

# **híradástechnika**

VOLUME LVI.

# **2001/10**

November

E 870

FF



8 000001 298514



**Útvonalválasztás**

**Mobil**

**Elméleti eredmények**

**Információs társadalom**

**Történelem**

**A Hírközlési és Informatikai Tudományos Egyesület folyóirata**



# Tartalom



**Dr. Lajtha György:**

E havi számunk.....1

## ÚTVONALVÁLASZTÁS

**Végső Csaba–Dr. Levendovszky János–Rétvári Gábor:**

Statisztikus egyenlőtlenségek elméletén alapuló QoS-útvonalkeresés  
hiányos linkinformáció esetén .....3

**Takács Attila–Lukovszki Csaba–Szabó Róbert:**

Egyszerű forgalomszabályozási módszer hangforgalom átvitelére IP-BSS hálózatokban.....13

## MOBIL

**Imre Sándor–Szalay Máté:**

Gyűrűhierarchia – megbízható IP-mikromobilitási hálózati topológia.....19

**Földi András–Cseh Sándor:**

Meddig terhelhető egy torony? Esettanulmány: egy magyarországi TV-torony története ....25

## ELMÉLETI EREDMÉNYEK

**Albrecht Sándor:**

Börszt módusú, szintetikus apertúrájú radar (SAR) jelek feldolgozása momentán  
Fourier-transzformáció alkalmazásával .....31

**Vesztergombi György–Dr. Levendovszky János–Elek Zsombor:**

Újszerű számítási eljárások a megbízhatósági analízisben .....43

**Horváth Gyula:**

Nanocsövektől a nanométernökökig .....49

## INFORMÁCIÓS TÁRSADALOM

**Páti Brigitta:**

Kis lépésekkel az infotársadalom felé.....53

## TÖRTÉNELEM

**Dénes Tamás:**

A rejtjelző rácsok születése Girolamo Cardano .....57

**Fekete Szilveszterné:**

Arckép a közelmúltból: Kozma László .....63

**Játék** .....66

**Angol nyelvű tartalom** .....68

### Főszerkesztő

ZOMBORY LÁSZLÓ

### Szerkesztőbizottság

Elnök: LAJTHA GYÖRGY

BARTOLITS ISTVÁN  
BOTTKA SÁNDOR  
CSAPODI CSABA  
DIBUZ SAROLTA

DROZDY GYŐZŐ  
GORDOS GÉZA  
GÖDÖR ÉVA  
HUSZTY GÁBOR

JAMBRIK MIHÁLY  
KAZI KÁROLY  
MARADI ISTVÁN  
MEGYESI CSABA

PAP LÁSZLÓ  
SALLAI GYULA  
TARNAY KATALIN  
TORMÁSI GYÖRGY



# E havi számunk

## November



A szakmai folyóiratok elsődleges feladata, hogy a legújabb ismereteket közvetítsék olvasóikhoz. A cikkeknek részben eleget kell tenniük a szakmai továbbképzés célkitűzéseinek is. Egy szaklapban lényegesen újabb eredményeket kell bemutatni, mint ami a könyvekben már megjelent. Mindez csak akkor lehetséges, ha sikerül megnyerni kutatókat, fejlesztőket, hogy eredményeikről az újság lapjain beszámoljanak. Vonzóvá kell tenni a publikálást.

A fiatal mérnököknek ahhoz, hogy a doktori iskolákba felvegyék őket, szükségük van publikációkra. Később a disszertáció elkészülte után a doktori cím elnyerése további publikációkhoz van kötve. Természetesen a követelmények különbséget tesznek a különböző folyóiratok között. Ezen belül is növeli a megjelent cikk értékét, ha azt nemcsak a szerkesztőbizottságban dolgozók ellenőrzik, hanem alapos szaktudású, az adott területen naprakész ismeretekkel rendelkező lektorok is. Bár valamennyi cikket gondosan átolvassuk, ügyelve arra, hogy tévtanok ne jelenjenek meg, és valóban aktuális témákról, érthetően megfogalmazott szöveget adjunk az olvasóknak, mégis némely cikknél, annak kiemelt újdonsága miatt további ellenőrzésre is felkérünk tekintélyes tudósokat. Reméljük, hogy ennek révén a különböző bíráló szervek elismert folyóiratban, lektorált cikk kategóriában megjelenő közleményként fogják ezeket a cikkeket értékelni.

A fenti célok érdekében már ebben számban alkalmazzuk ezt az eljárást. A szerzőt, a címet és a szerző

elérhetőségét tartalmazó, bekeretezett, halványszürke mező jobb alsó sarkában a *vastag, courier L* betű (**L**) hangsúlyozza, hogy a cikk többszörös ellenőrzés után került a folyóiratba.

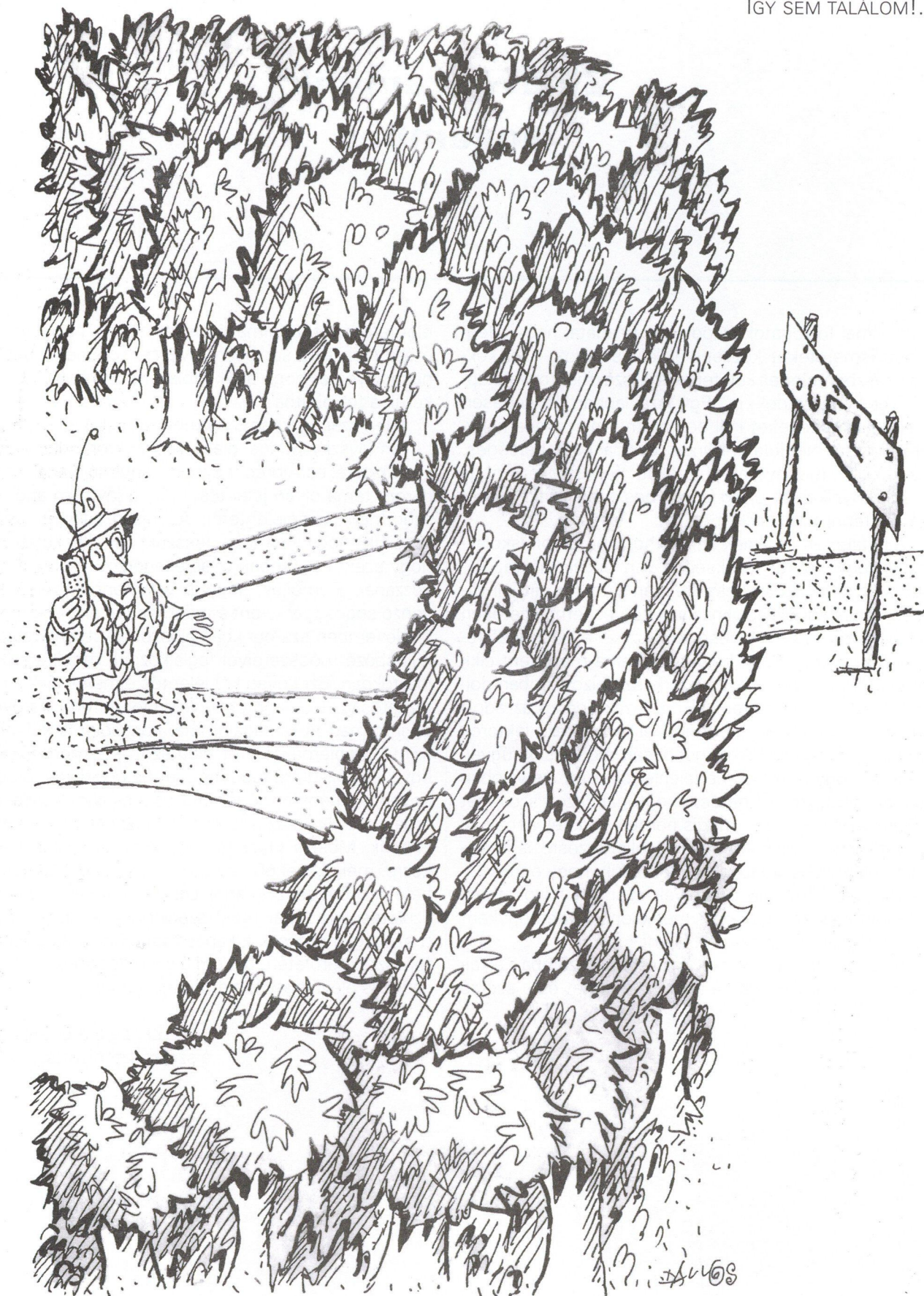
Jelen számunkban 3 cikknél helyeztük el ezt a jelet: Levendovszky János diákjaival, doktoranduszaival írt két cikkénél és Albrecht Sándor tanulmányánál. Mind a három téma olyan jelentős, hogy a jövőben angolul is szeretnénk megjelentetni. Az újság rangját azzal is emeljük, hogy lehetővé tesszük külföldi kutatóknak, hogy ezekre a valóban új és ellenőrzött cikkekre hivatkozzanak. Reméljük, hogy ez valamennyi szerzőnek vonzó segítséget jelent a tudományos elismertséghez.

Novemberi számunkban először az útvonalválasztás különböző módszereivel foglalkozunk mobil- és IP-hálózatokban. Ezt követi két jelentős elméleti cikk a megbízhatóság és a nanotechnológia területéről. Tárgyaljuk az információs társadalommal kapcsolatos különböző szintű problémákat. Két életrajzot is ismertetünk. Az egyik egy világhírű tudóst mutat be új oldalról. Cardano egyenletmegoldó módszereit és a csuklós csatlakozás erőátviteli alkalmazását leíró dolgozatait széles körben ismerik. Most a titkosítás egy aktuális eljárását adjuk közre, mely közel 500 év után még mindig jól használható. Jövőre lesz Kozma László professzor századik születésnapja. Már most szeretnénk felhívni a figyelmet, hogy nemcsak a kapcsolástechnika és a hálózatfejlesztés területén, hanem a számítógépek kidolgozásában is elévülhetetlen érdemei vannak.

Dr. Lajtha György  
a szerkesztőbizottság elnöke



ÍGY SEM TALÁLOM!...



A LEGJOBB ÚTVONALVÁLASZTÁS AKADÁLYA NÉHA AZ ERDŐ.



# Statisztikus egyenlőtlenségek elméletén alapuló QoS-útvonalkeresés hiányos linkinformáció esetén

VÉGSŐ CSABA <sup>(1)</sup>—DR. LEVENDOVSKY JÁNOS <sup>(1)</sup>—RÉTVÁRI GÁBOR <sup>(2)</sup>

Budapesti Műszaki és Gazdaságtudományi Egyetem (BME)

(1) Híradástechnikai Tanszék

(2) Távközlési és Telematikai Tanszék

L

A cikk egy újszerű QoS (Quality of Service, szolgáltatási minőség) útvonal-választási algoritmust javasol csomagkapcsolt hálózatok számára, amely a tradicionális algoritmusoknál hatékonyabb hálózatkishasználást eredményez. Az új algoritmus képes az optimális útvonal közelítésére egy olyan környezetben is, ahol nem áll rendelkezésre teljes információ a linkek aktuális állapotáról (linkkésleltetés, rendelkezésre álló sávszélesség stb.). A cikk az optimális útvonal közelítésére a jól ismert Chernoff-egyenlőtlenséget alkalmazza. A jelenlegi szabványokban rögzített metódusokhoz képest a linkmértékek valószínűségi változókként való kezelésével a minőségi szolgáltatást megkövetelő igények számára megfelelőbb útvonalat képes biztosítani. Az aktuális linkértékekre vonatkozó hiányos információt elsősorban éppen ezen szabványok által bevezetett információaggregálás eredményezi. Az ismertetésre kerülő algoritmusok segítségével a hiányos információs környezetben történő valós idejű útvonalválasztás válik lehetővé, így a forgalmi folyamatok számára előre definiált minőségi paramétereket (end-to-end késleltetés, jitter) lehet biztosítani.

## Bevezetés

A csomagkapcsolt hálózatok területén a jelenlegi egyik legnagyobb kihívás a minőségi paramétereket biztosító útvonal(ak) keresési mechanizmusának kidolgozása. Sok esetben a feladat adott end-to-end késleltetésű és sávszélességű útvonalak keresését jelenti [2,3,5]. Ezek eredményeképpen, a QoS-útvonalkeresés az eltérő minőségű útvonalak halmaza felatti optimalizálási feladatként fogható fel. Sajnos ezen feladat általános esetben nem polinomiális, azaz nem redukálható a legrövidebb útvonal keresésének problémájára, amelyre léteznek polinomiális komplexitással rendelkező algoritmusok (Dijkstra, Bellmann–Ford). Bizonyítható, hogy a link minőségi paramétereinek valószínűségi változókként való értelmezésével az útvonalkeresés NP nehéz feladattá válhat [5]. Ebben az esetben azonban a cél már azon útvonal kiválasztása, amely a legnagyobb valószínűséggel biztosítja az előre definiált minőségi paramétereket. A továbbiakban az ezen típusú útvonalválasztási feladatot MLPS (Maximum Likely Path Selection, maximális valószínűségű útvonal választása) eljárásnak nevezzük. Az MLPS a tradicionális additív mértékek szerinti optimalizálás helyett nemlineáris gráfoptimalizálási feladathoz vezet.

