslésével

A következőkben a prímszámok jelentős csoportjáról mutatjuk meg, hogy alkalmatlanok az RSA-modulus képzésére.

Legyen $p–1 = a^2$ valamint $q–1 = b^2$ és $N = pq$. Ekkor $\varphi(N) = (p–1)(q–1)$-re a következő összefüggést kapjuk: $\varphi(N) = (p–1)(q–1) = a^2b^2 = (ab)^2$

Ekkor N-re a fenti feltételek mellett adódik:

$$N = pq = (a^2+1)(b^2+1) = a^2b^2 + a^2 + b^2 + 1 =$$
$$= \underbrace{(ab)^2 + 2ab}_{(ab+1)^2} + \underbrace{1 + a^2 + b^2 - 2ab}_{(a-b)^2} = (ab+1)^2 + (a-b)^2$$

Tehát a fenti két összefüggés összevetéséből kapjuk:

$$b^2 = \frac{\varphi(N)}{a^2} \Rightarrow \quad N = \varphi(N) + a^2 + \frac{\varphi(N)}{a^2} + 1$$

Vezessük be az $x = a^2$ jelölést, amelyből következik, hogy x pozitív egész szám, amelyre a következő megoldásokat kapjuk:

$$0 = x^2 + x(\varphi(N) - N + 1) + \varphi(N) \quad \Rightarrow x_{1,2}$$
$$= \frac{-(\varphi(N) - N + 1) \pm \sqrt{(\varphi(N) - N + 1)^2 - 4\varphi(N)}}{2}$$

Tehát N és $\varphi(N)$ ismeretében a p és q prímtényezők kiszámíthatók. Érdemes megjegyezni, hogy máig bizonyítatlan az a sejtés, mely szerint a fentieknek megfelelő p, q prímekből végtelen sok létezik.

Megmutatjuk, hogy a gyökös kifejezés mindig egész szám és éppen a p, q prímtényezők különbsége:

$$N = pq, \quad \varphi(N) = (p-1)(q-1) = pq - p - q + 1 \Rightarrow$$
$$\Rightarrow A = \varphi(N) - N + 1 = pq - p - q + 1 - pq + 1 = 2 - p - q \Rightarrow$$
$$\Rightarrow A^2 = p^2 + q^2 + 2pq - 4p - 4q + 4 \Rightarrow$$
$$\Rightarrow \sqrt{A^2 - 4\varphi(N)} = \sqrt{p^2 - 2pq + q^2} = p - q$$

Az alábbi levezetés bizonyítja, hogy a fenti másodfokú egyenletnek bármely p, q prímszám esetén (nem csak a $p = a^2+1$, $q = b^2+1$ alakúak esetén) egész megoldása van és a két megoldás pontosan a $p–1$ és $q–1$ értékeket adja.

$$N = pq, \quad \varphi(N) = (p-1)(q-1) = pq - p - q + 1 \Rightarrow$$
$$\Rightarrow B = -(\varphi(N) - N + 1) = -pq + p + q - 1 + pq - 1 =$$
$$= p + q - 2 \Rightarrow$$
$$\Rightarrow x_{1,2} = \frac{B \pm \sqrt{A^2 - 4\varphi(N)}}{2} = \frac{p + q - 2 \pm (p - q)}{2} \Rightarrow$$
$$\Rightarrow \quad x_1 = p - 1, \quad x_2 = q - 1$$

Példa:
$N = 23.796.476.449$, $\varphi(N) = 23.794.913.536$
$A = –(23794913536–23796476449+1) = 1562914$

$$x_1 = a^2 = \frac{A + \sqrt{A^2 - 4 \cdot \varphi(N)}}{2} = 1547536 = 1244^2 \Rightarrow$$
$$\Rightarrow \quad p = a^2 + 1 = 1547537$$

$$x_1 = a^2 = \frac{A - \sqrt{A^2 - 4 \cdot \varphi(N)}}{2} = 15376 = 124^2 \Rightarrow$$
$$\Rightarrow \quad q = b^2 + 1 = 15377$$

Valóban $N = pq = 1547537 \cdot 15377 = 23.796.476.449$

Megjegyzés:
A $\varphi(N)$ érték az RSA nyilvános kulcsával közvetlenül nem áll rendelkezésre, azonban N igen. Így a támadás szempontjából lényeges az alábbi összefüggés:

$$\frac{\varphi(N)}{N} = \frac{(p-1)(q-1)}{pq} = \frac{pq - p - q + 1}{pq} = 1 - \frac{p + q - 1}{pq}$$

Ebből következik, hogy ha p és q n-jegyű decimális számok, azaz

$$p = \alpha 10^n \qquad q = \beta 10^n \qquad \left(\frac{1}{10} \le \alpha \le 1, \quad \frac{1}{10} \le \beta \le 1\right)$$

$$\varphi(N) = N - \frac{N((\alpha+\beta)10^n - 1)}{\alpha\beta 10^{2n}} \approx N - \frac{N(\alpha+\beta)}{\alpha\beta 10^n}$$

azaz $\quad N - \dfrac{2N}{10^{n-1}} \le \varphi(N) \le N - \dfrac{2N}{10^n}$

Ez azt jelenti, hogy tetszőleges N esetén egy N körüli $\frac{2N}{10^{n-1}} - \frac{2N}{10^n} = \frac{18N}{10^n}$ hosszúságú intervallumban helyezkedik el $\varphi(N)$, így maximum ennyi lépésben megtalálhatjuk.

Így maximum $\frac{18N}{10^n}$ lépésben N prímtényezői is megtalálhatók!

N számjegyeinek száma (két n-jegyű szám szorzataként) $2n$-jegyű, azaz

$$2n = \lfloor \lg N \rfloor + 1 \Rightarrow n = \frac{\lfloor \lg N \rfloor + 1}{2},$$

így a prímtényezők előállításához szükséges lépések maximális száma: $\frac{18N}{10^{\frac{\lfloor \lg N \rfloor + 1}{2}}}$

Példa:

$p = 1234577$, $q = 7654337$, $N = 9.449.868.410.449$

$$N - \frac{2N}{10^6} = 9.449.849.259.743,$$

$$N - \frac{2N}{10^7} = 9.449.866.720.680$$

tehát $9.449.849.559.743 \le \varphi(N) \le 9.449.866.720.680$

A pontosan számított érték: $\varphi(N) = 9.449.859.521.536$

Ha tehát N nagyságrendje 10^{2n}, akkor a fentiek szerint a $\varphi(N)$ meghatározásához szükséges maximális lépésszámra a következő összefüggést kapjuk:

$$N \approx 10^{2n} \Rightarrow \frac{18 \cdot 10^{2n}}{10^{\frac{\lfloor \lg 10^{2n} \rfloor + 1}{2}}} = 18 \cdot 10^{\frac{2n-1}{2}} = 18\sqrt{10^{2n-1}} = 18\sqrt{\frac{N}{10}}$$

Az RSA ellenszere Fermat-ba rejtve

Fermat egy tétele azt mondja ki, hogy ha egy tetszőleges m egész számot egy megadott modulus (N) szerint ismételten megszorzunk önmagával, akkor véges számú lépésben visszakapjuk a kiindulási számot.

Példa:

$N = 55$, $m = 6$

1.	$6^1 \equiv 6$	mod 55
2.	$6^2 \equiv 36$	mod 55
3.	$6^3 \equiv 51$	mod 55
4.	$6^4 \equiv 31$	mod 55
5.	$6^5 \equiv 21$	mod 55
6.	$6^6 \equiv 16$	mod 55
7.	$6^7 \equiv 41$	mod 55
8.	$6^8 \equiv 26$	mod 55
9.	$6^9 \equiv 46$	mod 55
10.	$6^{10} \equiv 1$	mod 55
11.	$6^{11} \equiv 6$	mod 55

$N = 55$, $m = 22$[3].

1.	$m^1 \equiv 33$	mod 55
2.	$m^2 \equiv 44$	mod 55
3.	$m \equiv 22$	mod 55

A tétel akkor is igaz, ha a kapott számot ismételten hatványra emeljük, $m_k = m_{k-1}^e N$.

$N = 55$, $m = 6$, $e = 3$

1.	$m_1 = m^3 \equiv 33$	mod 55
2.	$m_2 = m_1^3 \equiv 33$	mod 55
3.	$m_3 = m_2^3 \equiv 33$	mod 55
4.	$m_4 = m_3^3 \equiv 33$	mod 55

Ezen módszer segítségével meglepően gyorsan megfejthető a helytelenül választott RSA-kulcs, hiszen a megfejtéshez szükséges idő a kulcsgenerálás idejével szinte azonos.

Bemutatok egy példát, amelyben 60 jegyű RSA-modulussal dolgozunk, mégis 6 lépésben megtalálja a megoldást.

Legyen p és q két 30 decimális jegyű prímszám.

$p = 586203142714212103540772438083$

$q = 797648851083268082237297393713$, valamint

$N = pq = 467584263287392317254879360844851439325139765393920565972179$

$e = 227104576216343623581376514176931506454984828057257408953697$

Tehát az RSA publikus kulcs (N,e). Ezt ismerheti bárki. Vegyünk egy M üzenetet

$M = 200805001301200805130120090301120009142005121209070514030518$

$C = M^e \bmod N = 558899877578499654114721338354996634436912630684758356416031$

Erre a C-re indítsuk el az előző algoritmust.

$C_1 = C = 558899877578499654114721338354996634436912630684758356416031$

$C_2 = C_1^e \bmod N = 223750832076885567075596533921520571432669817831015567847029$

$C_3 = C_2^e \bmod N = 125570682192299884755285588845491334562889379789987617505740$

$C_4 = C_3^e \bmod N = 391905799288799316230065355244283729845303727255308484589194$

$C_5 = C_4^e \bmod N = 443206215744660358477637214037248569893336001413967401671 4$

$C_6 = C_5^e \bmod N = 200805001301200805130120090301120009142005121209070514030518$

$C_7 = C_6^e \bmod N = 558899877578499654114721338354996634436912630684758356416031$

$C_7 = C_1 \Rightarrow C_6^e \bmod N = M^e \bmod N$, tehát adódik, hogy $C_6 = M$, és a nyílt üzenetet a titkos kulcs ismerete nélkül, 6 lépésben megfejtettük. Ezen támadás ellen a kulcsgenerálás során lehet védekezni, ha figyelünk arra, hogy a választott e és d értékek megfelelően távol legyenek egymástól és a hatványozási ciklus hossza is elegendően nagy legyen. Ezen feltételek biztosítása lassítja az algoritmus használatát, de amint láthatjuk, szükséges az RSA-kulcsok biztonságához.

Az RSA-titkosítás matematikai alapjai a *kis Fermat*-tételre alapulnak, amit később Euler bizonyított be.

„kis Fermat-tétel":

Ha a nem osztható p-vel és p prímszám, akkor teljesül az alábbi kongruencia.

$a^{p-1} \equiv 1 \bmod p$

Euler ezt a tételt nemcsak bizonyította, hanem általánosította is, így ma már Euler-Fermat-tételnek nevezzük.

Euler-Fermat-tétel:

Legyen $m>1$ egész szám és $(a,m) = 1$, azaz a és m relatív prímek, akkor teljesül

$a^{\varphi(m)} \equiv 1 \bmod m$

Hogy ez valóban a *kis Fermat*-tétel általánosítása, ahhoz a $\varphi(m)$ Euler-féle függvény értelmezéséről kell beszélnünk. $\varphi(m)$ jelenti a $0, 1, 2, ..., m-1$ számok közül az m-hez relatív prímek számát. Az alábbi táblázatban az első néhány ilyen értéket bemutatjuk:

m	$1,2,3,\ldots,m-1$	m-hez relatív prímek	$\varphi(m)$
3 (prím)	1, 2	1, 2	2
4	1, 2, 3	1, 3	2
5 (prím)	1, 2, 3, 4	1, 2, 3, 4	4
6	1, 2, 3, 4, 5	1, 5	2
7 (prím)	1, 2, 3, 4, 5, 6	1, 2, 3, 4, 5, 6	6

Könnyen belátható, hogy ha $m = p$ prímszám, akkor $\varphi(p) = P-1$. Továbbá igaz az Euler-függvényre, hogy ha p és q prímek, akkor $\varphi(pq) = (p-1)(q-1)$. Így tehát az $N = pq$ RSA-modulusra alkalmazva az Euler-Fermat-tételt, éppen az RSA-algoritmus alapösszefüggését kapjuk.

Azonban vannak olyan n összetett számok, amelyek, adott n-hez relatív prím a-ra kielégítik a kis Fermat-tételt, vagyis

$a^{n-1} \equiv 1 \bmod n$ ahol n összetett szám és $(a,n) = 1$

Az ilyen összetett n számokat, amelyekre az összefüggés teljesül, a alapú pszeudoprímeknek, vagy álprímeknek nevezzük.

Talán még meglepőbb, hogy vannak olyan n összetett számok, amelyek minden n-hez relatív prím a-ra kielégítik a fenti összefüggést. Az ilyen n számokat nevezzük felfedezőjükről Carmichael-számoknak, melyekről csak a XX. század közepén sikerült bebizonyítani, hogy végtelen sok létezik belőlük.

A fenti tulajdonságaik alapján belátható, hogy az RSA-támadások szempontjából jelentősek a pszeudoprímek és ezek speciális reprezentánsai, a Carmichael-számok. Ugyanis ha az RSA-modulus egy Carhmichael-szám valamely osztója, vagy bizonyos tulajdonságokkal rendelkező pszeudoprím, akkor a fent bemutatott Fermat-féle ciklus hossza éppen 1. Néhány példa ennek illusztrálására:

2-es alapú pszeudoprímek: 341,561,645

$2^{341} \equiv 2 \bmod 341$, $2^{561} \equiv 2 \bmod 561$, $2^{645} \equiv 2 \bmod 645$

3-as alapú pszeudoprímek: 91,121,286

$3^{91} \equiv 3 \bmod 91$, $3^{121} \equiv 3 \bmod 121$, $3^{286} \equiv 3 \bmod 286$

5-ös alapú pszeudoprímek: 124,217,561

$5^{124} \equiv 5 \bmod 124$, $5^{217} \equiv 5 \bmod 217$, $5^{561} \equiv 5 \bmod 561$

A legkisebb Carmichael-szám az 561, tehát minden N-re, amelyik kisebb mint 561 és ahhoz relatív prím, igaz, hogy $N^{561} \equiv N \bmod 561$

Felmerülhet a kérdés, hogy ezek az RSA-rejtjelezés szempontjából veszélyes modulusok milyen valószínűséggel fordulnak elő? Ugyanúgy, ahogy a prímszámokra, a pszeudoprímekre és Carmichael,számok számára sem ismert zárt formula, azt azonban tudjuk, hogy mindkettőből végtelen sok van. R. G. E Pinch munkássága eredményeképpen léteznek az interneten is elérhető nagy pszeudoprím- és Carmichael-számtáblázatok [17][18], ezen táblázatok segítségével becsülhetjük az ily módon veszélyes RSA-modulusok arányát.

Intervallum	Pszeudoprímek száma	Carmichael-számok száma
1-10	1	-
1-100	30	-
1-1000	434	1
1-10000	5106	7
1-100000	55576	16

Mint az a táblázatból jól látható, a Carmichael-számok aránya 1 ezrelék körül mozog, a pszeudoprímek aránya ennél jóval magasabb, 55-60%. Ez a bizonytalansági tényező megingathatja az RSA biztonságába vetett hitet, és egyúttal egy új utat mutat az RSA-támadások területén.

A bemutatott számítások érdekesek, azonban ennek részletes ellenőrzésére nem vállalkoztunk. A szerkesztőség.

Irodalom

1 R. L. Rivest–A. Shamir and L. Adleman: A method for obtaining digital signatures and public key cryptosystems. Commun. ACM 21 120-126

2 M. Wiener: Cryptanalysis of short RSA secret exponents, IEEE Trans. Inform. Theory 36 (1990), 553-558

3 D. Boneh–G. Durfee: New results on crpyptanalysis of low private exponent RSA, preprint 1998

4 D. Coopersmith: Small solutions to polynomial equations, and low exponent RSA vulnerabilities, J. Cryptology 10 (1997), 233-260

5 J. Hastad: Solving simultaneous modular equations of low degree, SIAM J. Comput. 17 (1988), 336-341

6 A. Menezes–P. Van Oorschot–S. Vanstone: Handbook of Applied Cryptography, CRC Press, Boca Raton, FL, 1996.

7 Nicko van Sommeren: Adi Shamir

8 P. Kocher: Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems, CRYPTO'96, Lecture Notes in Computer Science, vol. 1109, Springer-Verlag, 1996, pp 104-113.

9 D. Boneh–G. Durfee–Y. Frankel: An attack on RSA given a fraction of the private key bits, AsiaCrypt'98, Lecture Notes in Computer Science, Springer-Verlag, Berling and New York, 1998

10 C. Pomerance: The quadratic sieve factoring algorithm, Proceedings of EUROCRYPT 84 (LNCS 209), 169-182, 1985
11 A. K. Lenstra–H. W. Lenstra–M. S. Manasse–J. M. Pollard: The Number Field Sieve, Vol. 1554 of Lecture Notes in Mathematics, 11-42, Springer Verlag, 1993.
12 Adi Shamir: Factoring Large Numbers with the Twinkle Device (Extended Abstract). CHES 1999: 2-12
13 Dan Boneh: Twenty years of attacks on the RSA cryptosystem, Notices of the AMS, February 1999, 203-213
14 Tamás Dénes: Complementary Prime-Sieve, P.U.M.A megjelenés alatt
15 S.W. Golomb: On factoring Jevons' number, CRYPTOLOGIA, vol XX. No3 1996
16 W. S. Jevons: The Principles of Sience, A Treatise on Logic and Scientific Method, Macmillan & Co. London. 1873 Second Edition. 1877
17 R. G. E. Pinch: The pseudoprimes up to 10^13 ftp://ftp.dpmms.cam.ac.uk/pub/PSP
18 R. G. E. Pinch: The Carmichael numbers up to 10^16 ftp://ftp.dpmms.cam.ac.uk/pub/Carmichael
19 Martin Gardner: Mathematical games A new kind of cipher that would take millions of years to break Scientific American, 1977.

Hírek

Az Ericsson előre fizetett rendszere (PPS) lehetővé teszi, hogy a szolgáltatásokért előzetesen fizető mobilfelhasználók élvezhessék a multimédiás üzenetkezelési szolgáltatást (MMS). A hálózatüzemeltetők az előre fizetett szolgáltatásaik felhasználóival a tartalom alapján számolhatnak el. Az olyan funkciókat, mint például színes képeket, animációkat, audio- és videoklipeket kínáló multimédiás üzenetkezelési szolgáltatások növekedést ígérnek a mobil üzenetkezelési lehetőségek terén. Elterjedésének titka a számlázásukra szolgáló, könnyen átlátható megoldás.

❖ ❖ ❖

Az elmúlt tizenhat hónap során duplájára duzzadt a magyarországi GSM piac, az ötvenszázalékos penetráció továbbra sem tűnik elérhetetlen álomnak.

A HIF október végi adatai alapján jelenleg a magyar lakosság 43 százaléka rendelkezik mobiltelefon-előfizetéssel.

Eredményesebb tizenkét hónapot tudhat maga mögött a Pannon GSM. Számos, úttörőnek számító szolgáltatást indított útjára, köztük egy európai viszonylatban is ritkaságszámba menő m-commerce-t.

Valamivel több mint 40 százalékuk, közel 1,8 millió ember a Pannon GSM ügyfele.

A mobilszolgáltatók azonban felismerték azt is, hogy a 18 év alatti korosztály mára meglehetősen fogékonnyá vált a mobiltelefónia iránt. Így a 2001. év fő fejlesztési iránya a tizenéves korosztályt érintette, hiszen a Pannon GSM igényeiket szem előtt tartva alakította ki a Bee márkát.

❖ ❖ ❖

A PSINet Magyarország is megkezdi ADSL-hozzáférések kiépítését, különböző ADSL-konstrukciók értékesítését. Elsősorban olyan cégek érdeklődésére számítanak, amelyek nagy mennyiségű információt kívánnak letölteni a világhálóról, az internet felé irányuló adatforgalmuk azonban kisebb. A szolgáltatáscsomagok különböző fürgeségű hozzáférési módot tartalmaznak, de a legalacsonyabb sebességű csomag is hétszer olyan gyors letöltést tesz lehetővé, mint a hagyományos dial-up kapcsolat.

A kínált csomagok mindegyike – kivéve a bevezető modellt – tartalmaz alapszintű tűzfal-szolgáltatást is. Ez az elem alapvetően új az ADSL-kínálatban. Az internet- és hálózati biztonság irányába tett bővítést nem csak a hackerkriminalisztika megjelenése indokolja. A cég vezetői szerint egyre több üzleti folyamat kerül a netre, olyan tranzakciók is, amelyekben az adatforgalom sérthetetlensége és vezényelt titkosítása elkerülhetetlen, mint például az on-line banking esetében.

A PSINet – kereskedelmi filozófiájának megfelelően – közvetlenül csak az üzleti felhasználók részére értékesíti ADSL-csomagjait. Nem maradnak ki az ügyfélkörből az otthoni igénylők sem: részükre a PSINet lakossági internetszolgáltató partnerei nyújtják a személyre szabott kapcsolási lehetőséget.

Hírek

A Sysdata Kft. egy éve nyitotta meg irodáját. Nyitáskor 20 munkatárs kapcsolódott be az elsősorban távközlési szoftverek fejlesztésével foglalkozó cég projektjeibe. Jelenleg 52 szakember dolgozik. A szegedi iroda további bővülése elsősorban a piaci helyzet további alakulásától függ. A szegedi munkatársak egy év alatt szakmai felkészültségükkel a megbízók elégedettségét vívták ki. Munkaerőigényét főként a Szegedi Tudományegyetemen végzett programozókkal, informatikusokkal elégíti ki. Az egyetem oktatási színvonalának emeléséhez a Sysdata is hozzájárul. Az oktatói állomány megtartása céljából a Sysdata többféle támogatást nyújt: tavaly PC-ket adott át, majd az ősszel egy közös innovációs projekt indult, valamint az 1 éves évforduló alkalmából az egyetem informatikai tanszékcsoportjának 6 oktatója részesült ösztöndíjban.

❖ ❖ ❖

Vasárnap kezdődött az Oracle OpenWorld konferencia, amely az Oracle technológiát használó ügyfelek, fejlesztők és partnerek legnagyobb nemzetközi összejövetele.

Az első nap egyik fő témája az új alkalmazáskiszolgáló termék, az Oracle 9i AS Release 2 volt. Az ezzel kapcsolatos híreket foglaljuk össze.

A fejlesztés alapjai. A fürtözési és gyorsító-tárazási megoldásai mellett a második verzió a legújabb Java 2 Enterprise Edition (J2EE) 1.3 szabványt is támogatja, ezáltal vállalati szintű webszolgáltatásokat és integrációt, egységes üzenetkezelést, új portálfunkciókat és a vezeték nélküli elérést támogató új funkciókat kínál.

A biztonsági elemek, rendelkezésre állás érdekében megvalósították a „gördülő" bővítést, a dinamikus átkonfigurálhatóságot, az üzem közbeni egységcserét. A Fast Start Fault Recovery architektúra, amely karbantartás vagy meghibásodás esetén kívülről észrevehetetlenül kapcsolja tartalékra az alkalmazáskiszolgáló és az adatbázis-kezelő réteget, s ezzel állásidő nélkül futtatja az Oracle 9i AS-re telepített alkalmazásokat. Az Oracle 9i átfogó biztonsági infrastruktúrát is kínál, valamint a külső és házi fejlesztésű alkalmazásokon is támogatja az egyszeri bejelentkezést és a felhasználók központi kezelését.

Információs lehetőségeket kínál a nyílt szabványokon alapuló rendszer, támogatja a más gyártóktól származó adatbázisokat és a kereskedelmi forgalomban kapható alkalmazáscsomagokat, valamint tág lehetőségeket biztosít a „dobozos" szoftverek, a webes szolgáltatások és az új Java-alkalmazások, a régebbi nagy számítógépek koordinálására.

Webes szolgáltatásokkal a vállalatok egyszerűen tudnak biztonságos és megbízható, Java alapú webes szolgáltatásokat kifejleszteni. Az Oracle 9i AS rendszeren kifejlesztett webes szolgáltatások az Oracle által támogatott operációs rendszerében – a UNIX és Linux összes elterjedt verzióján – futnak, és együttműködnek más szabványok alapján, például a Microsoft.NET technológiájával kifejlesztett szolgáltatásokkal. Biztosítja a kritikus fontosságú üzleti szolgáltatások esetében jelentkező sok résztvevős tranzakciós aszinkronátvételt és fejlett biztonsági funkciókat. Az önkiszolgáló, webes adminisztrációs eszközzel minden vállalat programozási ismeretek nélkül, saját maga határozhatja meg az üzleti folyamatok közti kapcsolatokat.

Az alkalmazáskiszolgáló új, vezeték nélküli funkciói a beszéddel elérhető internetes alkalmazások, a vezeték nélküli üzenetközvetítés, a vezeték nélküli alkalmazások biztonsága, a mobil e-mail és a helyfüggő szolgáltatások terén nyújtanak új lehetőségeket. Az egyedi igényeknek megfelelő kialakítást, helymeghatározást, üzenetközvetítő szolgáltatásokat és tartalomkezelést nyújtanak, bármilyen típusú tartalom és alkalmazás bármely eszközre való eljuttatásához, rendszerbe állításához és felügyeletéhez. A megoldás nem igényel sem különleges ismereteket, sem különleges hardvereszközöket.

❖ ❖ ❖

Az Axelero Internet idén novemberben felmérést végzett saját ADSL-előfizetői körében, amely az elégedettség mérésén túl az internetezési szokásokra is kitért. A válaszadási hajlandóság rendkívül magas volt, a megkérdezettek 28%-a felelt a kérdésekre, ami egy weben kitölthető kérdőívnél rendkívül jó arány.

A válaszok egyik érdekessége, hogy a megkérdezettek fontos felhasználási területként emelték ki az on-line rádiók hallgatását (27%), az MP3 zenei anyagok (49%), videók (51%) és grafikus fájlok (54%) letöltését, valamint az on-line játékokat (31%).

A magyar televíziózás jövője

KOMZA IMRÉNÉ

történész, társadalomkutató főmunkatárs
Magyar Informatikai Szövetség

A fenti címmel kétnapos konferenciát szervezett a Magyar Informatikai és Kibernetikai Egyesület (MIKE) elnöksége a Magyar Tudományos Akadémia székházában, Budapesten.

Bevezetés

A konferencián a szervező házigazda nevében Garádi János – a MIKE (1990. augusztus 20-án alakult és jelenleg közel ötezer tagja van, valamint 8 tagozata működik) elnöke üdvözlő szavaiban felhívta a hallgatóság figyelmét arra, hogy a jövőben az Európai Unióban helyzetünket a média jelentősen befolyásolhatja, lényeges továbbá, hogy hazánk eddig is jelentős szerepet játszott a televíziózás fejlesztésében.

Mind jövőnk, mind múltunk kapcsolatban van a tévétechnikával. Az Európai Unióhoz történő csatlakozásunk szempontjából nem lehet lényegtelen számunkra a leghatékonyabb média jövőbeli szerepe. Európában a szakemberek arról vitatkoznak, hogy valóban véget ért-e a minőségi televíziózás kora, és csak a gazdasági mutatókat kell és szabad figyelembe venni a kultúra rovására. Ennek ellenkezőjét is sokan állítják.

Múltunkból pedig kiemelkedik, hogy 76 évvel ezelőtt (1926-ban) jelentette be Tihanyi Kálmán magyar feltaláló a televíziózás máig érvényes alapelveit, melyet a UNESCO Világmemória Program Nemzetközi Tanácsadó Bizottsága 2001. évi őszi döntésével a szellemi világörökség részének nyilvánította, és felvette a Memory of the World Registerbe.