A link paramétereinek valószínűségi változókként való értelmezésének a szükségessége a (i) a jelenlegi szabványokban (OSPF, PNNI) helyet foglaló információ aggregálásából következik [1,4] (ahol a hálózat távoli komponenseire vonatkozó linkinformációkról csak egy átlagos érték áll rendelkezésre). A másik esetben (ii) a linkek paramétereinek folyamatos, véletlenszerű változásából ered (azok értékét mindig az aktuális forgalmi

viszonyok határozzák meg). Mindkét esetben – mivel a paraméterek pontos értéke nem ismert – az útvonalválasztási algoritmusoknak hiányos információval kell működniük, aminek során a cél azon útvonal megtalálása, amely a minőségi kritérium(oka)t maximális valószínűséggel elégíti ki.

## Útvonalválasztás hiányos linkinformációk esetén

A probléma modellezése érdekében tételezzük fel, hogy adottak a következő mennyiségek:

- $G(V,E)$  gráf, a hálózati topológia (ahol  $V$  a  $G$  gráf csomópontjainak,  $E$  a  $G$  gráf éleinek a halmazát jelöli);
- $\forall (u,v) \in E$  link  $(u,v \in V)$  esetén a minőségi paramétert leíró  $\delta_{(u,v)}$  valószínűségi változó (pl. a rendelkezésre álló sávszélesség, késleltetés), amelynek eloszlásfüggvénye

$$F_{(u,v)}(x) = P(\delta_{(u,v)} < x);$$

- end-to-end QoS-kritérium, pl.  $\min_{(u,v) \in R} \delta_{(u,v)} \geq A$  a sávszélességre ( $[A]=\text{Hz}$ ) vagy

$$\sum_{(u,v) \in R} \delta_{(u,v)} < T \text{ end-to-end késleltetésre } ([T]=\text{sec})$$

vonatkozó követelmény esetén;

Ezen mennyiségeket alapul véve a cél azon  $\tilde{R}$  optimális útvonal megkeresése, amely legnagyobb valószínűséggel biztosítja az adott QoS-kritériumot, nevezetesen:

$$\tilde{R}: \max_R P\left(\min_{(u,v) \in R} \delta_{(u,v)} \geq A\right) \quad (1a)$$

vagy



$$\tilde{R}: \max_R P\left(\sum_{(u,v) \in R} \delta_{(u,v)} < T\right) \quad (1b)$$

Az (1.a) esetben  $\delta$  „bottleneck” (ahol az útvonal minőségét a minimális minőségű link határozza meg, pl. rendelkezésre álló sávszélesség), míg a második esetben additív típusú (ahol az útvonal minőségét az útvonalhoz tartozó linkek minőségének az összege határozza meg, pl. késleltetés, késleltetésingadozás) link-metrikát jelent. A fentiekben bevezetett  $\tilde{R}$  útvonalra a továbbiakban az MLP (Most Likely Path, legvalószínűbb útvonal) jelölés vonatkozik. Additív metrika alapján történő útvonalkeresés esetén a fenti problémára mint ARII utalunk (Additive Routing with Incomplete Information, additív routing hiányos információ alapján).

Köztudott, hogy a legrövidebb útkeresés (SPR, Shortest Path Routing) polinomiális komplexitással megoldható feladat. Léteznek erre alkalmas módszerek, például a Dijkstra- vagy a Bellmann–Ford-algoritmus. Ezért az MLP-feladatnak SPR-feladattá történő konvertálása ekvivalens az MLP-feladat polinomiális időben történő megoldhatóságának bizonyításával. A következő tétel azt bizonyítja, hogy a bottleneck típusú metrikán alapuló MLP-probléma egyszerűen megoldható tradicionális SPR-algoritmusok segítségével.

**Tétel 1:** A hálózat linkjeinek függetlenségét feltételezve az

$$\tilde{R}: \max_R P\left(\min_{(u,v) \in R} \delta_{(u,v)} \geq A\right)$$

optimalizálási feladat ekvivalens azon legrövidebb útkeresési probléma megoldásával, ahol minden  $(u,v) \in R$  linkhez a

$$\mu_{(u,v)} = -\log P(\delta_{(u,v)} \geq A) = -\log\{1 - F_{(u,v)}(A)\}$$

mennyiség van rendelve mint linkmérték.

**Bizonyítás:** Keressük az

$$\tilde{R}: \max_R P(\min_{(u,v) \in R} \delta_{(u,v)} \geq A)$$

útvonalat, amely ekvivalens az

$$\tilde{R}: \max_R P(\cap_{(u,v) \in R} \{\delta_{(u,v)} \geq A\})$$

megoldásával. A linkenként független valószínűségi változókat feltételezve

$$P(\cap_{(u,v) \in R} \{\delta_{(u,v)} \geq A\}) = \prod_{(u,v) \in R} P(\delta_{(u,v)} \geq A)$$

azaz az eredeti (1.a) probléma felírható a következő formában:

$$\tilde{R}: \min_R \sum_{(u,v) \in R} -\log P(\delta_{(u,v)} \geq A).$$

Ebből eredően  $(u,v) \in E$  linkekhez

$$\mu_{(u,v)} := -\log P(\delta_{(u,v)} \geq A)$$

mértéket rendelve az MLP-útvonalválasztás valóban megoldható SPR-feladatként.

Azonban, ha az útvonalkeresés során a linkmérték a késleltetés (additív típusú metrika), akkor a QoS-útvonalválasztás nem polinomiális feladattá alakul, mint ahogy azt a következő tétel kimondja.

**Tétel 2** (Guerin at al): Az ARII-feladatra vonatkozó optimális

$$\tilde{R}: \max_R P\left(\sum_{(u,v) \in R} \delta_{(u,v)} < T\right)$$

megoldás megtalálása általános esetben NP nehéz probléma.

A bizonyítás azon alapul, hogy már az

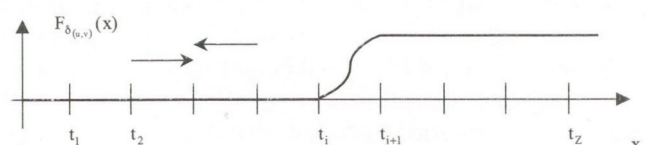
$$\tilde{R}: P\left(\sum_{(u,v) \in R} \delta_{(u,v)} < T\right) > \xi$$

feladat megoldásának a megkeresése is NP nehéz (minden  $0 < \xi < 1$  érték esetén). A bizonyításra vonatkozó részletesebb információért lásd [5]. A fentiekből eredően a továbbiakban a célunk olyan korlátozó feltételek bevezetése, amelyek teljesülése esetén az (1.b) optimalizálási probléma polinomiális komplexitással megoldható feladattá válik, mindamelllett az eredeti probléma jellegzetességeit megtartja (pl. valós hálózati viszonyok esetén előnyös megoldásokat kínál).

## Additív metrikán alapuló új routing algoritmushányos linkinformáció esetén

A nagy eltérések elméletén alapuló QoS-útvonalválasztási algoritmus a legnagyobb valószínűségű útvonal keresését „farokeloszlás-becslési” problémává (tail estimation problem) alakítja. Tegyük fel, hogy routerek a következő módon hirdetik meg a hozzájuk tartozó linkek késleltetését a többi router számára:

- A linkkésleltetések lehetséges értéktartománya egy  $D = \{t_i, i = 1, \dots, Z\}$  rácshálózattal van lefedve.
- Minden egyes pillanatban, ha az  $(u,v)$  link aktuális késleltetése meghaladja a  $t_i$  értéket, a megfelelő router meghirdeti ezen értéket a többi router számára mint az  $(u,v)$  aktuális késleltetését.



1. ábra A link késleltetésének meghirdetési módszere és a hozzá kapcsolódó valószínűségi modell



Ebből következik, hogy minden egyes router számára minden egyes pillanatban csak az az információ áll rendelkezésre az  $(u, v)$  link késleltetésére vonatkozóan, hogy az valahol a  $(t_i, t_{i+1})$  tartományon belül helyezkedik el, azaz  $\delta_{(u,v)} \in (t_i, t_{i+1})$ . Nyilvánvalóan a meghirdetésre használt jelzési sáv szélesség szoros összefüggésben van az alkalmazott rácshálózat felépítésével, azaz a rácspontok számával és a rácspontok elhelyezkedésével. Növelve a rácspontok közötti távolságot csökken a link késleltetések meghirdetéséhez szükséges sáv szélesség, viszont csökken az aktuális link késleltetésekre vonatkozó információ mennyisége is, hiszen azok nagyobb intervallumokon belül helyezkedhetnek el. Ugyanezen megfontolásból csökkentve a rácspontok közötti távolságot csökken a routerek tábláiban tárolt információ bizonytalansága (pontosabb útvonalválasztás végezhető el), viszont nő a link késleltetések meghirdetéséhez szükséges sáv szélesség. Jelenlegi kutatásaink éppen ezzel a dilemmával kapcsolatosak, nevezetesen: hogyan határozható meg az az optimális rácshálózat, amely esetén a lehető legpontosabb útvonalválasztás végezhető el, azzal a kényszerfeltétellel, hogy a jelzési sáv szélesség még egy bizonyos korlát alatt maradjon. A továbbiakban azonban nem foglalkozunk ezzel a problémával, feltételezzük, hogy a  $D$  rácshálózat adott.

Ezen előfeltételeken alapulva egy új algoritmust vezetünk be, amely képes az MLP (1.b) polinomiális időben történő approximálására a statisztikai egyenlőtlenségnek az útvonalon előálló ún. aggregált késleltetés farokeloszlás-bebecslésére történő alkalmazásával.

**Tétel 3:** A hálózat linkjeinek függetlenségét feltételezve a logaritmikus momentumgeneráló függvény

$$\mu_{(u,v)}(s) = \ln E(e^{s\delta_{(u,v)}}) = \ln \int f_{(u,v)}(x) e^{sx} dx \quad \forall s > 0, \quad (2)$$

alkalmazásával az ARII-probléma SPR-feladattá redukálható a következő additív, determinisztikus metrika alapján:

$$\kappa_{(u,v)} = \mu_{(u,v)}(\tilde{s}), \text{ ahol } \tilde{s} = \inf_{(u,v) \in \tilde{R}} \sum \mu_{(u,v)}(s) - sT. \quad (3)$$

**Bizonyítás:** A fentiek szerint azon útvonal meghatározása, amely maximalizálja a

$$P\left(\sum_{(u,v) \in R} \delta_{(u,v)} < T\right)$$

valószínűséget, ekvivalens azon útvonal meghatározásával, amely minimalizálja a

$$P\left(\sum_{(u,v) \in R} \delta_{(u,v)} > T\right)$$

valószínűséget. Az utóbbi valószínűség viszont felülről becsülhető pl. a Chernoff-egyenlőtlenség segítségével:

$$P\left(\sum_{(u,v) \in R} \delta_{(u,v)} > T\right) \leq e^{\mu_R(\hat{s}) - sT}, \quad (4)$$

ahol a  $\mu_R(s)$  az  $R$  útvonal aggregált késleltetésének logaritmikus momentumgeneráló függvénye, amely linkenként független valószínűségi változókat feltételezve egyszerűen számítható

$$\mu_R(s) = \sum_{(u,v) \in R} \mu_{(u,v)}(s).$$

Emiatt az (1.b) optimális megoldás ( $\tilde{R}$ ) a következőképpen approximálható:

$$\hat{R}: \min_R e^{\sum_{(u,v) \in R} \mu_{(u,v)}(\hat{s}) - sT} \quad \text{azaz}$$

$$\hat{R}: \min_R \sum_{(u,v) \in R} \mu_{(u,v)}(s). \quad (5)$$

Az utolsó minimalizálási probléma viszont már egy SPR-feladat a linkmértékek szerint.

A fenti módszerrel a továbbiakban „Egyszerű Chernoff-Algoritmus” néven utalunk (ahol az útvonalat a Chernoff-egyenlőtlenség alapján, adott  $s$  érték mellett keressük). Az (5) SPR-feladat megoldása azonban csak aszimptotikusan optimális megoldása lesz az eredeti (1.b) problémának, hiszen az eredeti célfüggvény helyett egy arra vonatkozó felső korlátot minimalizálunk. Továbbá, mivel

$$P\left(\sum_{(u,v) \in R} \delta_{(u,v)} > T\right) \leq e^{\mu_R(s) - sT} \Rightarrow$$

$$P\left(\sum_{(u,v) \in R} \delta_{(u,v)} < T\right) > 1 - e^{\mu_R(\hat{s}) - sT} \quad (6)$$

a QoS-követelmény legalább  $1 - \varepsilon$  valószínűséggel teljesül, ha  $\varepsilon = e^{\mu_R(\hat{s}) - sT}$ . Az „Egyszerű Chernoff-Algoritmus” mérnöki szempontból tehát igen hasznos.