A konferencia jellege

A megnyitót követően a két nap alatt összesen 28 előadásra (naponként 14-14) került sor. A konferencián négy országos testületet képviseltek a jelenlévő szakemberek. A Magyar Rádió Rt. elnöke és hat televíziótársaság vezetője számolt be a jelenről és a jövőbeni tervekről. Nyolc szövetség, egyesület, illetve alapítvány küldte el képviselőjét a rendezvényre. Tíz szakmai újság és tudósító cég képviseletében jelentek meg érdeklődő szakemberek. Az előadók Budapest, Eger, Szeged és Székesfehérvár képviseletében jöttek el, hogy értékes és érdekes előadásaikat megtartsák a jelenlévők részére. Az első alkalommal megrendezett konferenciának a Magyar Tudományos Akadémia székháza méltó helyet biztosított. A rendezők és a konferencián megjelentek egyöntetű véleménye az volt, hogy nagyon jó kezdeményezésnek lehettek részesei, és a jövőben ismét szükséges lenne találkozni.

A következő hasonló összejövetelt 2002. júniusban tervezik megtartani „A magyar televíziózásról" címmel, melyre a magyar nyelvterületekről is várnak vendégeket (előadónak és hallgatónak egyaránt). Jelen konferencián a plenáris ülések után, egymást követően a két nap alatt hat szekcióban hangzottak el az előadások. Néhány érdekes előadásból szeretnék részleteket közölni, mivel az elhangzottak teljes közlése a terjedelem miatt lehetetlen lenne.

Az előadások fő mondanivalója (1. nap)

A konferencia első napjának délelőttjén előadásában Vizi E. Szilveszter mint agykutató akadémikus (az MTA elnöke, a TIT alelnöke) kiemelte, hogy a XX. század második felében a tudomány robbanásszerű fejlődése azt idézte elő, hogy a televízió napjainkra mindenki számára hozzáférhetővé vált. Ez hatalmas hatással lehet az egyénre és a társadalomra. Ellentétben a könyvvel – ahol csak vizuális érzékszerven keresztül jönnek az impulzusok –, a televízióból jövő ingerek – a hallás is egy időben jelen van – egymást felfokozva nagyon jelentős hatást tud kifejteni érzelmileg és tudatilag az egyénre és a kisebb közösségekre.

Ezért igen nagy az erkölcsi felelőssége a televízióknak (a közszolgálatinak és a kereskedelminek egyaránt)

és a rádióknak. A tudat fejlesztésén túl az értékmegőrzés és értékteremtés területén is meghatározó a szerepe.

Az ún. „szappanoperák" sikerének a titka nagyon egyszerű (nem igényli az asszociatív kéregnek az aktivitását), főleg az érzelem világára hatnak és ezért sikeresek lesznek a jövőben is, amit tudomásul kell venni.

Azonban az, hogy az eseményeket hogyan, miként, milyen érzelmi töltéssel közvetíti a televízió, a generációk fejlődésében nagyon fontos szerepet játszik.

A televíziók, mint már említettük, nemcsak a generációk részére történő értékátadásban játszanak döntő szerepet, hanem az erkölcsök megtartásában vagy szétrombolásában is.

A délelőtt második plenáris előadásán Michelberger Pál akadémikus, a Műszaki és Természettudományi Egyesületek Szövetségének elnöke (az MTA volt alelnöke) az innováció fontosságát és a felgyorsult időt állította a középpontba.

A múltbeli műszaki fejlesztést és a jelenlegi, valamint a várható jövőbeni néhány sajátosságát elemezte előadásában. Ebből a legfontosabb következtetések talán két irányban jelentkeznek.

Az egyik a felgyorsult változás kérdése, az élethossziglani tanulás kényszerét hozza magával. A másik az egyes tudományterületek hatása más tudományterületek fejlődésére.

Egyéb nézőpontok is léteznek, de a televíziózás szempontjából ebből a két nézőpontból kiindulva kellene a műsorpolitikát kialakítani. Egy kutató – legfőképpen pedig egy akadémikus – számára nem jelent gondot, és még inkább nem kell magyarázni az élethossziglani tanulás szükségességét. A különböző technológiák változása megköveteli minden munkavállalótól a megszerzett tudásának időről időre történő megújítását. Tudomásul kell venni, ugyanis nem lehet iskolapadba beültetni embereket élethossziglan. A jelenlegi termelési viszonyok sem engedik meg azt, hogy visszaültessük az embereket az iskolapadba. Az élethossziglani tanulást valahogy játékosan is meg kell oldani, és ez az oktatás fejlesztésének a feladata. Itt nemcsak a saját szakmánkban kell megújulni, hanem az egész világszemléletünknek is újjá kell alakulnia.

Vizi E. Szilveszter akadémikusra hivatkozott előadásában az MTESZ elnöke, aki „az agyban elhelyezkedő idegsejtek számánál fontosabbnak tartja a közöttük levő kapcsolatrendszert". Az élethossziglani tanulási folyamat résztvevői számára a lexikális tudásnál is fontosabbak a szakmai megújulás, és még inkább a világszemlélet megváltozása következtében szükséges asszociációk, logikai kapcsolatok.

Alapvetően a televízió feladata és lehetősége a játékosabb, könnyebb megoldások keresése sok-sok olyan ember számára, aki nem hajlandó vagy nem képes úgy tanulni, mint egy tudományos pályára „rámozdult" ember.

Márpedig, ha nem igyekszünk, akkor lemaradunk, és aki lemarad, azt leírják – zárta gondolatait Michelberger Pál akadémikus.

Vámos Tibor akadémikus, tanácsadó a délutáni előadók közül elsőnek emelkedett szólásra. Előadásának azt a címet választotta, hogy „Televíziós változatok egy egységesítő technikájú információs világban".

Az előadás bevezetőjében utalt arra, hogy az információs eszközök integrálódását már megfigyelhetjük a jelenleg legdinamikusabb területen, a mobil kapcsolatokban. Egy ember általában egy megjelenítőt figyel egyszerre, ezt használja telefonnak, videokapcsolatnak, levelezésre, bevásárlásra, továbbá számos más internetalkalmazásra és természetesen televíziózásra is. Így a televízió jövőjét elsősorban ebben a sokcélú megjelenítőben nézhetjük. Ez annyit is jelent, hogy a mai típusú televíziós szolgáltatás csak ott érdekes, ahol a pillanatnyi jelenlét izgalma számít, sportközvetítésnél, rendkívüli híreknél, elnökjelöltek vitájánál.

A többi programszolgáltatótól szabadon (persze nem ingyen), tetszés szerint lehívott szórakoztató, oktató, információs, kereskedelmi és mindenféle egyéb célú anyag. Így a fő televíziózás utáni működési ág a programszolgáltatás lesz. A mai portálok továbbfejlesztése. Ez újra felveti annak a kérdését, hogy kell-e állami televízió, amit közszolgálatinak szépítenek, holott reklámok után szalad, sok ostoba műsorral próbál versenyezni, ezenkívül politikailag sem független.

Ha egy tisztességes állam kultúrát próbál támogatni, akkor ezt programtámogatások és nem szervezettámogatások képében kell hogy megkeresse, a programpályázatok elbírálása pedig néhány párhuzamos szakmai kuratórium ügye lehetne. A párhuzamos megjelölés arra vonatkozik, hogy egy területen se alakulhasson ki akár szakmai, akár stílusbeli monopólium – fejezte be gondolatait Vámos akadémikus.

Az akadémikusok elvi előadásait követően az Országos Rádió és Televízió Testület (ORTT) elnökének képviseletében dr. Nálik Gábor, a testület tagja ismertette a testület feladatait és további terveit. Őt követte Kondor Katalin elnök asszony rövid és gyors értékelése a Magyar Rádió jelenlegi helyzetéről, műsorairól és terveiről. A szünet előtt a két közszolgálati televízió vezetőjének előadását kísérhették figyelemmel a jelenlévő szakemberek.

A nap utolsó harmadában kaptak lehetőséget a kereskedelmi televíziók képviselői, melynek keretében vezetői beszámolóik igen érdekes tervekről, elképzelésekről és konkrét megvalósításokról adtak tájékoztatást a hallgatóságnak. Az első nap végén a két közszolgálati televízió kuratóriumainak elnökei összegezték jelen tapasztalataikat, melynek tanulságai alapján kialakult és megfogalmazott céljaikat ismertették a hallgatósággal.

Minden vezető fontosnak tartotta a megfelelő műszaki színvonal biztosítását, és vázolta a jelenlegi elmaradottság szintjét. Külön kiemelték a megfelelő minőségű televízió-műsorok iránti elkötelezettségüket, melyet a jelenlévők (szakemberek és nézők) egyaránt nagy örömmel vettek tudomásul.

Legfontosabb megállapítások (2. nap)

A következő nap délelőtti részében „A televíziós szakemberek képzése és a televízió alkalmazása az általános képzésben" szerepelt.

Elsőként Horváth Ádám (Színház- és Filmművészeti Egyetem) rektorhelyettes (a Magyar Televízió Rt. volt elnöke) a televíziós szakemberek képzése kérdés közben ismertette több évtizedes tapasztalatait és összegezte véleményét. Televíziós szakemberképzés több mint 30 éve folyik az egyetemen. A folyamatosan változó és az utóbbi időben egyre gyorsuló műszaki fejlődést hazánkban is feltétlenül követni kell. A most folyó képzés dilemmája az, hogy a jövő ifjú szakemberét arra képezzék-e, amit most művelnek a televíziós társaságok (virtuális hátterek, reklámok, felületes fogalmazás, elnagyolt témaközelítés), vagy a klasszikus tévézésre (ami nem jelenti az elavult ismeretek oktatását). Az egyetem a humán végzettségű és magas szakmai képzettséggel rendelkező szakemberek képzése mellett tette le a voksát. A közszolgálati média intézményeinek közel negyven-ötvenéves elavult építményei és eszközei vannak, és az pedig nem pénz, hanem döntés kérdése, hogy mi legyen ezeknek a sorsa.

Az új médiával összefüggő képzési törekvések a Budapesti Műszaki és Gazdaságtudományi Egyetemen címmel tartotta meg előadását dr. Magyar Gábor fejlesztési igazgató.

Előadásában többek között kitért arra, hogy a „digitális világ" még nagyon új, még nem alakultak ki az emberek gondolkodásában, és nem váltak mindennapivá alapvető kategóriái. Például az „egy kiló paradicsom" meghatározáshoz mindannyiunkban hasonló, a valós világ tényeihez illeszkedő képzet társul (körülbelül mennyi darab lehet, milyen nagy a térfogata stb.). „Egy megabyte adat" az emberek nagy többségének nem mond semmit, ehhez nem kötődnek reális és pontos képzetek.

Ez változni fog: az informatika, a távközlés és a média konvergenciája alapvetően érinti a gazdaság működését, befolyása kiterjed a társadalom és gazdaság korábban érintetlen területeire is. Az új, digitális médiatechnológiák által lehetővé tett változások érintik a fizika, az érzékelés-lélektan, az írásos kultúra kérdéseit is. Új munkamegosztási struktúrákat, új életmód-alternatívákat hozhatnak létre, megváltoztatják a társadalmi és állami döntési mechanizmusokat. A változó munkamegosztásban új szakmákra is keletkezik igény. Ezért ma különösen fontos a különböző diszciplínák képviselőinek együttműködése.

E nagy horderejű társadalmi változás természetesen komoly kihívást jelent az oktatás számára. A BME képzésének többrétű fejlesztésével reagál erre a kihívásra. Az audio/video technikát a BME Villamosmérnök és Informatikai Kar (VIK) villamosmérnöki képzése mélyen és naprakészen oktatja.

A médiarendszerek egyre inkább számítástechnikai műszaki megoldásokkal készülnek. A stúdió, az archívum, a médiahálózat egy-egy nagy informatikai rendszer is. A BME VIK műszaki informatikus képzése felkészíti a hallgatókat nagy informatikai rendszerek tervezésére, fejlesztésére, fenntartására. Interdiszciplináris feladatok is jellemzik az új médiát. Például a digitális tévé és rádió kulcskérdése az archívum, amihez funkcionális, műszaki, jogi, gazdasági kérdések együttes kezelése szükséges. Olyan képzést is indít a BME, ami kiterjed a humán és a műszaki ismeretek érintkező területeire.

A délelőtti oktatási szekció utolsó előadója dr. Zárda Sarolta, a budapesti Gábor Dénes Főiskola főigazgatója előadásában ismertette, hogy milyen távoktatási módszerekkel dolgoznak megalakulásuk (1992) óta.

Jelenleg 20 ezer aktív és 30 ezer passzív hallgatójuk van, alapvetően informatikát tanítanak. A távoktatás olyan tanulási folyamat, ahol az osztálytermi oktatást helyettesíti egy médiamix, ami olyan tananyagcsomag, amelynek több eleme van (eleme a tankönyv, eleme lehet a videokazetta és a nyilvános műsorszórás is).

Angliában az Open University a 70-es években alakult BBC-nek egy külön részlegét hozta létre óriási kormánytámogatással erre a célra. Nagyon érdekes felméréseket végeztek a televíziónak az oktatásban betöltött szerepéről. Létezik egy olyan kurzus, amely nagy népszerűségnek örvend és ez a hatékony menedzser címet viseli. Erre ötezer hallgató iratkozott be, amikor ezzel kapcsolatosan egy műsort sugároztak, és ezt az adást 100 ezren nézték. Tehát az a 95 ezer ember, aki nincs beiratkozva (nem kapja meg a tankönyvet, nem megy el vizsgázni), pusztán megnézi ezt a műsort, ingyenesen képződik („melléktermékként"), közel hússzorosa a beiratkozottak számának. A főiskolán is használják a televíziót, de elsősorban videóra veszik az oktatási anyagokat és azokat továbbítják a hallgatóknak.

Mi lesz valójában a jövő végberendezése? Nem tudjuk pontosan, hogy egy televízió, egy PC lesz a jövő végberendezése. Az azonban egészen biztos, hogy a távközlés, az informatika és a média konvergenciája bekövetkezik. Amikor ez a konvergencia valósággá válik, akkor természetesen a tananyagok továbbításának ez lesz a legkézenfekvőbb eszköze.

Lássunk most egy olyan területet, az elektronikus oktatást, amely jelenleg az e-businessben már több mint 10%-ot képvisel. Ha bekövetkezik a konvergencia, akkor a nyilvános műsorszórás és az elektronikus oktatás ötvözete fogja hatékonnyá tenni a távoktatás módszerét.

A főiskolának hét kihelyezett tagozata van (4 Erdélyben, 2 Szlovákiában, 1 pedig Szabadkán). A Duna Televízió oktatási sávjában kaptak ingyenes műsorközlési lehetőséget – ez két éve átrendeződött.

A második nap délutáni részében is igen izgalmas előadások követték egymást. Pungor Ernő akadémikus (volt OFMB-elnök és nyugalmazott miniszter) előadását A jövő technikai lehetőségei címet viselő szekció első előadójaként tartotta meg. Előadásában az innováció fontosságát emelte ki. Annak érdekében, hogy egy adott állam tudjon biztosítani egy adott célra – jelen

esetben a televíziók működéséhez – megfelelő tőkét, a gazdaságnak kell úgy fejlődni, hogy ezt megtehesse.

Magyarországon (a természeti kincsek mennyiségi és minőségi hiánya miatt) a fejlődéshez szükséges és alapvető a szellemi erő felhasználása, amellyel a gazdaság megfelelő sebességgel képes fejlődni. Itt a finnországi példára utalt az akadémikus, ahol 20 évvel ezelőtt rájöttek arra, ha nem végeznek olyan kutatásokat, amelyek újabb és újabb termékeket hoznak a gazdaságba, akkor nagy baj lesz.

Az innováció alapja a humán erőforrás, amelynek alapvető feltétele az, hogy az oktatás kezdettől olyan színvonalú legyen, hogy alkotó, innovatív szakembereket készítsenek fel az ipari fejlesztésre. Az iskolai oktatást az egyetem elvégzésével nem lehet befejezni, hanem jönnie kell a továbbképzésnek, mert a képzés értékcsökkenése a műszaki területeken igen gyors (különböző ágazatokban 4-8-10 év alatt következik be a tanult ismeretek elavulása). Itt elsősorban nemcsak a kutatók képzésére kell gondolnunk, hanem a mindennapi életben felhasználókat (a termelésben és a gazdasági életben) is ide kell sorolnunk. Példaként az USA-t hozta fel, ahol a továbbképzés nem az egyetemek kezében van, hanem az egyesületek kezében összpontosul, amelyek egymás után tartják a különböző továbbképző és átképző tanfolyamokat. Az innovációs folyamat új ismereteket igényel. Ez azt jelenti, hogy egy életen át való tanulás, mely az EU-nak is egy nagy-nagy programja, minden ország számára az egyetlen járható út.

Még inkább szeretném hangsúlyozni, hogy az innováció alapfeltétele az igen magas szintű és szervezettségű alapkutatás. Amennyiben az ország alapkutatási potenciálja csökken, akkor ez az innovációra is kihat. Magyarországon viszonylagosan az innováció és az alapkutatás aránya jó. Az innováció azonban abszolút értelemben rossz. Figyelembe kell venni azt, hogy az innovációhoz kb. 10-20-szoros tőke szükséges az alapkutatáshoz viszonyítva.

Az innováció nemcsak a szabadalmat jelenti, hanem ennek teljes folyamatában történő végigvitelét (alapkutatás átvételét, a technikai megoldások kidolgozását és a piackutatást a termelés utolsó fázisáig). Magyarországon nagyon sokszor hiányzik az első feltétel, a tőke.

Alapvető követelmény, hogy legyen egy olyan törvény, amely azt biztosítja, hogy az új termékeknél az adók és a vámok segítsék, sőt szükségessé tegyék az újnak a termelésbe való felvételét, mert ez mindig is nehéz volt. Az első innovációs törvény 20 évvel ezelőtt az USA-ban ilyen szempontokat figyelembe véve készült el, és sok állam követte őket. Magyarországon ez is hiányzik. Ha nincs innováció, akkor a kezünket adjuk el olcsó áron a termékeink, illetve az abba építhető „eszünk" helyett – mondotta Pungor akadémikus. Amíg Finnországban 20 évvel ezelőtt egy csúcstechnológia eladása után 8-10 vásárlásra került sor, addig mára (20 év után) egy csúcstechnológia vételére 6-8 eladás jut.

Az IBM Magyarország képviseletében Ákos György kereskedelmi igazgató tájékoztatta a jelenlévő hallgatóságot arról, hogy a közeljövőben milyen technikai lehetőségek közül választhatnak a média területén dolgozó szakemberek.

Előadásának keretében részletesen kitért az IT szerepére a médiában és a tartalomszolgáltatásban. Beszámolt a jelen és a közeli jövő kihívásairól, melyekkel a tartalomszolgáltatók szembesülnek.

Ismertette az IBM által – jelenleg – a média iparág számára kínált komplex megoldásokat, legfőképpen a video-tartalomra koncentrálva. A prezentációnak egyik érdekes része volt a modern televíziók alapjául szolgáló digitális archívum bemutatása.

Az előadás utolsó részében bemutattak megvalósult média-esettanulmányokat, melyek közül az egyik legjelentősebb a CNN televíziónál bevezetett IBM rendszer volt.

Pungor akadémikus előadásában a hazai innováció fontosságára hívta fel a figyelmet a szekció első előadásában. Az egyik ilyen jelentős magyar innovációs műhely a DIGITON Kft. A cég első embere, Bálint Zoltán ügyvezető igazgató hétvégi tárgyalásait megszakítva tartotta meg igen érdekes és minden hallgató figyelmét lekötő szakmai előadását. Előadásának azt a címet választotta, hogy „Új lehetőségek az interaktív televíziózásban és a televíziós nézettségmérésben". Ennek az is nagy jelentőséget adott, hogy a konferencia vezérvonala a magyar televízionéző személye volt. Arról beszéltek az előadók, hogy a minőségi televízionézőt hogyan lehet a legjobban kiszolgálni, és itt nagyon lényeges az, hogy az ő igényét a valóságban – torzításmentesen – közöljük a szolgáltató televíziós társaságokkal.

Az utolsó két előadásról részletesebben lapunk következő számára olvashatnak.

Helyesbítés:

11-dik számunkban megjelent:

Koszó Károly. Adatraktár-kezelés, üzleti intelligencia az SQL Server 2000-rel helyett,

Koszó Károly cikk alapján összeálllította, tömörítette Szilasi Hedvig

Kinek így, kinek úgy!

SIMONYI ENDRE

villamosmérnök

Ez az egyesített mérlege az iFORUM és a COMDEX/Las Vegas 2001. évi rendezvényeinek.

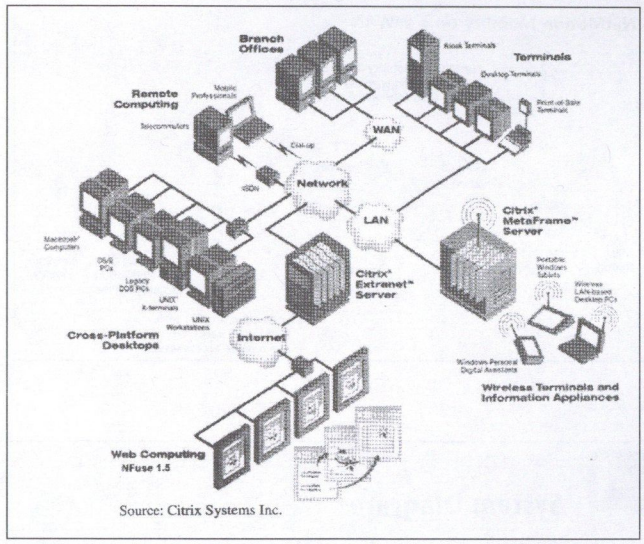
A COMDEX rendezvényeiről, különösen az őszi Las Vegas-iról már biztosan sokszor hallottak az olvasók, hiszen ez a legnagyobb amerikai számítástechnikai rendezvény. A másik viszont valószínűleg nem ismert. A számomra is meglepően nagy orlandói (Florida) rendezvény egyetlen magyar résztvevője voltam, ezért írok erről is.

Most negyedszer rendezték meg az iFORUM-ot, a COMDEX viszont már a huszonkettedikig jutott el. Az iFORUM eddig folyamatosan növekedett. A COMDEX 2000-ig (a nyolcvanas évek közepétől kezdve) szintén, de területe már 2000-ben is mintegy negyedével csökkent, és a csökkenés most a harmadára nőtt.

Az iFORUM egy informatikai cégnek (Citrix) a saját rendezvénye, ahol a cég termékeit és az azokhoz kapcsolódó megoldásokat, eszközöket mutatják be, de még ma sem akkora, mint a COMDEX. A nyitó plenáris előadáson is csaknem feleannyian vettek részt, mint a COMDEX Bill Gates-előadásán. Az iFORUM mindössze egy kétnapos előadás-sorozat és egy háromnapos kiállítás volt.

Mivel a Citrix név itthon kevesek számára ismert, ezért röviden bemutatom. A cég olyan szoftvereket fejleszt és gyárt, amiket használva vegyes platformú számítógépes hálózatok hozhatók létre. Ehhez alkalmazásszervereket és portálokat kiszolgáló szoftvereket készítenek. Ezek segítségével mind fix, mind mobil-, mind vegyes hálózatokat használhatnak, mert egységes kapcsolódási felületet láttak az alkalmazók. A cég ezen a területen vezető szerepet játszik. Ez alapján érthető, hogy a rendezvény kiállításán kiállító olyan neves cégek, mint a COMPAQ, a Computer Associates, a Dell, az EMC, a Hewlett-Packard, az IBM, a Microsoft, a Cable&Wireless, a National Semiconductor, a ViewSonic, a Wyse, összesen 67 vállalat miért dolgozta ki a Citrix-termékekhez illeszkedő megoldásokat, és azokat miért itt mutatták be.

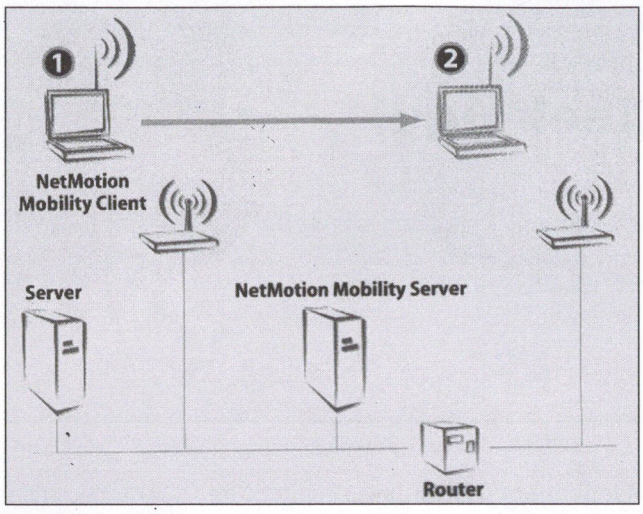
A Citrix a MetaFrame alkalmazásszolgáltató szoftverből, az NFuse alkalmazásportál-szoftverből, a Citrix Extranet VPN-szoftverből, az XPS portálszoftverből, alkalmazásmenedzselő termékekből, valamint a rendszer magjaként szolgáló szervertechnológiából (Citrix Independent Computing Architecture, ICA) álló család termékeit gyártja és forgalmazza. Egy tipikus nagyvállalati alkalmazás látható az 1. ábrán.



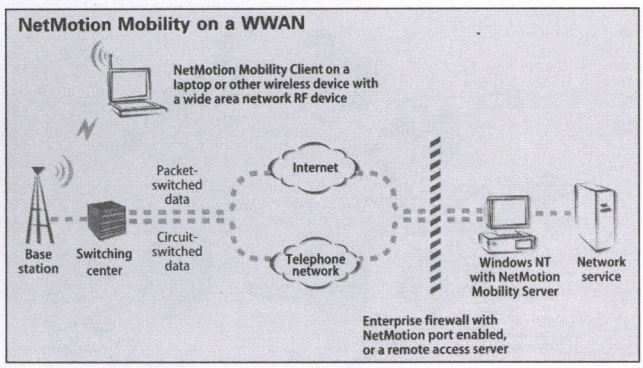
1. ábra

A Citrix-felhasználók közé tartozik a legnagyobb 500 amerikai vállalat kilenc tizede, az európai vezető 500 több mint fele (pl. a Cingular Wireless – a második legnagyobb amerikai vezeték nélküli szolgáltató –, a Dana – az autógyáraknak gépkocsialkatrészt, részegységet szállító cége –, a Kodak, a Jaguar, a DaimlerChrysler). Itt jelentette be a Citrix a „South Beach" elnevezésű portáltermékét, amit Mark Templeton, a cég elnök-vezérigazgatója a konferencián tartott nyitó előadásán a „virtuális munkahely" alapjának mondott. Ezzel az alkalmazott bárhonnan, bármikor és bármilyen internet-elérési eszközzel hozzá tud férni munkahelyi adataihoz. Az EMC elnöke egy demonstrációt is tartott előadása részeként, amelyben bemutatta, hogyan tudnak a MetaFrame és az EMC Symmetrix Remote Data Facility segítségével a hálózaton keresztül helyreállítani egy összeomlott rendszert.