A következő cél a fenti algoritmus hatékonyságának javítása érdekében azon optimális  $s$  érték ( $\hat{s}$ ) meghatározása, amely a legélesebb (4) felső korlátot biztosítja. Amint látható,  $\hat{s}$  magától az  $R$  útvonaltól függ. Következésképpen, valamilyen értéket választva és elvégezve a (5) legrövidebb útkeresést, rossz megoldást kaphatunk, hiszen valamely  $s_s$  érték teljesen más útvonalat eredményezett volna (amely esetleg sokkal jobb minőségű útvonal). Ezen probléma elkerülése érdekében a legkézenfekvőbb megoldást a következő „Kimerítő-s Algoritmus” jelentheti.



1. Defináljunk egy  $S = \{s_i, s_i > 0, i = 1, \dots, M\}$  rácshálózatot az  $s$  lehetséges értékei felett.
2. Vegyük  $s_i \in S$ .
  - 2.1 Végezzük el az SPR-t a Bellmann-Ford vagy a Dijkstra alkalmazásával a következő linkmértékek szerint:  $\mu_{(u,v)}(s_i) := \ln E(e^{s_i \delta_{(u,v)}})$ .
  - 2.2 A kapott  $\hat{R}$  útvonal alapján határozzuk meg az optimális  $s$  paramétert:
 
$$\hat{s}_i : \sum_{(u,v) \in \hat{R}_i} \frac{d\mu_{(u,v)}(s)}{ds} = T$$
 és számoljuk ki az általa biztosított felső határt:
 
$$B_i := e^{\sum_{(u,v) \in \hat{R}_i} \mu_{(u,v)}(\hat{s}_i) - \hat{s}_i T}$$
  - 2.3  $i = i+1$  és vissza a 2. pontra.
3. Keressük meg azt az útvonalat, amely a legkisebb felső határhoz tartozik

$$\hat{R}_j : \min_{\hat{R}_i} e^{\sum_{(u,v) \in \hat{R}_i} \mu_{(u,v)}(\hat{s}_i) - \hat{s}_i T} \quad i = 1, \dots, M$$

Nyilvánvaló, hogy az algoritmus komplexitása  $O(M|V|^2)$ , amely az  $s$  paraméter lehetséges értékei felett elhelyezett rácshálózat felbontásának megfelelő finomításával ( $M$  növelésével) hatalmas lehet. Továbbá, mivel az  $s$  paraméter bármilyen pozitív értéket felvehet, de az általunk rögzített  $S$  rácshálózat csak véges számú pontot tartalmaz, elvethetjük a legjobb minőségű megoldást azáltal, hogy figyelmen kívül hagyunk néhány  $s$  értéket.

### Rekurzív módszeren alapuló útvonalválasztó algoritmus az optimális útvonal approximálására

Az algoritmus numerikus komplexitása csökkenthető, ha ekvidisztáns  $D$  rácshálózatot tételezünk fel a linkkésleltetések lehetséges tartományán. Tegyük fel továbbá, hogy a késleltetés minden  $(t_i, t_{i+1})$  intervallumon ugyanazon diszkrét eloszlással írható le, azaz

$$P(\delta_{(u,v)} = a_{(u,v)} + m\Delta) = P_m \quad (7)$$

ahol  $m = -M, -M+1, \dots, -1, 0, 1, \dots, M-1, M$

$\delta_{(u,v)} \in (t_i, t_{i+1})$  és  $\Delta := \frac{t_{i+1} - t_i}{2M}$ . A (7) kifejezésben az

$$a_{(u,v)} = \frac{t_i + t_{i+1}}{2} \text{ az } (u,v) \in E$$

link késleltetésének utolsó meghirdetése után lehetséges késleltetéstartomány közepét jelenti. Ekkor a  $\mu_{(u,v)}(s)$  a következő módon határozható meg:

$$\mu_{(u,v)}(s) = \ln \left( \sum_{m=-M}^M P_m e^{s(m\Delta + a_{(u,v)})} \right), \text{ azaz}$$

$$\mu_{(u,v)}(s) = s a_{(u,v)} + \mu(s) \quad (8)$$

ahol

$$\mu(s) := \ln \left( \sum_{m=-M}^M P_m e^{s m \Delta} \right) \quad (9)$$

egy link független általános logaritmikus momentumgeneráló függvényt jelent. A fenti feltételezést alapul véve a következő tétel fogalmazható meg.

**Tétel 4:** A hálózat linkjeinek függetlenségét feltételezve adott  $QoS$ -kritérium és  $R$  útvonal esetén a legélesebb felső határ a következőképpen érhető el:

$$P \left( \sum_{(u,v) \in R} \delta_{(u,v)} > T \right) \leq e^{\sum_{(u,v) \in R} \mu_{(u,v)}(\hat{s}) - \hat{s} T}, \text{ ahol}$$

$$\hat{s} = \mu'^{-1} \left( \frac{T - \sum_{(u,v) \in R} a_{(u,v)}}{|R|} \right) \quad (10)$$

az ezen legélesebb felső határt biztosító  $s$  értéket jelenti.

A (10) összefüggésben  $\mu'^{-1}(x)$  a  $\mu(s)$  link független logaritmikus momentumgeneráló függvény deriváltjának az inverzét, míg  $|R|$  az  $R$  útvonal hoppszámát jelöli.

**Bizonyítás:** A legélesebb felső határ elérése érdekében az  $s$  paramétert a következőképpen kell optimalizálnunk:

$$\hat{s} : \inf_s \sum_{(u,v) \in R} \mu_{(u,v)}(s) - sT \quad (11)$$

Bizonyított, hogy a  $\mu(s)$  logaritmikus momentumgeneráló függvénynek egyetlen minimuma van az  $s$  függvényében [11], tehát  $\hat{s}$  meghatározható a

$$\sum_{(u,v) \in R} \mu_{(u,v)}(s) - sT$$

kifejezés differenciálásával, azaz



$$\hat{s} : \sum_{(u,v) \in R} \frac{d\mu_{(u,v)}(s)}{ds} = T. \quad (12)$$

Figyelembe véve, hogy  $\mu_{(u,v)}(s) = s a_{(u,v)} + \mu(s)$ , a (12) eredményeképpen

$$\sum_{(u,v) \in R} \mu'(s) = T - \sum_{(u,v) \in R} a_{(u,v)}$$

összefüggés kapható meg, amelyből

$$\hat{s} = \mu'^{-1} \left( \frac{T - \sum_{(u,v) \in R} a_{(u,v)}}{|R|} \right) \quad (13)$$

A 4. tétel alapján egyszerűen meghatározható az  $R$  útvonalhoz tartozó optimális  $\hat{s}$  paraméterérték. Az  $\hat{s}$  paraméterérték  $R$  útvonaltól való függésének érzékelteése érdekében a következőkben az  $\hat{s}(R)$  jelölést alkalmazuk.

Az  $s$  paraméter egyszerű optimalizálásából fakadóan egy új „Rekurzív Útvonalkereső – s Kereső Algoritmus”-nak nevezett útvonalválasztási algoritmus fogalmazható meg. Az algoritmus neve annak működéséből ered: adott  $s$  érték mellett meghatározzuk az  $\hat{R}(s)$  optimális útvonalat, majd ezen útvonal alapján meghatározzuk a legélesebb felső korlátot biztosító  $\hat{s}(\hat{R})$  optimális paraméterértéket, majd ezen érték alapján új útvonalat keresünk. Az algoritmus működése a következő:

Inicializálás :  $k = 0$ ;  $\hat{s}_0 = a$  ;

Rekurzió:  
amíg TRUE

$$\hat{R}_k : \min_R \{ \mu_R(\hat{s}_k) - \hat{s}_k T \}$$

ha  $\hat{R}_k = \hat{R}_{k-1}$  akkor kilépés az  $\hat{R}_k$  útvonallal

és  $\exp \{ \mu_{\hat{R}_k}(\hat{s}_k) - \hat{s}_k T \}$  felső határral

egyébként ha  $T \geq \sum_{(u,v) \in \hat{R}_k} a_{(u,v)} + |\hat{R}_k| M \Delta$  akkor

kilépés az  $\hat{R}_k$  útvonallal és az 1.0 felső határral

egyébként ha  $T \leq \sum_{(u,v) \in \hat{R}_k} a_{(u,v)} - |\hat{R}_k| M \Delta$  akkor

kilépés az  $\hat{R}_k$  útvonallal és a 0.0 felső határral

egyébként  $\hat{s}_{k+1} : \min_s \{ \mu_{\hat{R}_k}(s) - sT \}$   
 $k = k+1$

Mint az algoritmus működéséből kiderül, az egyes lépésekben vagy az útvonal minősége (adott  $s$  esetén megtaláljuk az  $\hat{R}(s)$ ), vagy az útvonalra vonatkozó felső határ minősége javul (adott útvonal esetén meghatározzuk az  $\hat{s}$  optimális értéket). Ebből következik, hogy a rekurzív jellegből adódóan az aktuális megoldás minőségét mindig javítjuk. Az algoritmus leáll, ha a következő feltétel teljesül:

$$\hat{R}_{k+1}(\hat{s}_{k+1}) = \hat{R}_k(\hat{s}_k), \text{ ahol } \hat{s}_{k+1} : \min_s \{ \mu_{\hat{R}_k}(s) - sT \}$$

ami azt jelenti, hogy adott  $\hat{s}_k$  esetén kapott  $\hat{R}_k$  optimális útvonal megegyezik azzal az útvonallal, amelyet az optimalizált  $\hat{s}_{k+1}(\hat{R}_k)$  érték alapján kapunk.

A „Rekurzív Útvonalkereső – s Kereső Algoritmus” leírásában megtalálható különböző leállási feltételek a Chernoff-egyenlőtlenség által az  $R$  útvonal esetén garantált felső határ és a  $T$  QoS-kritérium közötti összefüggésből erednek. Ezen összefüggés alapján a következő feltételeket kell megfogalmaznunk:



|    | Feltétel                                                                              | $P\left(\sum_{(u,v) \in R} \delta_{(u,v)} < T\right)$ where $\sum_{(u,v) \in R} \delta_{(u,v)} \in \left[\sum_{(u,v) \in R} a_{(u,v)} -  R M\Delta, \sum_{(u,v) \in R} a_{(u,v)} +  R M\Delta\right]$ |
|----|---------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C1 | $T \leq \sum_{(u,v) \in R} a_{(u,v)} -  R M\Delta$                                    | Nyilvánvalóan, ebben az esetben $P\left(\sum_{(u,v) \in R} \delta_{(u,v)} < T\right) = 0$ .                                                                                                           |
| C2 | $E \sum_{(u,v) \in R} \delta_{(u,v)} < T < \sum_{(u,v) \in R} a_{(u,v)} +  R M\Delta$ | $P\left(\sum_{(u,v) \in R} \delta_{(u,v)} < T\right) = 1 - P\left(\sum_{(u,v) \in R} \delta_{(u,v)} > T\right)$                                                                                       |
| C3 | $T \geq \sum_{(u,v) \in R} a_{(u,v)} +  R M\Delta$                                    | Nyilvánvalóan, ebben az esetben $P\left(\sum_{(u,v) \in R} \delta_{(u,v)} < T\right) = 1$ .                                                                                                           |

Az algoritmus stabilitásának bizonyítása érdekében vezessük be az  $\alpha(s, R) = \mu_R(s) - sT$  kifejezést és alkalmazzuk a Ljapunov stabilitási kritériumot. Az algoritmus stabil, ha

- $\alpha(s_k, R_k)$ -nak létezik globális alsó határa, azaz  $\exists L < \infty$ , hogy  $\alpha(s_k, R_k) \geq L \quad \forall k \geq 0$ .
- $\alpha(s, R)$  a rekúzió folyamán, az egyensúlyi pontoktól eltekintve szigorúan monotonon csökken  $\alpha(\hat{s}_k, \hat{R}_k) \geq \alpha(\hat{s}_{k+1}, \hat{R}_k) \geq \alpha(\hat{s}_{k+1}, \hat{R}_{k+1}) \quad \forall k \geq 0$ .