A kiállításon és az előadásokban is kiemelt szerepet kapott a mobilhálózatok témaköre. A NetMotion cég NetMotion Mobility termékére alapozott WLAN (Wireless LAN) és WWAN megoldásait mutatom be a



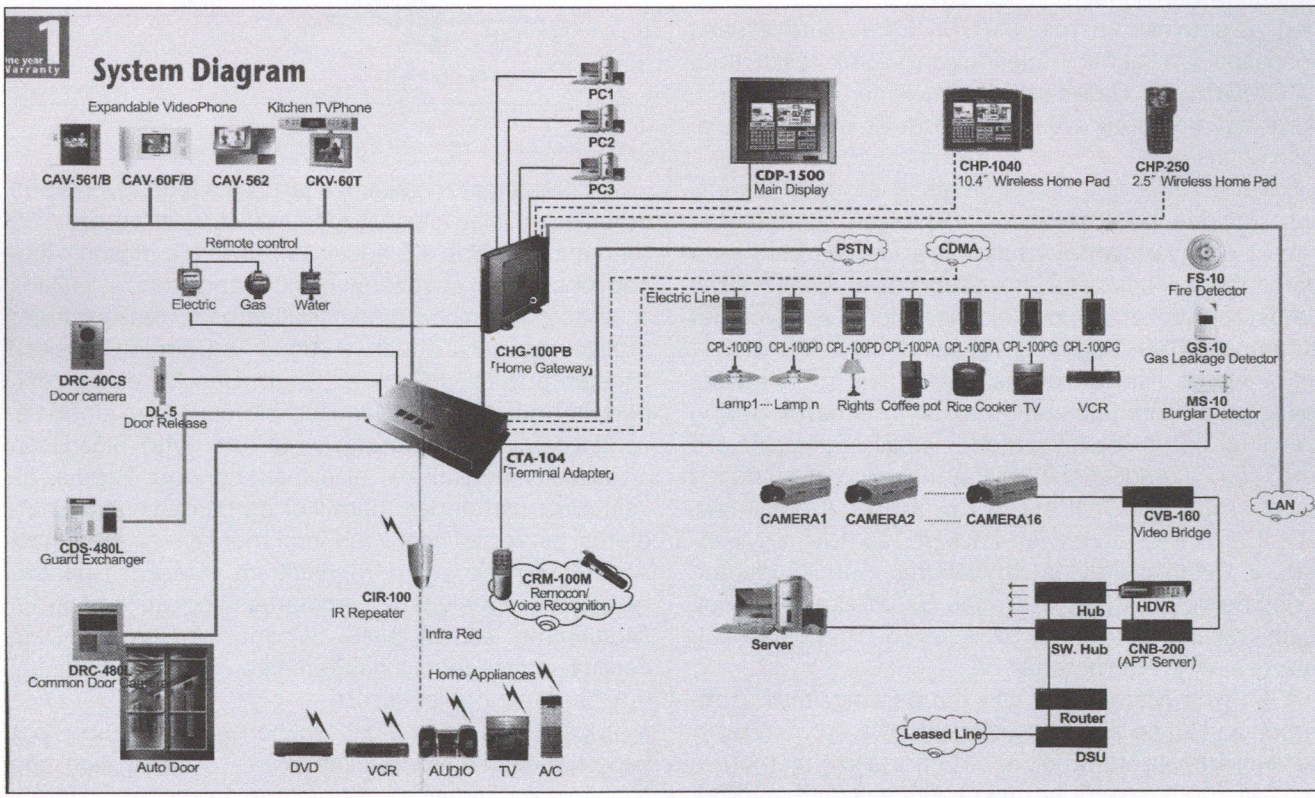
2. ábra



3. ábra

2. és 3. ábrán. A 2. ábrán az 1 jelű NetMotion Client segítségével egy hordozható számítógépen keresztül egy alhálózatot lehet a hálózathoz csatlakoztatni, felvéve egy új IP-címet úgy, hogy a rácsatlakoztatás nem okoz a vonalválasztónak a csomagküldés közben szakadást. A 3. ábra egy szokásosnak tekinthető nagyvállalati megoldásban mutatja a helyét a NetMotion programjainak.

A COMDEX számos ismert cég távollétével „vonta magára a figyelmet". Az ezáltal teremtett lehetőséget használta ki sok nem amerikai ország, így elsősorban Tajvan és a Koreai Köztársaság. Ez utóbbi egyik kiállítója, a COMMAX mutatta be – a még inkább csak a luxusházaknak szánt – házi hálózatát, melyhez nem kell új épületen belüli vezetékeket létesíteni. A 4. ábrán látható hálózat jellemzője a más hálózatokhoz (LAN, CDMA, ADSL, PSTN) kapcsolódás lehetősége, az illeszkedés a kaputelefonhoz és más belső/külső telefonokhoz, valamint a biztonsági (tűz-, gázömlés-, riasztó-) rendszerekhez, a szabályozórendszerek bemeneteinek (hang, táv) vételi képessége, bizonyos korlátozott képességű hangfelismerés. A rendszer egy 10,4 " képernyő méretű, vezeték nélküli csatolású eszközről (Wireless Home Pad) irányítható. Az említett jellemzők miatt a házi hálózat széles sávon kapcsolódik az internetre, a házon belül egy Ethernet-hálózatot ad. A cég nemcsak az általa gyártott részegységek, hanem az ábrán látható teljes rendszer szállítását is vállalja, telepítéssel, beüzemeléssel együtt. Az Egyesült Államok bármely részére megszervezi az üzembe helyezést, és még a szervizről is gondoskodik, akkor is, ha a ház a sivatagban vagy a magas északon van. (Talán nekünk sem ártana, ha a vállalkozások nálunk is ilyenek lennének!)

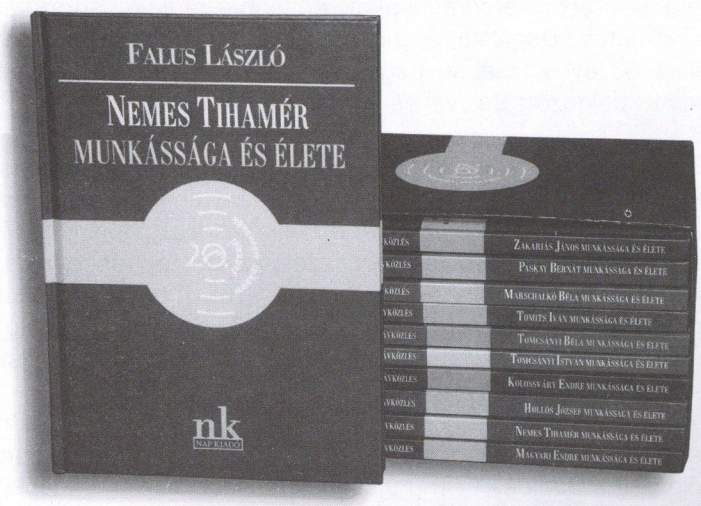


4. ábra

Könyvet ajánlunk

December hónapban rendkívül szép termés volt új kiadású könyvekből. Találunk köztük szakmai könyveket, történeti könyveket is, sőt olyat is, melyet szakmánk egyik kiemelkedő egyénisége írt, de a tartalma egyáltalán nem távközlés vagy informatika.

A jeles postamérnököket, a XX. század magyar mérnökeit bemutató könyvsorozat első 10 kötete elkészült. A szervezés munkáját a posta és a Távközlési Múzeumi Alapítvány vállalta magára. Az alapítvány igazgatónője, Kovács Gergelyné jól válogatta össze azt a 10 kiemelkedő távközlési egyéniséget, akiknek tevékenysége a század első 60 évének munkájában és fejlődésében meghatározó volt.



Hollós József nemcsak mint mérnök, hanem mint vezető is, a posta távközlési feladatainak megindulásakor tökéletesen látta, hogy milyen irányban érdemes haladni. Hollndonner László, e kötet szerzője a tényszerű adatokon túlmenően jól érzékelte ennek a több szakma iránt érdeklődő, humanista nézetű alkotónak az életét.

Marsalkó Béla kiváló vegyészként az anyagvizsgálatok és az ehhez kapcsolódó mérési módszerek kidolgozásában tűnt ki. Hosszú időn keresztül a PKÁ igazgatója volt, akinek vezetési nézetei egy életre befolyásolták fiatal munkatársait. Nem kizsákmányolta, hanem ösztönözte a kutatókat, és ezzel olyan kiváló eredményeket ért el, hogy irányítása alatt a posta minden műszaki jellegű döntésében vakon támaszkodhatott az állomásra. A berendezésszállítók is kritika nélkül elfogadták az állomás mérnökeinek véleményét, minősítését. Minderről rendkívül hűen Pálvölgyiné Láng Éva számol be.

Magyari Endre neve mindenki előtt ismeretes, hiszen az első stúdió, amit egy bútorszállító kocsiban hozott létre, jelképpé vált. Az a megnyitó műsor, ahol hegedült, indította el a mai műsorszórást. Ezenkívül geometriakönyveket írt, foglalkozott a gravitáció mérésével és megértéséhez elméletet dolgozott ki. Ez a sokoldalúság azonban nem gátolta abban, hogy még időskorában is végezzen hullámterjedési méréseket, melyek alapján a későbbiekben utódai és tanítványai sikereket értek el a nemzetközi frekvenciakiosztásban. A kötetet egyik munkatársa, Koós Árpád állította össze. Ugyancsak ő kutatta fel Tomits Iván munkásságát és életét. A CCIT-ben is elismert kutató a reflexió és az áthallás kapcsolatának felismerése után az erre vonatkozó ajánlásokat kidolgozta. Ennek a munkának kiemelkedő érdeme, hogy egy olyan mérnököt mutat be, akinek tevékenysége nem oly mértékben ismerős, mint az előbbiekben bemutatott kutatók és vezetők.

Nemes Tihamér igazi polihisztor. Az állomáson már a II. világháború előtt jelentős eredményeket ért el a televíziós közvetítések megvalósítása területén. Az 50-es években az adástechnika és a képátvitel kérdéseinek tisztázásával a hazai televíziózás egyik megalapítója lett. Mindez azonban nem kötötte le összes energiáját. Egyetemi előadásait emlékezetessé tette, hogy két kezével egyszerre különböző ábrákat tudott rajzolni. Az egyetemi újság, a „Vicinális dugóhúzó" karikatúrái is az ő nevéhez kapcsolódnak. Az informatika területén az aspiránsok irányítását végezte. Falus László nemcsak a tények ismertetésével, hanem az egyéniség bemutatásával is hozzájárult a sorozat sikeréhez.

Paskay Bernát munkássága átfogta a posta és a távközlés szinte valamennyi területét. Légvezeték-építéssel kezdte, majd központos lett. Dolgozott a posta Tanulmányi Hivatalánál, a rádiózás kezdeti szabványosítá-

sában is szerepet vállalt. Széles látóköre alkalmassá tette, hogy 1921–1932-ig a Posta Kísérleti Állomás igazgatója legyen. Ezalatt is aktív részt vállalt a rádiózás nemzetközi szabályozásában. Erről a gazdag életútról Dósa György készített áttekintő képet sok érdekes részlettel és fényképpel kiegészítve.

Tomcsányi István néhány évi üzemi gyakorlat után a Posta Kísérleti Állomáshoz került. Öt évvel a diploma megszerzése után főmérnökké nevezték ki, és a rádió osztályt irányította. Több stúdió megépítése fűződik a nevéhez. A 30-as években már a televíziózás kérdéseivel is foglalkozott. A II. világháború után Miskolcra, majd Berzékre vonult vissza, és élete utolsó két évtizedében már nem tudta ismereteit hasznosítani. Erről a szomorú végű életútról ifj. Heckenast Gábor írt könyvet.

Tomcsányi Béla is 1926-tól a Posta Kísérleti Állomáson dolgozott. Nagybátyjához hasonlóan ő is a rádiózás területén ért el eredményeket. Később a rádió-műsorszórás üzemeltetésével foglalkozott és a nagy adók folyamatos vizsgálata, ellenőrzése volt a feladata. A háború után a stúdió újjáépítését sikerrel befejezte, de élete 53 éves korában tragikus véget ért. Ennek a könyvnek Heckenast Gábor volt avatott szerzője, aki együtt dolgozott Bélával és utódja is lett.

Kolossváry Endre a MÁV-nál kezdte mérnöki munkáját, majd Baross Gábor miniszter másik 11 mérnökkel együtt, 1887-ben a postához irányította. Néhány év után az anyagvizsgáló laboratórium vezetésére kapott megbízást, majd a Posta Kísérleti Állomás igazgatója lett. Munkája eredményeként az állomás jelentős szerepet kapott a távíró- és távbeszélő-hálózat építésében, a központok kialakításában. Ennek megfelelően növekedett a létszám, és 1912-ben a Gyáli út egyik mellékutcájában önálló épületet kaptak. Később a posta műszaki vezérigazgató-helyettese és a 30-as évek közepéig a távközlés és műsorszórás műszaki fejlődésének meghatározója. Koós Árpád számos korabeli cikk felhasználásával számol be erről a sikeres életútról.

Zakariás János munkásságát elsősorban az eredmények népszerűsítése és játékos alkalmazása jellemezte. Rádióamatőr klubot alapított és működtetett számos fiatal bevonásával. Hosszú időn keresztül szerkesztője volt a Rádióélet című újságnak, és igyekezett mindenki számára érthetővé tenni a rádió működését és jelentőségét. Balás B. Dénes, a kötet szerzője vonzóan mutatja be ennek a széles érdeklődési körű embernek a szerepét a magyar rádiózásban.

Dr. Kovács Gergelyné munkája mindenki számára új információkat adott és számos jelentős mérnökegyéniség tevékenységét megörökítette. Természetes, hogy az olvasók újabb javaslatokkal állnak elő. A felsorolt 10 postamérnökön kívül még sokat tartanának érdemesnek arra, hogy munkásságuk hasonló kis könyvecskében megjelenjen. Ugyanakkor felmerül a kérdés, hogy a hazai távközlési mérnökök sorából szabad-e kihagyni azokat a nem a postánál dolgozó kutatókat-fejlesztőket és iparosokat, akiknek a tevékenysége szintén befolyást gyakorolt a magyar távközlés fejlesztésére. Munkásságuk sok esetben túlnőtt az ország határain és termékeiket Európa több országában, sőt más kontinenseken is sikerrel alkalmazták. Reméljük, hogy ennek a sorozatnak a sikere meggyőzi az ötletadót, hogy 2002-ben tovább folytassa értékes munkáját.

Kozma László: Egy Kossuth-díjas börtönévei

Kozma László naplóját a 2002-ben esedékes 100. születésnap előkészítésének jegyében adták ki. A munkához Kovács Győző írt méltatást és az ERICSSON támogatta a megjelenést.

A napló a standard per vallatási technikáját, az államosítás érdekében szükséges szabotázs bizonyítását, az egész hamis ügy hátterét és módszereit mutatja be. Utólag szinte elképzelhetetlen, hogy milyen sokan működtek közre egy koncepciós per sikerében, és milyen sok áldozatot követelt egy államosítási folyamat előkészítése. A későbbiekben kiderült, hogy ennek ellenére az állam fizetett a volt tulajdonosoknak valamennyi kártérítést, de ez csak növelte az elítéltek elkeseredését és rossz hangulatát.

A könyv értékét növeli és a mérnökök számára tanulságul szolgál, hogy Kozma László kínzások és megaláztatások közepette sem vesztette el a kedvét a műszaki újdonságok keresésében. Amint lehetősége nyílt, hogy egy kicsit kedvezőbb körülmények között töltse fogsága éveit, azonnal hozzákezdett új konstrukciók

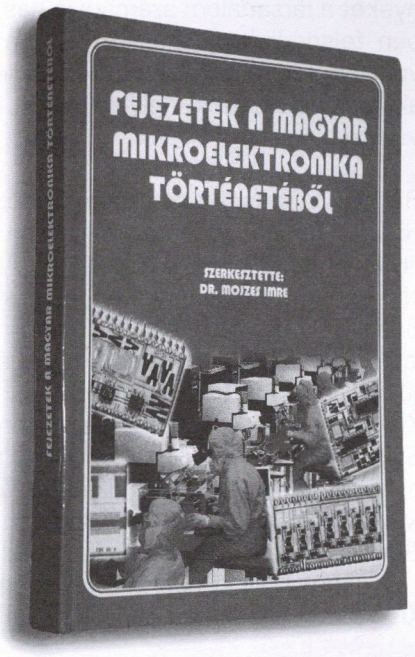
tervezéséhez. Számítógépet és központot konstruált. Már ekkor tisztán látta, hogy a kapcsolástechnika jövője szorosan kapcsolódik a számítástechnikához. Eredményeit szabadulása után realizálta.

Ajánljuk ezt a könyvet egyrészt azért, mert reális képet ad a Sztálin–Rákosi-korszak módszereiről, az 1949–53-as évek parancsuralmi rendszeréről. Érdekes olvasmány, mert a szerzőnek sok esetben utólag módja volt a hátteret is megismerni, mellyel még jobban leköti az olvasók figyelmét. A stílus pedig irodalmi, választékos és csak abból látszik, hogy milyen a börtönélet, amikor idézi a foglárok, vallatók és ávósok szövegeit. Igazi irodalmi alkotás.

Végül érdemes abból a szempontból is végignézni, hogy napjainkban sokan azt mondják, nem tudok alkotni, mert a klíma levegője zavar, vagy nem megfelelő a szoba elhelyezése, megvilágítása, és ezért nem tudtam megvalósítani főnökeim elvárását. De számtalan egyéb hivatkozási alap is van, mint például későn megérkező alkatrészek, nehezen hozzáférhető irodalmak, vagy rosszul megfogalmazott célok. Ha ezeket az ürügyeket összevetjük azokkal a körülményekkel, melyek között Kozma László alkotni tudott, akkor látjuk, hogy az igazi tehetséget semmi nem gátolja meg az újdonságok kidolgozásában.

A mai mérnökök számára feltétlenül ajánlott olvasmány és minden elismerésünk azoké, akik a naplót feldolgozták, és szép kivitelben közreadták.

Dr. Mojzes Imre (szerkesztő):
Fejezetek a magyar mikroelektronika történetéből



2001 végén jelent meg dr. Mojzes Imre szerkesztésében és a mikroelektronikai szakma számos kiválóságának közreműködésével egy közel 350 oldalas áttekintés a mikroelektronika elmúlt 100 évének hazai eredményeiről és a sikerekben szerepet vállaló kutatók, mérnökök munkájáról. A könyv bemutatja, hogy a mérnökök mindent megtettek a hazai mikroelektronikai ipar sikereinek előmozdításáért.

A könyv a tudománytörténeti előzményekkel kezdődik, majd áttekintést ad a hazai mikroelektronikai kutatásokról, fejlesztésekről. Ezt követi néhány jelentős hely bemutatása. Zanati Tibor beszámolót ír a Tungsramban elért eredményekről, amely a fényvezető-fejlesztés, -gyártás és -értékesítés terén minden elismerést megérdemel. Dr. Herman Ákos a HIKI-MEV történet áttekintésével bizonyítja, hogy Magyarországon is lehetett volna az eredményekkel a nemzetközi élvonalba kerülni, azonban számos szerencsétlen körülmény, és végül a rendkívül ambiciózus beruházások szerencsétlen módon tűz áldozatává váltak.

Jelentős két nagy gyártó-fejlesztő vállalkozás mellett külön fejezet foglalkozik a mikroelektronika hazai kezdeteivel, olvashatunk a vékonyréteg-kutatás eredményeiről és megismerkedhetünk a magyar mikroprocesszor történetével. A Budapesti Műszaki Egyetemen is értek el eredményeket a hibrid integrált áramkör kutatásában, de ennek legnagyobb értéke, hogy a legújabb eredmények folyamatosan megjelentek az oktatásban is.

Olvashatunk az optoelektronikáról, a magyar szilíciumvölgy ígéretes terveiről. A múlt mellett optimista előretekintés is szerepel a könyvben.

A fejezetek felsorolása kapcsán nem említettük meg a kiváló szerzők és közreműködők nevét, nem említettük meg azt a rengeteg kutatót, akiknek munkájáról a könyv megemlékezik. Ezt az olvasókra bízzuk. Egy szerzőt azonban szeretnénk kiemelni: dr. Szent-györgyi Zsuzsát, aki „Magyar elektronikai ipar: meghalt vagy megölték" címmel értékelte az 1990–94-es időszak eredményeit vagy eredménytelenségét. A fejezet összhangban van az egész könyv tartalmával, elégtételt ad a kutatóknak és bizonyítja, hogy akik e területen dol-

goztak, minden tőlük telhetőt megtettek, nem rajtuk múlt, hogy ez az iparág nem vált meghatározóvá a hazai gazdaságban.

A szép kiállítású könyvet ajánljuk mindenki figyelmébe. Mint szakmai áttekintés, magas színvonalon mutatja be a kitűzött célokat és az elért eredményeket. Mint történeti könyv, helyes arányérzékkel emlékezik meg a területen dolgozókról. Végül érdemes a szerkesztői útószó néhány mondatát idézni, amely a sikerekkel és kudarcokkal átszőtt könyv végén optimizmust ad: „A legnagyobb tanulság az, hogy megláttam azt az erőt, amely ebben a szakmában mindig is jelen volt, és egyértelművé tette azt, hogy ez meg is maradt. Azok a kezdeményezések, amelyek a kilencvenes évek elején születtek, többségükben sikeresek voltak. Ezek ... kisebb, de életképesebb egységekben jelentek meg. Egy későbbi történeti mű tehát sokkal több szereplőről fog szólni, de biztosan kevesebb lesz az illusztrációként mellékelt államigazgatási határozat." Reméljük, hogy a szerkesztőnek igaza lesz.

A XXI. századi kommunikáció új útjai

A Westel támogatásával, az MTA Filozófiai Kutatóintézete kiadásában Nyíri Kristóf szerkesztett egy értékes tanulmánykötetet. A közel 300 oldalas kötet 11 tanulmányt, előszót és könyvismertetéseket tartalmaz. A szerzők főként filozófiai, szociológiai szempontból vizsgálják a hirtelen kifejlődött távközlés és informatika hatását az egyénre és a társadalomra. A különböző szempontok szerint megírt tanulmányok közös célja, hogy a műszaki eredményeket a társadalom számára is hasznossá tegyék. A következőkben felsoroljuk a tanulmányok címeit, mely segít abban, hogy vonzóvá tegye a könyvet, és akik egy kicsit a jelenségek mögé akarnak nézni, azok mely területen, milyen kérdésekre kaphatnak választ.

Benczik Vilmos: Másodlagos szóbeliség és mobiltelefónia
Rituper Tamás: Jobbára ártalmatlan: chat a wapon
Nyírő András: Miért jó az oplogó? Az új vizuális népművészetről
Nyíri Kristóf: Képjelentés és mobil kommunikáció. Vázlat
Buda Béla dr.: Az elektronikus kommunikációs kultúra árnyoldalai? Aggályok és tények az internet és a mobiltelefon visszaélő, ill. túlhasználatával kapcsolatban
Krajcsi A.–Kovács K.–Pléh Cs.: Internethasználók kommunikációs szokásai
Sükösd Miklós–L. László János: Az m-kormányzat (h)őskorszaka. Hogyan használják a mobilt a magyarországi önkormányzatok, és ki fizeti a számlát?
Mester Béla: Politikai közösség és a médiumok. A felhasználó mint állampolgár
Gedeon Péter: Piac és pénz a mobil információs társadalomban
Laki János–Palló Gábor: Projektvilág és informális hálózat a tudományban
Kiss Ulrich SJ: A kommunikáció teológiája

Az információs társadalom felé (Tanulmányok és hozzászólások)
Szerkesztette: Dombi Gábor és Lafferton Emese

Az információs társadalommal foglalkozó irodalom hatalmas. Mi indokolhatja egy új könyv megjelentetését ezen a területen? Nos, ilyen indok lehet a specifikus és/vagy változó környezet, új statisztikai és egyéb kutatási eredmények, az információs társadalommal kapcsolatos párhuzamos – olykor polemizáló – nézetek ismertetése, csokorba foglalása.

Ez a gyűjtemény valamennyi felsorolt kritériumnak eleget tesz. A megcélzott és részleteiben is vizsgált környezet hazánk: Magyarország, amely 2001. május 17-én lépett az információs korszakba. Ezen a napon jelentette be Stumpf István kancelláriaminiszter a Nemzeti Információs Társadalom Stratégia (NIST) elkészültét. Új, részletes statisztikák mutatják a világ országainak, köztünk hazánknak az eredményeit és elmaradását az információs társadalom mutatóiban. Érdekes tanulságokat lehet levonni a posztszocialista országok információs társadalomképének fejlődéséből, különösen az éllovas USA célkitűzéseivel összevetve. Napjainkban pedig szomorú aktualitása is van az egész folyamatot meghatározó internettel kapcsolatos jogi megfontolásoknak és lépéseknek. Végezetül, az átalakulás jelenlegi felgyorsult időszakában különleges jelentőséget kap a területért felelősséget érző és viselő politikusok véleményének megismerése. Mindezt megtaláljuk a könyvben.

A tanulmánykötet Dombi Gábor által írt bevezetője önmaga is egy rövid tanulmány Információs társadalom és politika címmel. Felveti az internet felhasználásának felelősségét, szabályai kialakításának szükségességét. Alapvetőnek tartja a demokrácia megerősítését és a társadalmi bizalom megnyerését. A tartalom legnagyobb szűrőjének az emberi szellemet tartja. Ezért látja szükségesnek az oktatás színvonalának emelését – szemben a tartalom korlátozásával. Fontos állítása, hogy az informatikai forradalom véget ért, most az energetika, majd a biotechnológia és az orvostudomány új korszaka következik. Nekünk azonban most az információs téren van feladatunk: éppen a fejlődéshez felzárkózást biztosítja a szabad hozzáférés az információs kincshez. „Az informatika jelentősége ... az eszközök felhasználása által létrejött jobb életminőségben rejlik."

A kötet első részét kitevő tanulmányok és fő állításaik az alábbiak.

Szakadát István tanulmányának címe: Tartalom mindenek felett, infrastruktúra mindenek alatt. A digitális gazdaságtan két alapelvét megtestesítő jelmondat első felének állítása lényegében azt a sokszor elemzett, sőt vitatott tételt összegzi, hogy az információs társadalom meghatározója a tartalom és annak kommunikációja. Az infrastruktúra eszköz, a számítógép tudásautomata. Ennek legfontosabb jelentése az információ, a tudás újrahasznosításának lehetősége. A második állítás azonban arra utal, hogy a tartalom kifejezése, részben a technikai környezet hatása alatt, gyakorta nem éri el azt a szintet, amellyel ki tudná használni az infrastruktúra lehetőségeit, amellyel valóban újrahasznosíthatóvá formálná a tudást – olykor globális léptékben.

A tanulmány a digitális gazdaság jellemzésére makrogazdasági mutatókat használ. Ezek alkalmasak az országok összehasonlítására, jellemző pozíciójuk meghatározására. Kimutatható például, hogy az internethasználók lakossági arányában hazánk nem áll túl jól, a posztszocialista országok közül Szlovénia, Észtország, Szlovákia, Lettország és Lengyelország is megelőzi, igaz, az utolsó kettő csak kevéssel. A sok bizonytalansággal terhelt egyszeri adatok helyett célszerűbbnek látja a szerző az idősorok elemzését. Számos ország top level domainek alatti hostok számáról mutat be 1990 óta gyűjtött adatokat. Ezek alapján a fejlődés jellege szerint három csoportba sorolja az országokat: az északi országokba, a középmezőnybe és a leszakadókéba. Hazánk – az országok jelentős részével együtt – a középmezőnyhöz tartozik. PC-ellátottságban Magyarország pozíciója viszonylag gyenge. A szerző véleménye szerint ez az internet gyorsabb terjedésének legfontosabb akadálya.

Tamás Pál Az elkésettek stratégiái, avagy a posztszocialista információs társadalom jövőképéről címmel írt tanulmányt az információs társadalmak kelet-európai állapotáról. A tanulmány az információs társadalom értelmezési kísérleteinek elemzése után az információs technológiák globalizációs hatásait mutatja be a volt szocialista országokban. A fejlesztési stratégiákat elemezve bemutatja a „főútvonal" és „mellékútvonal" megközelítéseket, és egyes országok stratégiájának fokozatos átértékelődését az idő és a változó feltételek és körülmények eredményeként. Rendkívül érdekes a volt szocialista országokban, mint „posztkoloniális" társadalmakban lejátszódó folyamatok elemzése. Csak címszavakban a következő részek tartalma: információs és kommunikációs mítoszok, nemzetközi innovációs rendszerek és a megjelenő új információs rend, technológiai mozgáspályák, információs infrastruktúra, az információs ágazatok és technológiák szerepe a gazdasági növekedésben. A dolgozat befejezésül a „kiberhatárvidék" hipotézisét ismerteti.

Eszerint a kelet-európai térség az informatikai társadalom vonatkozásában az „Amerikai Nyugat" analogonja, ahhoz hasonló előremozdító hatásokkal és veszélyekkel. A dolgozat függeléke az információs társadalom fejlettségének mérésére és az egyes társadalmak összehasonlíthatósága céljából statisztikai adatokat közöl. Érdekes ezen adatok és az előző tanulmány mérőszámainak összehasonlítása.