**Tétel 5:** A „Rekúzió Útvonalkereső – s Kereső Algoritmus” Ljapunov-értelemben stabil.

**Bizonyítás:** Az algoritmusból látható, hogy a második feltétel mindig teljesül, mivel  $\alpha(\hat{s}_k, \hat{R}_k) \geq \alpha(\hat{s}_{k+1}, \hat{R}_k) \geq \alpha(\hat{s}_{k+1}, \hat{R}_{k+1})$

Az első feltétel teljesülése érdekében  $\alpha(s, R)$ -re vonatkozóan a következő alsó határ vezethető be:

$$\begin{aligned} \alpha(s, R) &= \sum_{(u,v) \in R} sa_{(u,v)} + |R|\mu(s) - sT = \\ &= \sum_{(u,v) \in R} sa_{(u,v)} + |R|\ln\left(\sum_{m=-M}^M P_m e^{sm\Delta}\right) - sT \geq \\ &\geq \sum_{(u,v) \in R} sa_{(u,v)} + |R|\ln e^{-sM\Delta} - sT = \sum_{(u,v) \in R} sa_{(u,v)} - |R|sM\Delta - \\ &sT = \left(\sum_{(u,v) \in R} a_{(u,v)} - |R|M\Delta - T\right) \end{aligned} \quad (14)$$

Ha a C2 feltétel teljesül (szükséges feltétele a megoldás minősége k-adik lépésben történő javításának), akkor

$$\sum_{(u,v) \in \hat{R}_k} a_{(u,v)} - |\hat{R}_k|M\Delta - T > -2|\hat{R}_k|M\Delta$$

és (14) alapján

$$\alpha(\hat{s}_k, \hat{R}_k) > -2\hat{s}_k|\hat{R}_k|M\Delta \geq -2\hat{s}_k(|V|-1)M\Delta. \quad (15)$$

Az  $\hat{s}_k$  érték számítása (11) (13) szerint történik, ahol  $\mu'(s)$  (9) alapján

$$\mu'(s) = \frac{\Delta \sum_{m=-M}^M m P_m e^{sm\Delta}}{\sum_{m=-M}^M P_m e^{sm\Delta}} = \frac{\Delta E\{m e^{sm\Delta}\}}{E\{e^{sm\Delta}\}}. \quad (16)$$

A (16) kifejezésből könnyen belátható, hogy  $\mu'(s)$  az  $s$  paraméter szigorúan monotonon növekvő függvénye, továbbá  $|\mu'(s)| < M\Delta$ . Azaz  $\mu'(s)$  invertálható és  $\mu'^{-1}(s)$  véges értéket vesz fel a  $(-M\Delta, M\Delta)$  tartományon belül. Tehát,

$$\hat{s}_k = \mu'^{-1}\left(\frac{T - \sum_{(u,v) \in \hat{R}_k} a_{(u,v)}}{|\hat{R}_k|}\right) \leq \mu'^{-1}\left(T - \sum_{(u,v) \in E} a_{(u,v)}\right). \quad (17)$$

A (15) és (17) összefüggésekből a következő alsó határ vezethető be:

$$\alpha(\hat{s}_k, \hat{R}_k) > -2(|V|-1)M\Delta \mu'^{-1}\left(T - \min_{(u,v) \in E} a_{(u,v)}\right),$$

ahol felhasználtuk, hogy  $\alpha(\hat{s}_k, \hat{R}_k)$  a minimumát  $\hat{s}_k$  maximumánál veszi fel.

A fenti tétel bizonyította az algoritmus stabilitását, annak optimalitását azonban eddig még nem vizsgáltuk. Ez a Ljapunov-elmélet alapján a lokális minimumokban való megakadás lehetőségéből ered. Fontos megjegyezni, hogy itt optimalitáson az (5) feladat ( $\hat{R}$ ) megoldásának a megtalálását értjük, ami nyilvánvalóan nem egyezik meg az eredeti probléma (1.b) optimális ( $\tilde{R}$ ) megoldásával. A szimulációs fejezetben szereplő eredmények legfőbb célja éppen az analitikus kapcsolatok jelenlegi hiánya következtében a „Rekúzió Útvonalkereső – s Kereső Algoritmus” által elérhető megoldás, az (5) feladat optimális megoldása és az eredeti (1.b) probléma optimális megoldása közötti minőségi kapcsolat analízisa valós hálózati méretek és paraméterértékek esetén.

## Teljesítőképeség-analízis

A fentiekben ismertetett „Rekúzió Útvonalkereső – s Kereső Algoritmus” hatékonyságát saját fejlesztésű szimulációs programcsomag segítségével végeztük el. Az algoritmus által szolgáltatott szuboptimális megoldás minőségének vizsgálatára a következő mértékeket vezettük be. Az algoritmus hatékonyságát

- adott forgalmi szituáció ( $G$ ), kezdő- ( $S$ ) és végpont ( $f$ ), valamint QoS-kritérium ( $T$ ) mellett

$$\eta_{\text{method}}(G, s, f, T) =$$



$$= \frac{P(\sum_{(u,v) \in R_{\text{method}}(s,f)} \delta_{(u,v)} < T)}{P(\sum_{(u,v) \in R_{\text{exhaustive search}}(s,f)} \delta_{(u,v)} < T)} \quad (18)$$

- adott forgalmi szituáció ( $G$ ), QoS-kritérium ( $T$ ) mellett az összes lehetséges kezdő- ( $s$ ) és végpont ( $f$ )

$$\eta_{\text{method}}(G, T) =$$

$$= \frac{1}{|V|^2 - |V|} \sum_{s \in E(G)} \sum_{f \in E(G), f \neq s} \eta_{\text{method}}(G, s, f, T) \quad (19)$$

- a forgalmi szituációt ( $G \in \Gamma$ ) és a QoS-kritériumot véletlenszerűen generálva

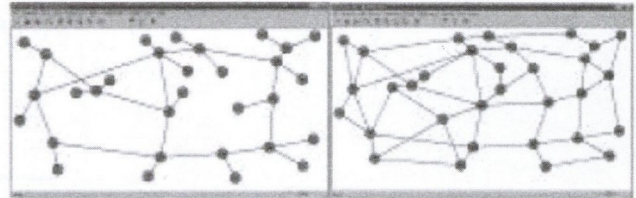
$$\eta_{\text{method}} = \frac{1}{|\Gamma|} \sum_{G \in \Gamma} \eta_{\text{method}}(G, T) \quad (20)$$

alapján határoztuk meg, ahol  $R_{\text{method}}(s, f)$  az  $s$  kezdő- és az  $f$  végpont között a „Rekurzív Útvonalkereső – s Kereső Algoritmus” által talált útvonalat ( $\tilde{R}$ ), míg  $R_{\text{exhaustive search}}(s, f)$  az (1.b) kimerítő keresés segítségével meghatározott

megoldását ( $\tilde{R}$ ) jelöli. Látható, hogy minél jobb az algoritmus által szolgáltatott megoldás minősége, annál közelebb kerül mindhárom mérték az 1 értékhez.

### Szimulációs eredmények

A teljesítményanalízis során az ANSNET nemzetközi gerinchálózat topológiájának – a konnektivitás növelése és a pontok közötti többszörös utak létezésének biztosítása érdekében – módosított változatát használtuk.



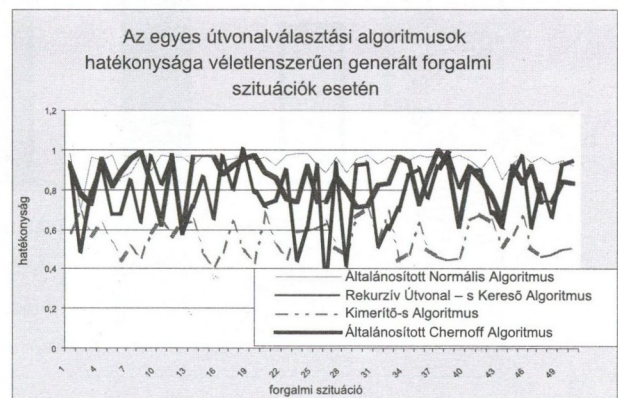
2. ábra Az ANSNET és az analízis során alkalmazott hálózati topológia

Ezen hálózati topológia mellett a linkésleltetések, valamint a QoS-kritérium értékeit a következő eloszlások alapján generáltuk [7,8].

| Paraméter        | Név                                                                   | Érték                                          |
|------------------|-----------------------------------------------------------------------|------------------------------------------------|
| $T$              | QoS = kritérium                                                       | Egyenletes eloszlás [30 ms, 160 ms]            |
| $\tau_{(u,v)}$   | Csak a linkenkénti $(t_i, t_{i+1})$ intervallum generálására szolgál. | Egyenletes eloszlás [0 ms, 50 ms]              |
| $\delta_{(u,v)}$ | Linkésleltetés a $(t_i, t_{i+1})$ -ben                                | Egyenletes eloszlás $(t_i, t_{i+1})$ , $M = 5$ |
| $t_{i+1} - t_i$  | A linkésleltetési értékeket lefedő rácshálózat felbontása.            | 10ms                                           |

1. táblázat A szimuláció során használt paraméterértékek

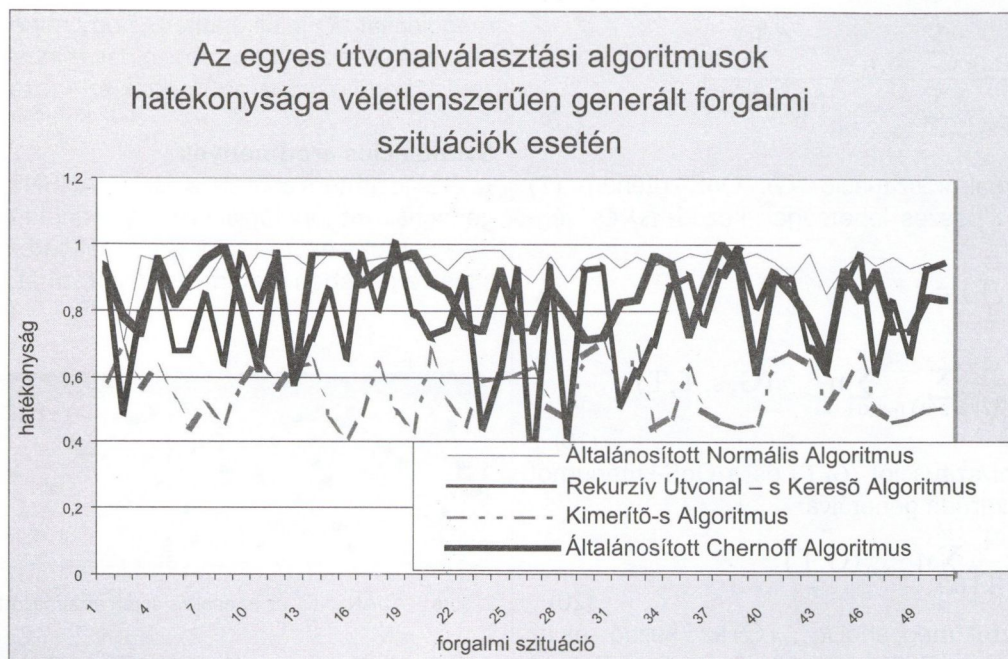
Az 1. táblázatban feltüntetett eloszlások alapján generálva a 2. ábrán látható hálózat linkjein a késleltetési értékeket a következő eredményeket kaptuk. A 3. ábra az egyes algoritmusok hatékonyságát (19) mutatja 50, véletlenszerűen generált forgalmi szituáció esetén. Látható, hogy a „Rekurzív Útvonalkereső – s Kereső Algoritmus” sokkal jobb minőségű útvonalválasztást eredményez, mint a „Kimerítő-s Algoritmus” (ahol  $S = \{0.5, 1.0, 1.5, \dots, 5.0\}$ ). Az ábra a más algoritmusokkal való összehasonlítás érdekében két további metódus [3], az „Általánosított Normális Algoritmus” és az „Általánosított Chernoff Algoritmus” hatékonyságát is ábrázolja. Az „Általánosított Normális Algoritmus” az MLP-t Gaussi-approximáció segítségével transzformálja SPR-feladattá, majd azt egy módosított Bellmann–Ford-algoritmus segítségével oldja meg. Az „Általánosított Chernoff Algoritmus” az itt ismertetett, Chernoff-egyenlőtlenségen alapuló technikát alkalmazza MLP-re, de a legrövidebb út megtalálására az „Általánosított Normális Algoritmus” módosított Bellmann–Ford-algoritmusához hasonló útkeresést végez.



3. ábra Az egyes algoritmusok hatékonysága a (19) teljesítmény-jellemző alapján

A 4. ábra a generált forgalmi állapotok felett végzett átlagolás eredményét mutatja (20) szerint, amelyből ugyancsak azt a következtetést lehet levonni, hogy a „Rekurzív Útvonalkereső – s Kereső Algoritmus” hatásos alternatívát jelent az útvonalválasztásra hiányos linkinformációk esetén.





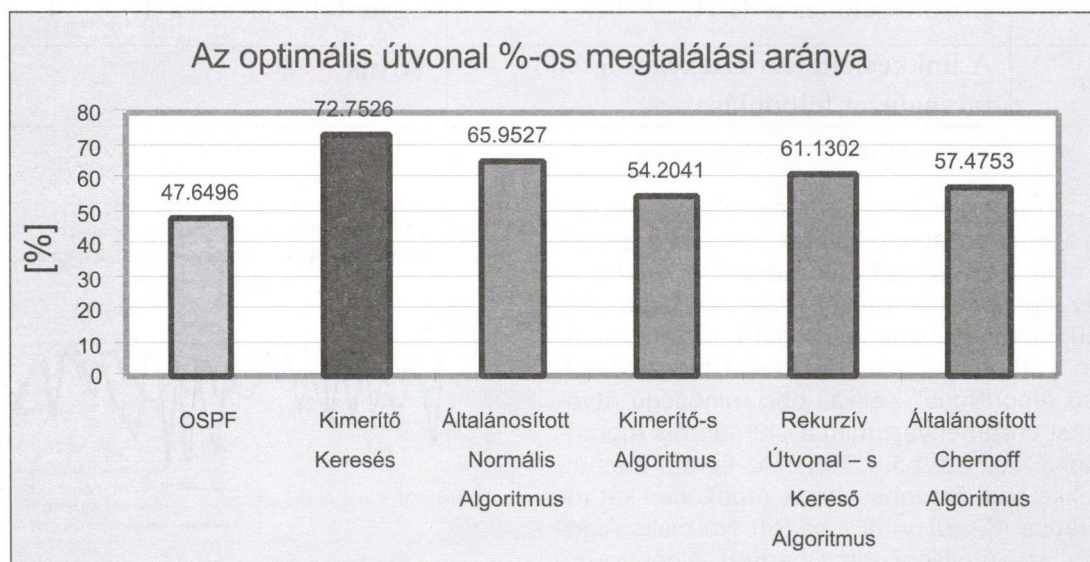
4. ábra Az egyes algoritmusok hatékonysága a (20) teljesítményjellemző alapján

A fenti két ábra ugyan alátámasztja a bemutatott „Rekurzív Útvonalkereső – s Kereső Algoritmus” hatásosságát, de nem mutatja meg, valójában milyen előny származik az algoritmus alkalmazásából a jelenlegi szabványokban megfogalmazott, napjainkban használatos eljárásokkal szemben.