Mayer Erika tanulmányának címe: Virtuális tangó a tartalomszabályozás körül, avagy két lépés előre, egy lépés hátra az internet normatív szabályozásában. Érdekes a jogszerűtlen és a nem illő (az eredeti szóhasználatban: illetlen) kategóriák bevezetése és annak kihangsúlyozása, hogy a kettő közötti határ országonként változik. Ez nehezíti az egységes nemzetközi jogi normatívák megalkotását. A jog alkalmazását pedig az internet tulajdonságai különösen megnehezítik. Teszik ezt olyan általánosan elítélt tartalmak esetén is, mint a gyermekpornográfia, erőszak vagy rasszizmus.

Ezzel együtt az erotika, a szexualitás, a legális pornográfia interneten való megjelenésének korlátozása a kiskorúak és az emberi méltóság védelmének méltányolható célja mellett komoly üzleti érdekeket sért.

Az USA és az EU eddigi jogalkotásának és -alkalmazásának tapasztalatai arra utalnak, hogy a minimálisan szükséges állami beavatkozás mellett az önszabályozás és a megfelelő technikai (szűrő) megoldások nyújthatják a lényegi megoldást.

Lassányi Tamás: A véleménynyilvánítás szabadsága az interne-ten témakörét járja körül. A szerző szkeptikusabb az önszabályozás hatékonyságával kapcsolatban, mint az előző tanulmány. Ugyanakkor a személyes szelekció lehetőségének tekintetbevételével rendkívül fontosnak tartja megtalálni a jogi szabályozásnak és korlátozásnak azt a mértékét, amely nem sérti az internet egyedülálló lehetőségeit a gondolat kifejezésében, terjesztésében és cseréjében; azt a mértéket, ahol az internet szabadsága sem szenved csorbát, és az állam, illetve a társadalom érdekei sem sérülnek.

Nagy Adrienn tanulmányának témája Az USA kormányzata az információs társadalomban. Ismerteti a Clinton–Gore-kormányzat tevékenységét az állampolgárok digitális egyenlőségének elérése érdekében.

A kötet második felében az alábbi rövid tanulmányok találhatók:
Informatikai Érdekegyeztető Fórum: Magyar Informatikai Charta
Magyar Bálint: Információs társadalom: az eddigi lépések
Rogán Antal: A digitális Magyarország
Sík Zoltán: Az Informatikai Kormánybiztosság első évének eredményei
Simon Gábor–Szabó Zoltán: Az információs társadalom kialakulásának eddigi lépései Magyarországon
Stumpf István: Változások az információs társadalomban. Magyarország polgárai és szervezetei számára

Hírek

A Siemens IC Mobile ágazata és a Siemens leányvállalat „designafairs" európai és ázsiai diákok számára tervezési tábort indít márciusban. Itt két tutor segítségével szemeszterenként tíz különböző szakon tanuló diák fogja a távközlés különféle kérdéseit öt hónapon át tanulmányozni és feldolgozni, végül eredményeiket alkotó módon átültetni a gyakorlatba. A tanulmányozható kérdések a „digitális" társadalom tudati változásaira, a kultúraváltásra vonatkoznak, valamint a kommunikáció ebből adódó új koncepcionális modelljére. A 2002. márciustól júliusig, részben Sanghajban megtartandó első szemeszter résztvevőinek kiválasztása megtörtént. A designlab működésének költségeit, beleértve a diákok ösztöndíját, a Siemens IC Mobile fedezi. A szeptemberben induló második szemeszterre pályázni lehet az alábbi címeken:

info@designlab-siemens-mobile.org, vagy
Anke Gebhard, Tölzer Strasse 2c, 81379 München.

❖ ❖ ❖

A Sun Microsystems, a Disney és a Pixar koprodukcióban egész estés animációs filmet készített Sun technológiával. A film jeleneteit a Pixar rendszerfarmján készítették el, ahol összesen 250, Solaris operációs rendszert futtató középkategóriás Sun Enterprise 4500 szerver gondoskodott a grafikus számításokról. A gépeken közel 4 terabyte memóriát használtak. A Monsters, Inc. című film már az amerikai mozik műsorán szerepel, a magyarországi bemutatóig a film honlapját érdemes meglátogatni.

KÖZLEMÉNY

A PanTel Novum Távközlési Szolgáltató Korlátolt Felelősségű Társaság (1134 Budapest, Tüzér utca 39–41.) ezúton tájékoztatja jelenlegi és leendő ügyfeleit, hogy a Hírközlési Felügyelet a BH 12767-1/2001. számú, 2001. december 14-én jogerőre emelkedett határozatában a PanTel Novum Kft. részére közcélú adathálózati (adatátviteli és bérelt vonali) szolgáltatások nyújtását engedélyezte.

A Szolgáltató által nyújtani kívánt szolgáltatás

Menedzselt Nagybiztonságú Szélessávú (MNSZ) adatátviteli szolgáltatás

Az ATM- (Aszinkron Transzfer Mód) technológián alapuló menedzselt nagybiztonságú szélessávú adatátviteli szolgáltatás több helyszínt összekötő integrált információátviteli rendszer. Alkalmas ugyanazon a fizikai összeköttetésen keresztül hang- és adatátvitelre egyaránt. Az egyes összeköttetések sávszélessége dinamikusan, adott határok között változhat a forgalom függvényében, ezáltal a rendelkezésre álló kapacitás maximálisan kihasználható.

A felhasználóhoz olyan hálózati végberendezés kerül, amely a különböző alkalmazások által igényelt interfészek mindegyikét tudja biztosítani (pl. LAN kapcsolat és telefonközpontok közötti összeköttetés). Az így létrejövő integrált kapcsolat sávszélessége a különböző alkalmazások igényeinek megfelelően 2 Mbit/sec és 155 Mbit/sec között lehet, 1Mbit/sec-os lépésekben.

Analóg bérelt vonali szolgáltatás

Az „analóg bérelt vonali szolgáltatás" egy – a MOL Rt. analóg hálózatán kialakított – pont-pont közötti állandó kapcsolatú analóg áramkör, melynek sávszélessége 300 Hz – 3,4 kHz, az ITU-T M1020 ajánlásának megfelelő paraméterekkel beszéd célra vagy (beszédsávi modemmel) adatátviteli célra.

Kiterjesztett használat szolgáltatás

A „kiterjesztett használat szolgáltatás" lehetővé teszi, hogy az Előfizető a telefonközponttól nagyobb távolságra (~km) elhelyezkedő analóg távbeszélő mellékállomását is elérhesse. A telefonközpont központi táplálású (CB) analóg mellékállomási vonalát egy CB/LB adapter LB táplálásúra alakítja és így továbbítja MOL Rt. távkábelén vagy analóg hálózatán keresztül, majd a végponton egy adapter visszaalakítja CB táplálásúra. Így tetszőleges távolságra hosszabbítható egy analóg mellékállomási vonal.

Bérelt vonali adatátviteli szolgáltatás

A „bérelt vonali adatátviteli szolgáltatás" lehetővé teszi az Előfizető részére, hogy két telephely között pont-pont jellegű (digitális) adatkapcsolatot hozzon létre. Az átvitel protokoll- és felhasználásfüggetlen transzparensátvitelt biztosít tetszőleges (adat-, videó- és multimédia-) alkalmazásokhoz.

Az Előfizetőnél elhelyezett végberendezés a szabványos adatkapcsolati interfészeket támogatja (ITU-T G.703, V.35, X.21). A szolgáltatás kiterjed az ITU-T (CCITT) ajánlásában előírt üzemszerű működésre és az egyedi előfizetői szerződésben rögzített igények kielégítésére.

Az adatkapcsolat sebessége n×64 kbit/s (n=1...31) vagy kis sebességű (150 bit/s – 33,6 kbit/s).

A Szolgáltató által vállalt kötelezettségek

A távközlési rendszer üzemzavarainak kategorizálását, az üzemvarok eseteit, a hibaelhárítás megkezdésének idejét és a meghibásodás bejelentésétől számítva a szolgáltatás visszaadási időpontját az alábbi táblázat tartalmazza:

1. sz. táblázat

Kategória	A hiba megnevezése	Az elhárítás megkezdése (1)	Szolg. visszaadása
I.	Adatátviteli áramkörök, amennyiben az átterhelésre az alternatív irány kiépített és annak biztosítására az előfizető szerződött.	2 órán belül	6 óra
II.	A távközlő rendszer gerincirányának megbénulása, Kiemelt fontosságú átviteltechnikai helyi irány megbénulása (pl. 5 vagy több adat áramkört tartalmaz), Több áramkörös, ill. több felhasználót kiszolgáló berendezések áramellátó egységeinek meghibásodása, vagy a 220 V-os betáplálásnak a megszűnése, I kategóriába nem tartozó adatátviteli áramkör meghibásodása.	2 órán belül	36 óra
III.	A távközlő rendszer nem kiemelt fontosságú átviteltechnikai helyi irányának megbénulása, A távközlő rendszer csoportszintű meghibásodása (kivéve, ha nincs benne élő áramkör), Az I. és II. kategóriába nem tartozó élő áramkörök meghibásodása.	A bejelentés napján	48 óra

(1) Az elhárítás megkezdését az ügyfélszolgálatnak történő bejelentés időpontjától kell számítani.

Általános minőségi paraméterek:

Minőségi mutatók:

Az 1. sz. táblázat I. kategóriájába sorolt áramkörök üzemzavar miatti kiesése 1 hónapban	<=1%
Az 1. sz. táblázat II. kategóriájába sorolt áramkörök üzemzavar miatti kiesése 1 hónapban	<=3%
Az 1. sz. táblázat III. kategóriájába sorolt áramkörök üzemzavar miatti kiesése 1 hónapban	<=6%

Szolgáltató által vállalt rendelkezésre állás (RÁ):

Szolgáltatás	RÁ %-ban
Adatátviteli szolgáltatás	
ATM szolgáltatás	99.7
Bérelt vonali szolgáltatás	
Analóg bérelt vonali szolgáltatás	99,00
Kiterjesztett használat	99,00
Analóg adatátviteli szolgáltatás	99,00
Digitális adatátviteli áramkör	99,70
Menedzselt bérelt áramköri szolgáltatások	99,70

PanTel Novum Kft. BH12767-1/2001. számú határozatában jóváhagyott vállalkozási feltételek szerinti távközlési díjszabása

Adatátviteli szolgáltatások

Díjtétel megnevezése	Mennyiségi egység	Nettó ár (Ft/hó)	Áfa	Bruttó ár (Ft/hó)
Menedzselt nagybiztonságú szélessávú adatátviteli szolgáltatás				
MNSZ előfizetési díj				
MNSZ interface E1 (2 Mb/sec)	db	163 478	40 869	204 347
MNSZ interface E3 (34 Mb/sec)	db	1 209 435	302 359	1 511 794
MNSZ interface STM 1 (155 Mb/sec)	db	3 289 668	822 417	4 112 085
MNSZ interface STM 4 (622 Mb/sec)	db	8 947 874	2 236 969	11 184 843
MNSZ átviteli sávszélességi díj				
MNSZ 2 Mb/sec CBR	km	6 976	1 744	8 720
MNSZ 2-8 Mb/sec közötti CBR 1 Mb/sec lépcső ár	1 MB/km	2 002	501	2 503
MNSZ 8 Mb/sec CBR	km	18 957	4 739	23 696
MNSZ 8-34 Mb/sec közötti CBR 1 Mb/sec lépcső ár	1 MB/km	1 363	341	1 704
MNSZ 34 Mb/sec CBR	km	51 567	12 892	64 459
MNSZ 34-155 Mb/sec közötti CBR 1 Mb/sec lépcső ár	1 MB/km	927	232	1 158
MNSZ 155 Mb/sec CBR	km	140 229	35 057	175 286
MNSZ 155-622 Mb/sec közötti CBR 1 Mb/sec lépcső ár	1 MB/km	639	160	799
MNSZ 622 Mb/sec CBR	km	381 419	95 355	476 774
MNSZ 2 Mb/sec VBR	km	4 888	1 222	6 110
MNSZ 2-8 Mb/sec közötti VBR 1 Mb/sec lépcső ár	1 MB/km	1 406	351	1 757
MNSZ 8 Mb/sec VBR	km	13 270	3 317	16 587
MNSZ 8-34 Mb/sec közötti VBR 1 Mb/sec lépcső ár	1 MB/km	959	240	1 198
MNSZ 34 Mb/sec VBR	km	36 093	9 023	45 116
MNSZ 34-155 Mb/sec közötti VBR 1 Mb/sec lépcső ár	1 MB/km	650	162	812
MNSZ 155 Mb/sec VBR	km	98 161	24 540	122 701
MNSZ 155-622 Mb/sec közötti VBR 1 Mb/sec lépcső ár	1 MB/km	447	112	559
MNSZ 622 Mb/sec VBR	km	266 996	66 749	333 744

Bérelt vonali szolgáltatások

Analóg bérelt áramköri szolgáltatás

Díjtétel megnevezése	Mennyiségi egység	Nettó ár (Ft/hó)	Áfa	Bruttó ár (Ft/hó)
BÉRELT ÁRAMKÖRI SZOLGÁLTATÁS				
Analóg bérelt vonali szolgáltatás				
Pont-pont közötti analóg áramkör távolsági hálózaton (I. díjzóna)	áramkör végpont db	17 161	4 290	21 452
Pont-pont közötti analóg áramkör távolsági hálózaton (II. díjzóna)	áramkör végpont db	32 940	8 235	41 175
Pont-pont közötti analóg áramkör távolsági hálózaton (III. díjzóna)	áramkör végpont db	42 552	10 638	53 190

Kiterjesztett használat szolgáltatás

Díjtétel megnevezése	Mennyiségi egység	Nettó ár (Ft/hó)	Áfa	Bruttó ár (Ft/hó)
BÉRELT ÁRAMKÖRI SZOLGÁLTATÁS				
Kiterjesztett használat				
Kiterjesztett használatú áramkör távolsági hálózaton (I. díjzóna)	áramkör végpont db	17 161	4 290	21 452
Kiterjesztett használatú áramkör távolsági hálózaton (II. díjzóna)	áramkör végpont db	32 940	8 235	41 175
Kiterjesztett használatú áramkör távolsági hálózaton (III. díjzóna)	áramkör végpont db	42 552	10 638	53 190

Bérelt vonali adatátviteli szolgáltatás (n×64kbit/s)