Az 5. ábra az egyes algoritmusok által a generált linkértékek szerint optimális útvonal (csak a szimuláció ál-

tal ismert, hiszen ezen útvonal az útvonalválasztás pillanatában aktuális – a valóságban nem ismert – linkértékek alapján határozható meg) megtalálásának az arányát mutatja.

Az ábrán feltüntetésre került az OSPF PNNI ( $R_{OSPF}$ : SPR a  $t_i^{(u,v)}$  linkmérték szerint) által jelenleg elérhető arányszám is.



5. ábra Az optimális útvonal megtalálásának gyakorisága az egyes algoritmusok esetében

Az 5. ábra utolsó öt oszlopa alapján látható, hogy az útvonalválasztás során valószínűségi modellek felállításával a hálózat sokkal hatékonyabb (az OSPF-hez képest) kihasználása válik lehetővé. Nyilvánvalóan ezen modellek segítségével az OSPF-, PNNI-szabványokkal szemben akkor érhető el igazán jelentős előny, ha szigorú megkötések vannak a hálózatban jelzési célok érde-

kében felhasználható sávszélességre vonatkozóan. Ez a mi esetünkben azt jelenti, hogy a  $t_{i+1}-t_i$  nemlehet a lehetséges linkkésleltetési értékek tartójához képest egy relatívan kis érték. A rácshálózat felbontását növelve (ezzel együtt a hálózatban rendelkezésre álló sávszélesség nagy részének jelzési célokra történő felhasználásával) nyilvánvalóan ez az előny egyre inkább eltűnik.



Ugyanis,

- $\lim_{t_i \rightarrow 0} P(R_{OSPF} = \tilde{R}) = 1$  hiszen valószínűségi modell során használt eloszlások tartója egyre inkább a  $t_i$  értékre koncentrálódik, azaz  $P(\delta_{(u,v)} = t_i^{(u,v)}) \approx 1$ . Azaz ezen modellek alapján történő útvonalválasztás  $t_i^{(u,v)}$  linkmértékek szerinti SPR-feladattá redukálódik (OSPF, PNNI).
- $\lim_{t_i \rightarrow 0} P(\hat{R} = R_{OSPF}) = 1$  hiszen a Chernoff-egyenlőtlenség alkalmazása esetében az OSPF -, PNNI - algoritmus által szolgáltatott megoldáshoz való konvergencia analitikusan a következő módon fejezhető ki:

$$\begin{aligned} \tilde{R} : \min_R \sum_{(u,v) \in R} \lim_{t_{i+1}^{(u,v)} \rightarrow t_i^{(u,v)}} \mu_{(u,v)}(s) &= \min_R \sum_{(u,v) \in R} \lim_{t_{i+1}^{(u,v)} \rightarrow t_i^{(u,v)}} \log E e^{s \delta_{(u,v)}} = \\ &= \min_R \sum_{(u,v) \in R} \lim_{t_{i+1}^{(u,v)} \rightarrow t_i^{(u,v)}} \log \left[ \sum_{j=0}^{2M+1} p_j \exp \left\{ s \left( t_i^{(u,v)} + j \frac{t_{i+1}^{(u,v)} - t_i^{(u,v)}}{2M} \right) \right\} \right] = \\ &= \min_R \sum_{(u,v) \in R} \lim_{t_{i+1}^{(u,v)} \rightarrow t_i^{(u,v)}} \log \left[ e^{s t_i^{(u,v)}} \sum_{j=0}^{2M+1} p_j \exp \left\{ j s \frac{t_{i+1}^{(u,v)} - t_i^{(u,v)}}{2M} \right\} \right] \end{aligned}$$

azaz

$$\begin{aligned} \tilde{R} : \min_R \sum_{(u,v) \in R} \left\{ s t_i^{(u,v)} + \lim_{t_{i+1}^{(u,v)} \rightarrow t_i^{(u,v)}} \log \left[ \sum_{j=0}^{2M+1} p_j \exp \left\{ j s \frac{t_{i+1}^{(u,v)} - t_i^{(u,v)}}{2M} \right\} \right] \right\} = \\ = \min_R \sum_{(u,v) \in R} s t_i^{(u,v)} = \min_R \sum_{(u,v) \in R} t_i^{(u,v)} \quad \forall s > 0 \end{aligned}$$

A rácshálózat felbontását egyre inkább finomítva a valószínűségi modellek ( $\hat{R}$ ), az OSPF vagy PNNI által szolgáltatott útvonalak ( $R_{OSPF}$ ) egyre gyakrabban egyeznek meg az optimális útvonallal ( $\tilde{R}$ ).

## Összefoglalás

A cikkben egy új útvonalválasztási algoritmust mutattunk be, amely figyelembe veszi az útvonalválasztási feladat technológiai okokból származó valószínűségi tulajdonságait az additív metrika esetén keletkező NP nehéz probléma optimális megoldásának jó minőségű approximációjára. Az eredeti probléma SPR-feladattá konvertálása által az algoritmus az útvonalválasztást gyorsabban képes elvégezni. A napjainkban kidolgozott útvonalválasztási algoritmusokkal [6,7,9,10] szembeni hátránya, hogy nem képes elosztott módon működni többszörös útvonalak keresésére. A működés

jellegéből adódóan szükséges még a valószínűségi modell által megkívánt linkenkénti eloszlások kezelése vagy legalább arra vonatkozó a priori információk begyűjtése, ami további kutatásaink tárgya.

## Irodalom

1. Cherukuri, R.–Dykeman, D.: „PNNI draft specification”. ATM Forum 94-0471, November 1995.
2. Lorenz, D.–Orda, A.: “QoS routing in networks with uncertain parameters”, IEEE/ACM Trans. Networking, vol. 6., December 1998, pp. 768–778.
3. Levendovszky, J.–Rétvári, G.–Dávid, T.–Fancsali, A.–Végső, Cs.: “QoS routing in packet switched networks – novel algorithms for routing with incomplete information”, Proceedings of 9th IFIP Working Conference on Performance Modelling and Evaluation of ATM & IP Networks. Budapest, Hungary, 27-29 June, 2001. pp. 249–260.
4. Lee, W.: “Spanning tree methods for link state aggregation in large communication networks”. Proc. INFOCOM, Boston, MA, April 1995.
5. Guérin, R.–Orda, A.: “QoS routing in networks with inaccurate information: theory and algorithms”, IEEE/ACM Trans. Networking, vol. 7., June 1999, pp. 350–364.
6. Chen, S.–Nahrstedt, K.: “Distributed QoS Routing with Imprecise State Information”. Proceedings of 7th IEEE International Conference on Computer, Communications and Networks, Lafayette, LA, October 1998. pp. 614–621.
7. Chen, S.–Nahrstedt, K.: “On Finding Multi-Constrained Paths”. Proceedings of 7th IEEE International Conference on Communications, Atlanta, GA, June 1998. pp. 874–879.
8. Chen, S.–Nahrstedt, K.: “An overview of quality of service routing for next generation high-speed networks: Problems and solutions”. IEEE Network Magazine, Special Issue on Transmission and Distribution of Digital Video, November-December 1998. 12(6): 64–79.
9. Sun, Q.–Langendorfer, H.: “A new distributed routing algorithm with end-to-end delay guarantee”, IWQoS'97, May 1997.
10. Kelly, F. P. – Williams, R. J.: “Dynamic Routing in Stochastic Networks”, Stochastic Networks, 71: 1995. pp. 169–186.
11. Gallager, R. G.: “Information Theory and Reliable Communication”. Wiley, 1968.



NEM MINDIG ILYEN NYILVÁNVALÓ A NEM KIELÉGÍTŐ MINŐSÉG









hozzáférési hálózatban is, fontos feladat a megfelelő mechanizmusok kidolgozása szolgáltatásminőség (QoS – Quality of Service) biztosítására a RAN-ban. Az UMTS-rendszerek a szolgáltatások széles spektrumát nyújtják az előfizetők számára, ezen szolgáltatások közül csak egy a speciális minőségigényű telefónia. [3][4]

## A telefónia minőségi igényei

A beszédkommunikáció szűk korlátot kíván meg a jel körbejárási késleltetésére, amit 200–400 ms-ban szab meg. Természetesen nem lehet pontos értéket adni e késleltetésekorlátra, hiszen ez nagymértékben függ a kommunikáló felek szubjektív beszéd minőség megítélésétől. A csomagvesztés mindemellett nem jelent olyan nagy problémát, mint adatátvitelnél. Az igényelt sáv szélesség csökkentése érdekében azonban a beszédet kódolt formában visszük át. A kódolt átvitel érzékenyebb a csomagvesztésre, ezért ennek korlát alatt tartása is fontos szempont. A legnagyobb problémát az egymás után jövő csomagok elvesztése, a burstös csomagvesztés jelenti, ezért csomagkapcsolt hálózatokban, ahol a csomagvesztés ilyen tulajdonságú, erre is érdemes odafigyelni.

## Topológia

Cikkünkben egy IP-alapú hozzáférési hálózatot (IP-BSS – IP based Base Station Subsystem) mobil hozzáférési hálózaton vizsgáltunk a különböző ütemezési és táркеzési eljárások szempontjából. Mivel a célunk az volt, hogy megvizsgáljuk az általunk javasolt módszerek alkalmazhatóságát a telefonbeszélgetések kezelésére, a hálózatot úgy tekintettük, mintha csak hangforgalom számára lenne dedikálva.

A választott hálózati topológia 3G-RAN architektúrán alapul. A RAN a bázisállomásokból (BS – Base Station) és vezérlőkből (RNC – Radio Network Controller) épül fel. Mivel a 3G rendszerek bevezetése a ma meglévő 2G rendszereken alapul, sok mai eszköz fog együtt létezni és üzemelni az új technológiákkal. Ezért meg kell találni a módot a különféle eszközök együttműködésére. A szolgáltatók is minél kevesebb eszköz lecserélésével kívánnak átlépni a 3G „korába”, hiszen ezzel komoly költségeket takaríthatnak meg. Ezért nem csoda, hogy sokan a ma meglévő BSS-hálózatot kívánják felhasználni az UMTS hozzáférési hálózatának, ezért már vizsgálják az IP bevezetésének módját a BSS-hálózatokba. Mi is ezért választottuk vizsgálataink alapjául a ma igen elterjedt fa struktúrájú BSS-hálózatot (1. ábra). Mivel minden csomagnak el kell jutnia a topológia csúcsára, valamint feltételezve, hogy minden BS által lefedett terület azonos módon generálja a forgalmat, a sáv szélességeket hierarchikusan állítottuk be, mellyel csökkenthető a szolgáltató által sáv szélességbe ruházott tőke.

## Kiszolgálási modell

Egy egyszerű modellt választottuk, ahol mindössze egy minőségi paramétert rendeltünk a hívásokhoz, ez a késleltetéselevárás. A hangcsomagok végponttól végpontig terjedő késleltetése számos tényezőtől adódik. A (i) kódolási késleltetés ( $D_{enc}$ ) az az idő, mely az analóg jel kódolásához szükséges. Ez a keretképzési időből, az előretekintési késleltetésből és a feldolgozási időből áll. A (ii) csomagolási késleltetés, mely annak a függvénye, hogy hány keret kerül egy csomagba. A hálózatban haladva minden csomag minden csomópontonál várakozik, ez az (iii) átviteli késleltetés ( $T_h$ ). Ehhez járul még a (iv) jelterjedési késleltetés ( $P_h$ ) és (v) sorban állási késleltetés ( $Q_h$ ). A vevőben a csomagok várakoznak a (vi) visszajátszási vagy jittermentesítő pufferben ( $D_{playback}$ ), végül pedig (vii) dekódolódnak. Ha úgy tekintjük, hogy a processzási idők elhanyagolhatóan kicsik, akkor a teljes késleltetés a következőképpen adódik:

$$D = D_{enc} + \sum_{h \in path} (T_h + P_h + Q_h) + D_{playback}$$

Legrosszabb esetben [5] a  $D_{playback}$  a maximális sorban állási idő, amit a csomag elszoríthat a hálózatban, hiszen ez adná a legnagyobb lehetséges jittert.

Szimulációs vizsgálataink során az RPE-LPC codecet feltételeztük. Jó minőségűnek tekinthető átvitelt szerettünk volna biztosítani, ezért az egyirányú megengedhető késleltetés  $D = 100$  ms.

A késleltetéselevárás mellett figyelembe kell venni az adott híváshoz tartozó útvonalat, pontosabban a csomópontok közötti szakaszok (hop) számát. Hiszen két azonos késleltetéselevárással, de különböző hop számmal rendelkező hívás közül a nagyobb hop számút kell előnyben részesíteni, hiszen annak a késleltetés elvárása több csomópontra oszlik el.

## Forgalomszabályozás

A forgalomszabályozás feladatai: (i) hívásengedélyezés (CAC – Call Admission Control), (ii) csomagosztályozás és (iii) csomagkezelés (ütemezés és táркеzés).

A QoS-garanciákat biztosító modellek alapja, hogy a kapcsolat kezdeményezésekor a kliens az adni kívánt forgalom típusát és az igényelt minőséget megadja. Ez alapján a rendszer dönt, hogy elfogadja-e az új kérelmet, ha igen, akkor ezzel garantálja a kért minőséget mindaddig, amíg a kliens meg nem szegi a forgalmi specifikációt. Vizsgálataink során arra voltunk kíváncsiak, hogy megoldásaink mennyire hatásosak, ezért hívásengedélyezési kérdésekkel nem foglalkoztunk.

Ahhoz, hogy valóban teljesíteni tudja a hálózat a kívánt QoS-t, megfelelő csomagkiszolgálási mechanizmusokra van szükség a routerekben. Csomagkapcsolt hálózatokban a csomagok minden csomópontban kölcsönhatásba kerülnek egymással. Megfelelő szabályozás nélkül ez az egymásra hatás negatívan befolyá-



solhatja a hálózat teljesítményét. A csomagkiszolgálási mechanizmusok szabályozzák a csomagok kiszolgálását és ezzel azok egymásra hatását. [8] A két legfontosabb erőforrás a sáv szélesség és a tárhelykapacitás. Az ezeket kezelő módszerek az ütemezés és a táркеzelés. A táркеzelés dönt arról, hogy mely csomagokat tárolja és melyeket dobja el. Az ütemezés pedig kiválasztja, hogy mely csomag legyen a következőként kiszolgálva.

## Legkorábban lejáró ütemező

A legkorábban lejáró (EDF – Earliest Deadline First) ütemező a dinamikus prioritásos ütemezők egy formája. Lejáratit időt ( $D_{ij}$ ) rendel az ütemező minden csomaghoz, ami a beérkezési idő ( $a_{ij}$ ) és a lokális késleltetési korlát ( $d_{ij}$ ) összege (i. szervernél, j. folyam csomagjaihoz):

$$D_{ij} = a_{ij} + d_{ij}$$

A legkisebb lejáratit idejű csomag kerül először továbbításra. Az EDF-ütemező minimalizálja a csomagok maximális késleltetését, ahol a késleltetés a lejáratit idő és a valódi továbbítási idő különbségeként értendő. Másik fontos tulajdonsága, hogy ha homogén a forgalom, akkor a lejáratit idő túllépésének a valószínűsége minden folyamra egyenlő. [9][10]

## Javasolt csomagkiszolgáló eljárások

A javasolt megoldások mind az EDF-ütemezőn alapulnak. Azért esett az EDF-re a választás, mert egy olyan ütemezőre volt szükség, mely képes megfelelő szolgáltatásminőségi differenciálást biztosítani, ugyanakkor csak egyszerű mechanizmusokat használ. Így a létesítési költségeket alacsonyan lehet tartani. Továbbá megfelelő hívásengedélyező eljárásokkal az EDF-ütemezővel lehetőség van késleltetési korlát-garanciákat nyújtani.

**BE:** A hagyományos best-effort szolgáltatásnál használt, „elsőit először” (FIFO – First In First Out) ütemező.

**S4:** A lejáratit idő ( $D$ ) számítását úgy alakítottuk, hogy jobban megfeleljen a modellünknek.

$$D = a + \frac{\text{késleltetéselvárás}}{\text{hátralévő hopok száma}}$$

A késleltetéselvárás azt adja meg, hogy mennyi idő áll a csomag rendelkezésére, amit sorban állással tölthet el a célíg. E változó számítása a következő: a minimális átviteli idő ismert, legyen ez  $d_{static}$ , ez alapján a forrásnál  $E - d_{static}$  érték kerül a csomagba, ahol  $E$  a megengedett késleltetéselvárás. Majd minden csomópontban a csomag távozásakor a sorban állási késleltetéssel csökkentjük az értéket.

**S7:** Ennél a módszernél az eltérő átviteli időket is figyelembe vettük, így a számítás kissé bonyolódik (a j.

folyam k. csomagja, az i. csomópontban, és n az utolsó router az útvonalon):

$$D_{ij}^k = a_{ij}^k + \left\{ \frac{\text{késleltetéselvárás}_{ij}^k}{\sum_{l=i}^{n-1} \text{átviteli idő}_{lj}} \right\} * \text{átviteli idő}_{ij}$$

Megfelelő táркеzelési eljárások is szükségesek a hatékony működéshez.

**B1:** A módszer lényege, hogy minden csomagot dobunk el, melynek már nincs ideje a routerekben várakozni.

$$\text{késleltetéselvárás} < 0$$

**B2:** E megoldásnál az eltérő átviteli időket is figyelembe vesszük, és minden olyan csomag eldobásra kerül, melynek már nincs mód legalább egy csomag kiszolgálását megvárni a hátralévő csomópontokban.

$$\frac{\text{késleltetéselvárás}_i}{\sum_{l=i}^{n-1} \text{átviteli idő}_l} < 1$$

## Csomagokra bontás

A GSM-hálózatokban használt hangkeretek továbbításához az IP-hálózatban azokat csomagokba kell foglalni. A fő problémát a nem hasznos terhelés minimalizálása jelenti. A cél tehát az IP-csomagok fejrész általi okozott terhelés csökkentése. Alapvetően két megközelítés létezik. Az egyik minél több keretet gyűjt egy csomagba, de ez megnöveli a késleltetést, hiszen a csomagképzési idő az összeggyűjtött keretek számával arányosan nő. A másik módszer a fejrész méretének csökkentését írja elő. Vizsgálataink során ezt az utóbbit módszert választottuk. Fejrész-tömörítési eljárásokkal az IP-, UDP- és RTP-fejrészek 4 bájtba tömöríthetők, CRC-mezővel együtt.

| Tömörített IP-fejrész | Differenciáláshoz szükséges mezők | Payload (egy 20 ms-os keret) |
|-----------------------|-----------------------------------|------------------------------|
| 4 bájt                | 3 bájt                            | 33 bájt                      |

2. ábra Csomagszerkezet

Annak ellenére, hogy a fejrész-tömörítés extra mechanizmusokat követel meg a csomópontokban, és periodikusan igényli a teljes fejrész újraküldését, összességében mégis jó megoldás a többletterhelés csökkentésére. A fejrész-tömörítésről bővebben a [6] és [7] referenciákban találhat az érdeklődő olvasó.

Szimulációinkban egy csomag egy keretet tartalmazott, mely 33 bájt hosszú volt (RPE-LPC-nek megfelelően), emellett a késleltetéselvárás és hop szám tárolá-



sára két mező volt szükséges összesen 3 bájtot igényelve. Hozzáadva a 4 bájtos tömörített fejrészt, a teljes csomagméret 40 bájtra adódik. (2. ábra.)

## Szimulációs eredmények

A szimulációs vizsgálatokat 30%, 70% és 90% hálózati terhelés mellett végeztük, ezek alapján jól kirajzolódott, hogy amennyire hatékonyak az egyes megoldások. A szimulációkat Network Simulator segítségével végeztük. Vizsgálódásaink további feltételeit a Budapesti Műszaki és Gazdaságtudományi Egyetemen működő Nagysebességű Hálózatok Laboratóriuma biztosította.

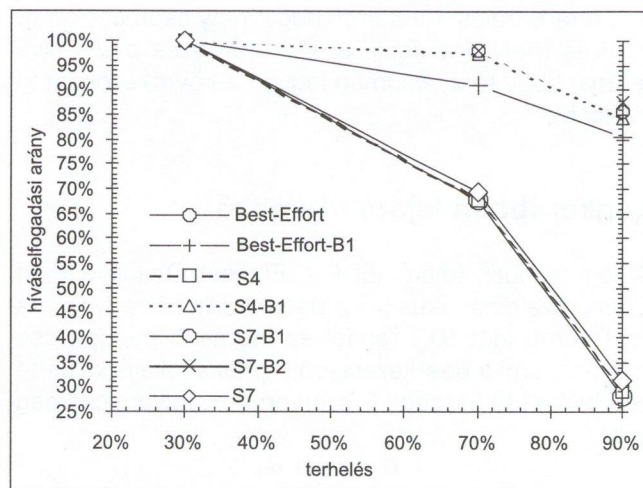
### Teljesítmény-mérőszámok

A fő teljesítményjellemző, melyet az eredmények kiértékelésénél használtunk, a hívásfogadási szabályt kielégítő hívások száma volt. Egy hívás akkor elégíti ki a hívásfogadási szabályt, ha csomagjainak 90 százaléka a késleltetési követelményeket kielégítve ér célba. A cél tehát, hogy a lehető legtöbb hívás teljesítse ezt a szabályt. Természetesen nem csak ezt kell figyelembe venni az eredmények kiértékelésekor. A telefónia számára a három érzékeny mérőszám a késleltetés, a csomagvesztés és a jitter. A késleltetést figyeljük a fent említett szabállyal. A csomagvesztés elfogadhatóan kis értéken tartása és a jitter alacsonyan tartása ugyancsak elengedhetetlen. A bemutatásra kerülő differenciálás során még egy fontos kérdés merül fel, a pártatlanság kérdése. Mivel a hop számot is figyelembe vesszük a hívások csomagjai közti megkülönböztetés során, vigyázni kell, nehogy a rövidebb vagy a hosszabb útvonalon haladó csomagok előnyösebb helyzetbe jussanak, hiszen ez azt eredményezné, hogy attól függően, hogy topológiaiilag hosszabb vagy rövidebb útra kényszerülnek a csomagok, az előfizető különböző minőségű kiszolgálást kapna a hálózattól. Ezért a módszerek ilyen irányú teljesítményét is nagyító alá vesszük.

### Hívásfogadási arány

Mivel a legfontosabb mérőszámnak a hívásfogadási szabályt kielégítő hívások számát tekintettük, ezért ennek a bemutatásával kezdjük a sort. A 3. ábra a szabályt teljesítő hívások és az összes hívás arányát mutatja a terhelés függvényében. Az ütemező megoldások közül a legrosszabb a BE, a legjobb az S7 megoldás. A különbségek a terhelés növelésével egyre jobban kirajzolódnak. A 3. ábrán jól megfigyelhető, hogy a szolgáltatásnak megfelelő tárkezelést nem alkalmazó megoldások – ahogy az várható volt – nagyon gyengén teljesítenek a megfelelő pufferkezelést alkalmazókhöz képest. Tehát, a B1 és B2 tárkezelések segítségével a hívásfogadás jelentősen növelhető, továbbá elmondható, hogy a B2 megoldás effektívebb, hiszen nagyobb terhelés mellett jobb eredmény elérését teszi lehetővé. Összegezve ebből a szempontból a legjobban az

S7-B2 kombináció vizsgázott. A megfelelő következtetések levonásához elengedhetetlen, hogy megvizsgáljuk az egyes módszerek teljesítményét a csomagvesztés, a jitter és a pártatlanság terén is.



3. ábra Elfogadott hívások aránya a terhelés függvényében

### Csomagvesztés

A hangátvitel szempontjából relatív kis csomagvesztés szükséges, mivel a beszédminőség gyorsan romlik, ha nő a csomagvesztés. A csomagvesztést is a terhelés függvényében vizsgáljuk.

A csomagvesztés elsősorban a felhasznált pufferkezelési módszerektől függ. Az 4. ábrán jól megfigyelhető, hogy a csomagvesztés akkor a legnagyobb, ha a szolgáltatásspecifikus csomageldobási mechanizmusokat használjuk. Ez annak köszönhető, hogy minden olyan csomagot eldobunk, melyet az adott algoritmus úgy ítél meg, hogy már nincs esély az időbeni célba juttatására. Ez a csomageldobás az ára annak, hogy ezen megoldások nagyobb hívásfogadást tudnak elérni. Hiszen minden csomag eldobásra kerül, mely fölöslegesen foglalna sávszélességet, és így megakadályozná más, esetleg még kielégíthető elvárású csomag célba juttatását.

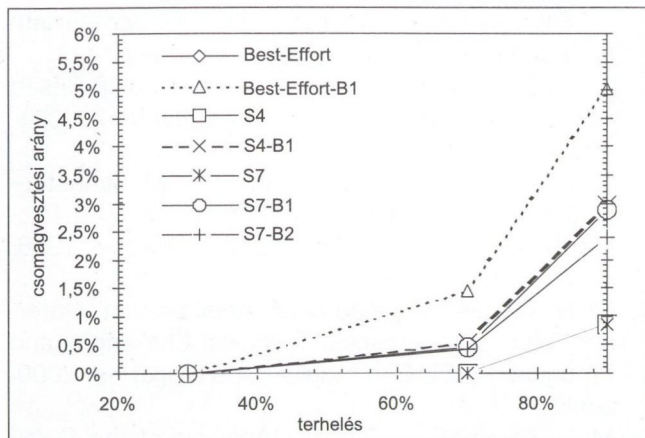
A legnagyobb csomagvesztés a BE-B1 kombinációnál tapasztalható. Ez elsősorban annak köszönhető, hogy a FIFO-kiszolgálás miatt az egyes hangcsomagok nem a rendelkezésükre álló késleltetési tartalék alapján kerülnek továbbításra, így annak a valószínűsége, hogy lejár az idejük, elég nagy.