Díjtétel megnevezése	Mennyiségi egység	Nettó ár (Ft/hó)	Áfa	Bruttó ár (Ft/hó)
BÉRELT ÁRAMKÖRI SZOLGÁLTATÁS				
64 kb/s átviteli sebességű adatátviteli áramkör				
Pont-pont közötti 64 kbps-os áramkör helyi hálózaton	áramkör végpont db	34 730	8 683	43 413
Pont-pont közötti 64 kbps-os áramkör távolsági hálózaton (I. díjzóna)	áramkör végpont db	42 063	10 516	52 579
Pont-pont közötti 64 kbps-os áramkör távolsági hálózaton (II. díjzóna)	áramkör végpont db	59 367	14 842	74 209
Pont-pont közötti 64 kbps-os áramkör távolsági hálózaton (III. díjzóna)	áramkör végpont db	81 619	20 405	102 024
128 kb/s átviteli sebességű adatátviteli áramkör				
Pont-pont közötti 128 kbps-os áramkör helyi hálózaton	áramkör végpont db	45 580	11 395	56 975
Pont-pont közötti 128 kbps-os áramkör távolsági hálózaton (I. díjzóna)	áramkör végpont db	55 427	13 857	69 284
Pont-pont közötti 128 kbps-os áramkör távolsági hálózaton (II. díjzóna)	áramkör végpont db	93 079	23 270	116 348
Pont-pont közötti 128 kbps-os áramkör távolsági hálózaton (III. díjzóna)	áramkör végpont db	126 744	31 686	158 430
256 kb/s átviteli sebességű adatátviteli áramkör				
Pont-pont közötti 256 kbps-os áramkör helyi hálózaton	áramkör végpont db	79 786	19 947	99 733
Pont-pont közötti 256 kbps-os áramkör távolsági hálózaton (I. díjzóna)	áramkör végpont db	101 777	25 444	127 221
Pont-pont közötti 256 kbps-os áramkör távolsági hálózaton (II. díjzóna)	áramkör végpont db	162 445	40 611	203 056
Pont-pont közötti 256 kbps-os áramkör távolsági hálózaton (III. díjzóna)	áramkör végpont db	223 681	55 920	279 602

Bérelt vonali adatátviteli szolgáltatás (n×64kbit/s)

Díjtétel megnevezése	Mennyiségi egység	Nettó ár (Ft/hó)	Áfa	Bruttó ár (Ft/hó)
BÉRELT ÁRAMKÖRI SZOLGÁLTATÁS				
512 kb/s átviteli sebességű adatátviteli áramkör				
Pont-pont közötti 512 kbps-os áramkör helyi hálózaton	áramkör végpont db	147 520	36 880	184 400
Pont-pont közötti 512 kbps-os áramkör távolsági hálózaton (I. díjzóna)	áramkör végpont db	177 020	44 255	221 275
Pont-pont közötti 512 kbps-os áramkör távolsági hálózaton (II. díjzóna)	áramkör végpont db	299 323	74 831	374 154
Pont-pont közötti 512 kbps-os áramkör távolsági hálózaton (III. díjzóna)	áramkör végpont db	369 622	92 406	462 028
2 Mb/s átviteli sebességű adatátviteli áramkör				
Pont-pont közötti 2 Mbps-os áramkör helyi hálózaton	áramkör végpont db	247 934	61 984	309 918
Pont-pont közötti 2 Mbps-os áramkör távolsági hálózaton (I. díjzóna)	áramkör végpont db	328 399	82 100	410 498
Pont-pont közötti 2 Mbps-os áramkör távolsági hálózaton (II. díjzóna)	áramkör végpont db	561 800	140 450	702 250
Pont-pont közötti 2 Mbps-os áramkör távolsági hálózaton (III. díjzóna)	áramkör végpont db	912 596	228 149	1 140 746

Bérelt vonali adatátviteli szolgáltatás (200 bit/s – 33,6 kbit/s)

Díjtétel megnevezése	Mennyiségi egység	Nettó ár (Ft/hó)	Áfa	Bruttó ár (Ft/hó)
BÉRELT ÁRAMKÖRI SZOLGÁLTATÁS				
Analóg adatátviteli szolgáltatás				
Pont-pont közötti analóg adatáramkör távolsági hálózaton (I. díjzóna)	áramkör végpont db	25 391	6 348	31 739
Pont-pont közötti analóg adatáramkör távolsági hálózaton (II. díjzóna)	áramkör végpont db	41 170	10 292	51 462
Pont-pont közötti analóg adatáramkör távolsági hálózaton (III. díjzóna)	áramkör végpont db	50 782	12 695	63 477

A szolgáltatásokról bővebb információ a PanTel Novum Kft. ügyfélszolgálatán kérhető levélben a 8600 Siófok, Sió u. 74. Pf. 182. címen, telefonon a (06 84) 505 888, faxon a (06 84) 505 796 számokon.

KÖZLEMÉNY

A PanTel Novum Távközlési Szolgáltató Korlátolt Felelősségű Társaság (1134 Budapest, Tüzér utca 39–41.) ezúton tájékoztatja jelenlegi és leendő ügyfeleit, hogy a Hírközlési Felügyelet a BH 12768-1/2001. számú határozatában a PanTel Novum Kft. részére közcélú internetszolgáltatások nyújtását engedélyezte.

A Szolgáltató által nyújtani kívánt szolgáltatás

A Szolgáltató internet-hozzáférést biztosít bérelt vonalon keresztül e-mail-címmel és meghatározott méretű tárolókapacitással, amennyiben az Előfizető az internetszolgáltatásra szerződést köt és az árjegyzékben meghatározott díjat megfizeti.

Az internetszolgáltatás hozzáférési pont a Szolgáltató berendezésének interfésze, mellyel ahhoz a távközlőhálózathoz csatlakozik, melyen keresztül Előfizető a szolgáltatást igénybe veszi.

A szolgáltatás biztosítja a szükséges azonosítókat, jelszavakat, melyek segítségével az Előfizetői berendezés valamelyik távközlőhálózaton keresztül csatlakozva a hozzáférési pontra, eléri a szolgáltatást, azaz az internethálózatot, amelyen keresztül Előfizetőnek lehetősége nyílik az internet alkalmazásainak igénybevételére, úgymint, de nem kizárólag: e-mail, WWW, FTP, News, Telnet, IRC, ICQ, Chat. A PanTel Novum Kft. biztosítja előfizetői weboldalak elhelyezését saját webszerverén.

A Szolgáltató által vállalt kötelezettségek

A távközlési rendszer üzemzavarainak kategorizálását, az üzemzavarok eseteit, a hibaelhárítás megkezdésének idejét és a meghibásodás bejelentésétől számítva a szolgáltatás visszaadási időpontját az alábbi táblázat tartalmazza:

Kategória	A hiba megnevezése	Az elhárítás megkezdése	Szolg. visszaadása
I.	Hibás bérelt vonali internetszolgáltatás esetén, amennyiben az átterhelésre az alternatív irány kiépített és annak biztosítására az Előfizető szerződött	2 órán belül	6 óra
II.	Az I. kategóriába nem tartozó hibás bérelt vonali internetszolgáltatás esetén	2 órán belül	36 óra

Fő specifikus minőségi paraméterek:

Minőségi paraméter	Szolgáltatás
	Bérelt vonali internet-hozzáférés
Éves rendelkezésre állás (1)	99,5%
Átlagos csomagvesztési arány	1%
Maximális csomagkésleltetés (2)	300 ms
Csomagkésleltetés középértéke	–

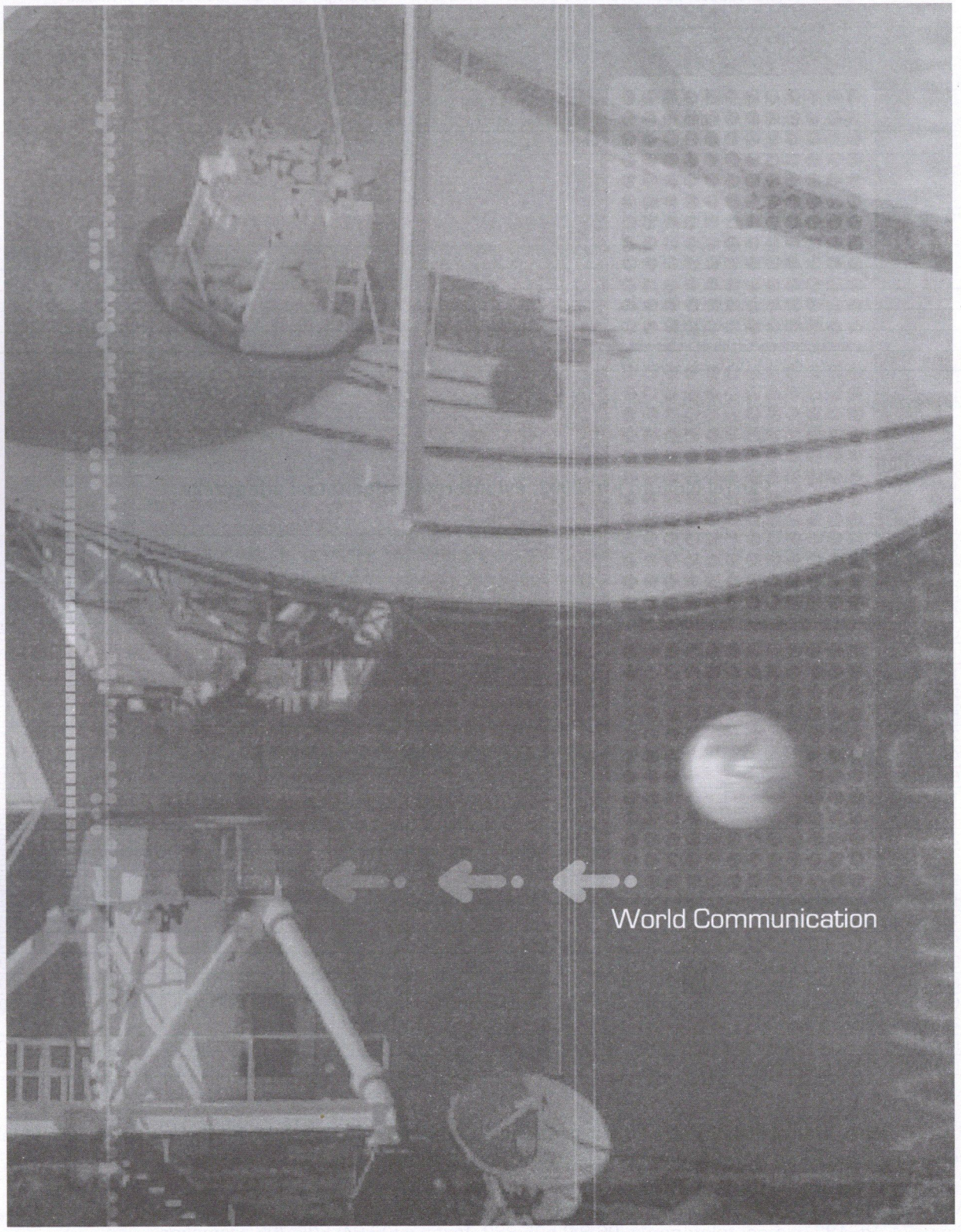
Megjegyzések: (1) Felhasználóként évente, 12 egymást követő hónapra
(2) Csomagméret max. 100 bájt

PanTel Novum Kft. 2002. évi internetszolgáltatási árjegyzéke

Szolgáltatás megnevezése	Mérték-egység	Nettó ár (Ft/hó)	Áfa	Bruttó ár (Ft/hó)
Bérelt vonali internetszolgáltatás				
Átlagos sávszélesség				
64 kbit/s	db	74 900	18 725	93 625
128 kbit/s	db	114 900	28 725	143 625
192 kbit/s	db	148 900	37 225	186 125
256 kbit/s	db	198 900	49 725	248 625
512 kbit/s	db	299 900	74 975	374 875
2 Mbit/s	db	799 900	199 975	999 875
Garantált sávszélesség				
64 kbit/s	db	133 900	33 475	167 375
128 kbit/s	db	206 900	51 725	258 625
192 kbit/s	db	266 900	66 725	333 625
256 kbit/s	db	354 900	88 725	443 625
512 kbit/s	db	534 900	133 725	668 625
2 Mbit/s	db	1 436 900	359 225	1 796 125
További internetszolgáltatások				
További e-mail-cím	db	320	80	400
E-mail-tárfoglalás 1 MB felett (minden megkezdett MB-ra)	MB	1 560	390	1 950
Előfizetői weboldal elhelyezése Szolgáltató webszerverén (3 MB-ig)	db	4 160	1 040	5 200
Előfizetői weboldal elhelyezése Szolgáltató webszerverén (3 MB-felett)	MB	1 040	260	1 300
Önálló webszerver üzemeltetése Szolgáltató telephelyén (elhely., táp, klíma, helyi Ethernet kapcs.)	db	15 600	3 900	19 500
Internetkapcsolódáshoz helyszíni PC+modem konfigurálás	db	3 120	780	3 900
Internethasználat részletezése	db	1 040	260	1 300

A bérelt vonali szolgáltatások árai a korlátlan internet-hozzáférés költségét foglalják magukban, a helyi bérelt vonal díját és az előfizetői végberendezés(ek) árát nem tartalmazzák.

A szolgáltatásról bővebb információ a PanTel Novum Kft. ügyfélszolgálatán kérhető levélben a 8600 Siófok, Sió u. 74. Pf. 182. címen, telefonon a (06 84) 505 888, faxon a (06 84) 505 796 számokon.



Contents

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

Hirdetési árak:
1/1 (205 x 290 mm) 4C 120 000 Ft + áfa
Borító 3 (205 x 290 mm) 4C 180 000 Ft + áfa
Borító 4 (205 x 290 mm) 4C 240 000 Ft + áfa

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

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

2001-ES ELŐFIZETÉSI DÍJAK
Hazai közületi előfizetők részére
1 évre bruttó 30 000 HUF

Hazai egyéni előfizetők részére
1 évre bruttó 6 000 HUF

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

www.hte.hu

Felelős kiadó: MÁTÉ MÁRIA
Lapmenedzser: Dankó András

Design by: Kocsis és Szabó Kft.
HU ISSN 0018-2028

Printed by: Regiszter Kft.