Ebből a vizsgálati szempontból is elmondható, hogy az S7-B2 megoldás elfogadhatóan alacsony dobási arányt produkált, így figyelembe véve az elfogadott hívások arányát is, az S7-B2 egy jó választásnak tekinthető.

### Jitter

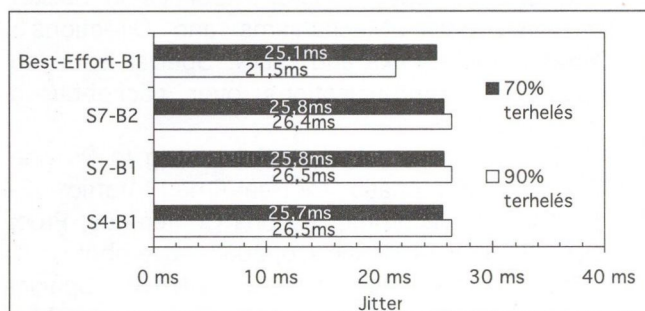
Mivel a vevő oldalon alkalmazott jittermentesítő puffer mérete a maximális jitter értékétől függ, ezért fontos, hogy a késleltetésingadozást minél kisebb értéken tartsuk. A szimulációk azt mutatták, hogy a tárkezelési eljárások alkalmazása nélkül a jitter elfogadhatatlanul magas a telefonszolgáltatás számára. Ugyanakkor, ha





4. ábra Csomagvesztés a terhelés függvényében

alkalmazzuk a B1 vagy B2 megoldást, a jitter az alkalmazott ütemezési eljárástól lényegében függetlennek tekinthető, egyedül a BE megoldás kivétel ez alól (5. ábra). A legkisebb jitter a BE-B1 megoldással kapható, ez annak köszönhető, hogy a FIFO-kiszolgálás miatt az egyes hívások jitternövekedése lényegében csak a terheléstől függ. Ebből a szempontból tehát a BE-B1 megoldás a legjobb, de nem annyira kiemelkedő az eredménye, hogy ezzel kompenzálna nagyon gyenge teljesítményét a hívásfogadás terén.



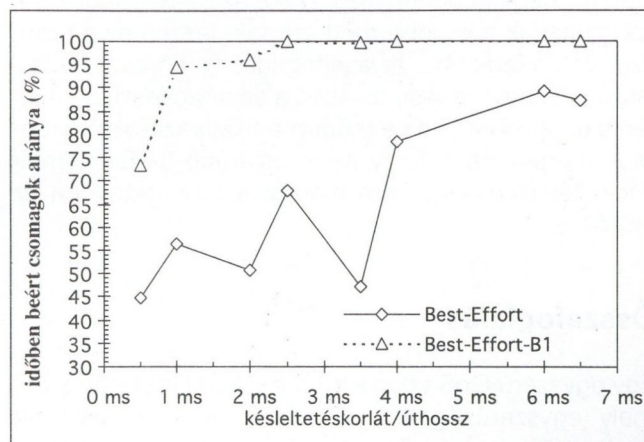
5. ábra Jitter

### Pártatlanság

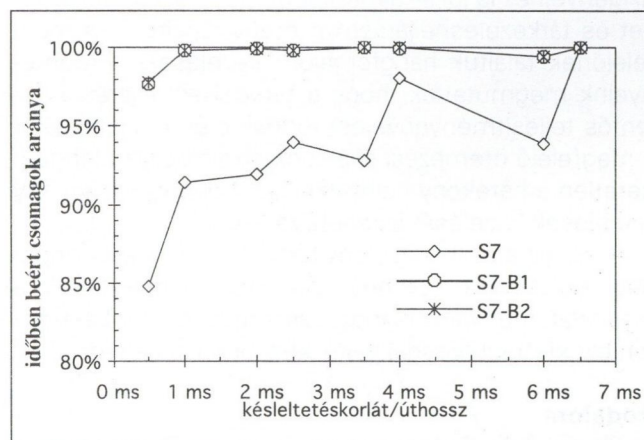
A pártatlanság kérdése nagyon fontos, hiszen megengedhetetlen, hogy egy hívás csak azért kapjon rosszabb minőségű kiszolgálást, mert hosszabb utat kell megtennie csomagjainak. A pártatlanság a választott ütemezőtől és a táркеzelési eljárástól egyaránt függ. Általánosságban elmondható, hogy minél bonyolultabb az ütemező és a puffervezelő eljárás, annál jobb az eredmény a pártatlanság szempontjából.

A BE megoldás a legegyszerűbb ütemezőt alkalmazza, a FCFS-t, így nem csoda, hogy itt a legrosszabb a pártatlanság. Táркеzelés alkalmazásával ez javítható, de még így is jelentősen elmarad a többi megoldás eredményétől. A 7. és 8. ábrák az időben beért csomagok arányát mutatják a késleltetéskorlát/úthossz függvényében. Mivel a késleltetéskorlát a szimulációk során nem változott (minden hívásnak adott minőségű szolgáltatást kívántunk nyújtani), ezért az ábrák tulajdonképpen az úthossz függvényében mutatják a beérési arányt. A rövid utak a grafikon bal oldalán, a

hosszú utak a jobb oldalán helyezkednek el. Ideális esetben egy egyenest kellene látnunk. Az S4 és S7 megoldások nagyon hasonlóan viselkedtek, ezért csak az S7 eredményeit ábráztuk. Jól látható, hogy az S7-B1 és az S7-B2 jól közelíti a kívánt egyenest, ezért ezek fairnek tekinthetők (7. és 8. ábra).



7. ábra Pártatlanság 90% terheltségnél



8. ábra Pártatlanság 90% terheltségnél

### Összefoglaló

Vizsgálataink elején felvázoltunk egy egyenletet, mely alapján a késleltetéskorlátot számoltuk azzal a céllal, hogy a 100 ms-os egyirányú késleltetést ne lépjük túl. Most felhasználhatjuk a szimulációs eredményeket, hogy a valóban elért késleltetés maximumát származtathassuk.

$$D = D_{enc} + \sum_{h \in path} (T_h + P_h + Q_h) + D_{playback}$$

A legrosszabb esetben  $D_{playback}$  a maximális jitterrel egyenlő. A késleltetéskorlát célja az volt, hogy korlátot szabjon a értéknek (vizsgálataink során 47 ms-ban). A maximális jitter a szimulációk alapján 90% terhelés mellett adódott, 26,5 ms. Ekkor az egyirányú késleltetés  $D = 20 \text{ ms} + 47 \text{ ms} + 26,5 \text{ ms} = 93,5 \text{ ms}$ . Tehát nem csupán a kívánt 100 ms-ot sikerült elérni, hanem még az elhanyagolt processzási időkre is maradt tartalék.

Az eredmények alapján kitűnik, hogy mindkét megoldás, az S4 és az S7 jól kezeli e speciális környezet és



szolgáltatás igényeit. A megfelelő szolgáltatásspecifikus pufferkezelés jelentős hatása is megfigyelhető a grafikonokon. A pártatlanság szempontjából is jól vizsgáltak különböző megoldások, hiszen az ideális esetet, a vízszintest jól közelítették.

Amennyiben az egyes megoldások komplexitása nem mérlegelendő tényező, akkor az S7-B2 megoldást választhatjuk a legjobb módszernek, hiszen ez a módszer volt a legjobb a hívásfogadás terén és a pártatlanság szempontjából, továbbá a csomagvesztés és jitter is elfogadható volt e módszer alkalmazásakor. Érdeemes megemlíteni, hogy az egyszerűbb S4-B1 kombináció teljesítménye sem maradt el számottevően az előzőétől.

## **Összefoglalás**

Egy egyszerű QoS-t biztosító megoldást mutattunk be, mely egyszerűségével jól illeszkedik a Differenciált Szolgáltatások modelljéhez. A felvázolt differenciálás a fa topológiájú hálózathoz és a telefonszolgáltatás egyedi igényeihez is jól alkalmazkodott. A javasolt ütemezőket és tárkezelési eljárásokat megvizsgáltuk, és megfelelőnek találtuk hangforgalom kezelésére. Eredményeink megmutatták, hogy a tárkezelési eljárások jelentős teljesítménynövelést tudnak elérni, ugyanakkor a megfelelő ütemezési eljárások alkalmazása elengedhetetlen a hatékony hálózatkihasználáshoz, mely nagy terhelések kezelését is lehetővé teszi.

A vizsgálatok során nem tértünk ki a hívásbeengedési eljárásokra, jóllehet ezek elengedhetetlenek a gyakorlati megvalósításhoz, ezért további munkánk során ezt kívánjuk vizsgálataink központjába helyezni.

## **Irodalom**

1. Takács A.–Császár A.–Lukovszki Cs.–Szabó R: "Simulation Study over IP Based GSM Backbone".

- IEEE International Conference on Telecommunication, Bucharest, Románia, 2001. június 4–7.
2. Lieve Bos–Suresh Leroy: "Toward an All-IP-Based UMTS System Architecture". IEEE Network, 2001. január/február.
3. T. J. Kostas–M. S. Borella–I. Sidhu–G. M. Schuster–J. Grabiec–J. Mahler: "Real-Time Voice Over Packet Switched Networks". IEEE Network, 1998. január/február.
4. M. Hassan–A. Nayandoro–M. Atiquzzaman: "Internet Telephony: Services, Technical Challenges and Products". IEEE Communications Magazine, 2000. április.
5. M. J. Karam–F. A. Tobagi: "Analysis of the Delay and Jitter of Voice Traffic Over the Internet". IEEE INFOCOM 2001, Anchorage, Alaska, 2001. április 22–26.
6. M. Engan–S. Casner–C. Bormann: "IP Header Compression over PPP". IEEE RFC 2509, 1999. február.
7. S. Casner–V. Jacobson: "Compressing IP/UDP/RTP Headers for Low-Speed Serial Links". IEEE RFC 2508, 1999. február.
8. Hui Zhang: "Service Disciplines for Guaranteed Performance Service in Packet-Switching Networks". Proc. IEEE, Vol. 83.
9. R. Guérin–V. Peris: "Quality-of-Service in Packet Networks Basic Mechanisms and Directions". Computer Networks and ISDN. Special issue on multimedia communications over packet-based networks, 1998.
10. Stefan Bodamer: "A New Scheduling to Provide Relative Differentiation for Real-Time IP Traffic". IEEE Global Telecommunications Conference, Proc. pp. 646–650, San Francisco, 2000. november.
11. "The European Path towards UMTS". Special issue of the IEEE Personal Communications Magazine, February 1995.



# Gyűrűhierarchia – megbízható IP-mikromobilitási hálózati topológia

IMRE SÁNDOR–SZALAY MÁTÉ

Budapesti Műszaki és Gazdaságtudományi Egyetem (BME), Híradástechnikai tanszék

*A Mobile IP, az internet mobilitási protokollja jól támogatja a globális mobilitást, azonban cellás mobilitási környezetben túl lassú. Olyan környezetekben, ahol nagyon gyakori a cellaváltás, mikromobilitási protokollokra van szükség. A legtöbb mikromobilitási protokoll fa topológiájú hálózatot használ, mert ilyen hálózatban az útvonalválasztás (routing) viszonylag egyszerű. Azonban egy ilyen topológiájú hálózat megbízhatósága gyenge. Ez a cikk egy speciális hálózati topológiát, az ún. gyűrűhierarchiát mutatja be. Ez a topológia jól megfelel a mikromobilitási hálózatok követelményeinek. Sokkal megbízhatóbb, mint a fa topológia, és az útvonalválasztása sem sokkal bonyolultabb.*

## Bevezetés

Napjainkban az internet és a távközlés konvergál egymáshoz. Ennek a konvergenciának az eredményét infocom hálózatnak hívják, mely előreláthatólag IP-alapú hálózat lesz. A követelmények ma már merőben mások, mint az IPv4 tervezésekor, ezért az IPv6, az új verzió számos kiegészítést és módosítást fog tartalmazni. Az új hálózatnak új forgalmi igényeket kell kielégítenie: a beszédátvitelnél kis késleltetés szükséges, adatátvitelnél nagy sáv szélesség. Az IPv4 mobilitáskezelése nehézkes volt, a Mobile IP azonban szerves részt képez az IPv6-nak [9.] [10].

Az egységes infocom hálózat egy közös IP-gerinchálózattól és hozzáférési hálózatokból áll. A tendencia azt mutatja, hogy a vég-vég IP-kapcsolatok biztosítása érdekében a hozzáférési hálózatokat is IP-alapra kell helyezni. Az „IP-gerinchálózat” és az „internet” kifejezéseket ebben a cikkben szinonimaként használjuk.

Mivel a Mobile IP [4] sok kommunikációt igényel a mobilegység (mobile node, MN) és az otthoni ügynök (home agent, HA) között, globális, de lassú mobilitást biztosít (makromobilitás). Az otthoni ügynök értesítése néhány másodpercet vehet igénybe. Ezért van szükség mikromobilitási protokollokra.

A mikromobilitási protokollok egy jól körülhatárolt területen – általában egy hozzáférési hálózaton – belül biztosítanak mobilitást. A Mobile IP otthoni ügynök csak arról kap értesítést, ha a mobilegység belép a hozzáférési hálózatba vagy elhagyja azt, a hálózaton belüli cellaváltások esetén nem. A hálózaton belüli cellaváltásokat hálózaton belül kezeljük, ezért nagyon gyorsak, és nem generálnak forgalmat az IP-gerinchálózaton.

Bár a terület még nagyon új, máris számos mikromobilitási protokollajánlás létezik, például a Cellular IP [5] vagy a HAWAII [6]. Valamennyi fa topológiára épül,

ami gyors útvonalválasztást tesz lehetővé, ugyanakkor megbízhatósága gyenge.

Ez utóbbi probléma kiküszöbölésére szolgál a „gyűrűhierarchia” nevű hálózati topológia, amelyet ebben a cikkben részletesen bemutatunk. Áttekintést adunk arról, hogy ilyen topológiára hogyan lehet mikromobilitási protokollt építeni. A megbízhatóságra koncentrálunk, de más mikromobilitási szempontokról is szó lesz (pl. útvonalválasztás és paging).

A bevezető után a mikromobilitási hálózatok szokásos felépítését mutatjuk be. Ezt követően a különböző topológiaalternatívákat tekintjük át, pl. busz, csillag, gyűrű. Végül a gyűrűhierarchia topológiát ismertetjük.

Ez a cikk főleg az [1] és [2] irodalmakra támaszkodik.

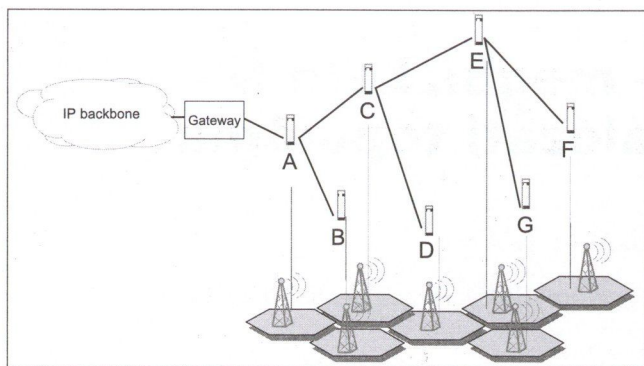
## Mikromobilitási hálózatok klasszikus felépítése

### Hálózati topológia

Az IP-mikromobilitási hálózatokat átjárók (gateway) kötik az IP-gerinchálózatra. A legtöbb mikromobilitási protokoll fa topológiájú hálózatot definiál, a fa gyökerében egyetlen átjáróval. A fában minden csomópontnak pontosan egy szülőcsomópontja van és lehet néhány gyermekcsomópontja. Az 1. ábrán például a C csomópont szülőcsomópontja az A csomópont, és egyik gyermekcsomópontja a D csomópont. Azokat a csomópontokat, amelyekhez nem kapcsolódik gyermekcsomópont, a fa leveleinek nevezzük. A levelek a bázisállomások (base station, BS) a mikromobilitási hálózatban, a többi csomópont útvonalválasztó (router).

Az IP-gerinchálózathoz csatlakozó gyökércsomóponton, vagyis az átjárón (lásd 1. ábra) a mikromobilitási hálózat teljes forgalma keresztül folyik.





1. ábra Fa topológiájú mikromobilitási hálózat

### Forgalomirányítás

A szolgálatelérési pontokat (service access point, SAP) a vezeték nélküli hozzáférés miatt bázisállomásoknak (base station, BS) nevezzük. Egy mikromobilitási hálózatban a forgalom nagy része a bázisállomások és az átjáró között folyik. A „downlink” forgalom (az átjárótól a bázisállomás felé) tipikusan sokkal nagyobb, mint az „uplink” forgalom (a bázisállomástól az átjáró felé), mert a mobilegységek hosszú válaszokat kapnak rövid kérdésekre, mint például webböngészés esetén.

A forgalomirányításnak időben változnia kell, mivel a mobilegység a hálózaton belül időről időre változtathatja a helyét. Tehát a forgalomirányítás a mikromobilitási protokollok lényeges része. Minden mobilegység aktuális pozícióját egy (esetleg elosztott) adatbázisban kell tárolni.

Minden router nyilvántartást vezet azokról a mobilegységekről, amelyek a router alatti részében kapcsolódnak a hálózathoz. Ezt a nyilvántartást „routing cache”-nek nevezik [7]. Így a routerek a megfelelő gyermekcsomópontnak tudják továbbküldeni az érkező csomagokat.

A mobilegységek által küldött („uplink”) csomagokat a routerek egyszerűen felfelé továbbítják a szülőcsomópont felé. A csomag lépésről-lépésre halad, amíg el nem éri a fa gyökerében található átjárót.

Ahogy feljebb és feljebb haladunk a fában, egyre nagyobb és nagyobb kapacitású összeköttetésekre van szükség.

### Megbízhatóság

A fa topológiából következően a hálózat bármely két csomópontja között pontosan egy út található. Tehát egy bázisállomás és a hálózat átjárója között egy út van.

Ez nyilvánvalóan egy sérülékeny topológia. Vizsgáljuk a topológiát egy olyan modell szerint, ahol a csomópontoknak és az összeköttetéseknek két állapotuk van: tökéletesen jó és tökéletesen rossz állapot. Egy link meghibásodása egyenértékű a link „alján” található csomópont meghibásodásával. Ha egy csomópont vagy összeköttetés meghibásodik, egy teljes részfa szakad le a hálózatról.

Még súlyosabb a helyzet, ha az átjáró vagy az átjáró és a gerinchálózat közötti link hibásodik meg. Ekkor a teljes mikromobilitási hálózat leszakad az internetről. Ilyenkor semmiféle adatátvitel nem lehetséges sem-

milyen, a hálózatban tartózkodó mobilegység és az internet egy más gépe között.

Ha ez a hálózati topológia ennyire sérülékeny, akkor miért épül a legtöbb mikromobilitási protokoll mégis fa topológiára? A válasz egyszerű: a fa topológia teljesen megfelel a mikromobilitási hálózat forgalomirányítási és jelzési igényeinek. Az útvonalválasztás mindkét irányban nagyon egyszerű. További előnye a topológiának a jó skálázhatóság.

A gyenge megbízhatóság kiküszöbölésére két út kínálkozik. Az egyik egy teljesen más topológia használata, a másik, hogy bizonyos változtatásokkal megpróbáljuk a fa topológiát megbízhatóbbá tenni. Ha az első megoldást választjuk, a topológia kiválasztásánál óvatosságnak kell lennünk. Több szempont szerint kell választani. Azáltal, hogy a fánál megbízhatóbb topológiát használunk, nem szabad az útvonalválasztást túlságosan bonyolulttá tennünk vagy a skálázhatóságot túlzottan lerontanunk.

Ha a fa topológiát módosítjuk, akkor a szempontjaink hasonlóak. A csomópontokat és összeköttetéseket duplikálhatjuk és fizikailag szétválaszthatjuk, hogy növeljük a megbízhatóságot. Az új topológia előnye, hogy sok tulajdonságát örökli a fától. Például a jelzések hasonlóak maradhatnak, és a topológia továbbra is megőrzi a jó skálázhatóságot. Ezzel együtt a forgalomirányítás bonyolultabb lesz, új protokollokra lehet szükség.

### Alternatív topológiák vizsgálata

Ebben a fejezetben néhány gyakorlatban használt hálózati topológiát vizsgálunk meg mikromobilitási szempontok alapján. A mikromobilitás legfontosabb szempontjai a következők:

- megbízhatóság, sérülékenységi,
- skálázhatóság,
- kapcsolódás az internethez,
- a forgalomirányítás bonyolultsága,
- speciális forgalom kezelése.

#### Fa

Ez a „klasszikus” mikromobilitási topológia. Fa topológiára épül a Cellular IP [5] és a HAWAII [6] is. Majdnem az összes követelménynek megfelel, legnagyobb hiányossága a sérülékenység.

#### Busz

Ha a busz topológiát több átjáró köti az internethez, a megbízhatóság megfelelő lehet. Útvonalválasztás nincs, helyette buszhozzáférési protokollt használunk. Ilyen hozzáférési protokoll az ALOHA vagy a CSMA. A legsúlyosabb probléma a rossz skálázhatóság. Ha busz topológiára építjük mikromobilitási hálózatunkat, a hálózat mérete erősen korlátozott lesz.

#### Csillag

A csillag egy erősen centralizált topológia. Minden csomópont a központi csomópontokhoz kapcsolódik. Nyilván



a központi csomópont lesz az átjáró a mikromobilitási hálózatban. Minden funkciót a központi csomópontba koncentrálhatunk, a többi csomópont nagyon egyszerű, tehát nagyon olcsó lesz. Csak a központi csomópontban van szükség forgalomirányításra. A csillag topológia nagyon jól illeszkedik a mikromobilitási hálózat forgalmi igényeihez, ahol a forgalom az átjárótól vagy az átjáróba folyik. A sérülékenységi probléma itt is probléma, mert a központi csomópont meghibásodásával a teljes hálózat használhatatlanná válik. Ennek kiküszöbölésére alkalmazhatunk kettős csillag topológiát. A központi csomópontot duplikáljuk, így ha az egyik meg is hibásodik, a hálózat tovább működik a másik csomóponttal.

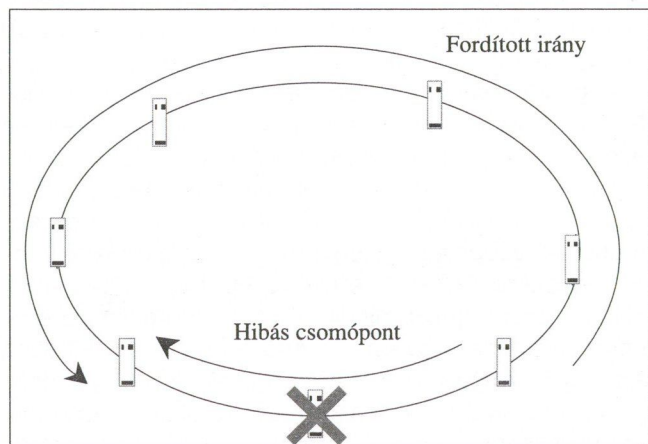
A csillag topológia egy másik hátránya a rossz skálázhatóság. Ha a bázisállomások számát növeljük, a forgalomirányítási feladatok miatt nő a központi csomópont terhelése.

## Gyűrű

Egy gyűrűben két út van bármely két csomópont között. Ha egy csomópont vagy összeköttetés meghibásodik, akkor is marad egy út, tehát ez a topológia sokkal robusztusabb a fánál. Megbízhatósági megfontolásokból nyilván több átjárót kell használni. A gyűrűben az útvonalválasztás is egyszerű. Hátránya, hogy nem igazán felel meg a speciális forgalomnak, és skálázhatósága is rossz. Ahogy a bázisállomások számát növeljük, a forgalomirányítás nem lesz bonyolultabb, csak az összeköttetések túlterhelte válhatnak.

Egy fontos gyűrűtípus az öngyógyító gyűrű. Egy öngyógyító gyűrűben a kapacitásnak csak a felét használjuk normális forgalomra, a másik fele tartalék, melyet meghibásodás esetén használunk fel. Öngyógyító gyűrű például az SDH MSSP (Multiplex Section Shared Protection) gyűrűje. Ha egy összeköttetés megszakad, vagy egy csomópont meghibásodik, a szomszédos csomópontok ezt észlelik, és az összes többi összeköttetés tartalék kapacitását hibajavításra használják fel (2. ábra). Így az IP-szint alatt javítottuk ki a hibát, tehát az IP-mikromobilitási protokollt egy megbízható topológiára építhetjük fel.

Gyűrű topológiájú mikromobilitási hálózatot mutat be részletesen a [2].



2. ábra Öngyógyító gyűrű működése

## Általános hálózat (mesh)

Teljes összeköttetést (full mesh) nyilván nem alkalmazhatunk, mert nagyon rosszul skálázható, és a különleges forgalmi igényeknek sem felel meg. Részleges összeköttetésű általános hálózat (partial mesh) több átjáróval skálázható, és megbízható megoldásnak tűnik. A probléma az, hogy az útvonalválasztás nagyon bonyolult. A csomagokat akkor is jól kell irányítani, ha néhány összeköttetés vagy csomópont hibás. Így bonyolult útvonalválasztási protokollra van szükség, melyben minden csomópontnak routerként kell működnie, így egy kis hatékonyságú és költséges megoldást kapunk.

## A gyűrűhierarchia

### Topológia

A fa topológiájú mikromobilitási hálózat megbízhatóságának javítása két alapvetően különböző módon történhet. Az egyik mód a topológia megváltoztatása, a másik mód egy teljesen új topológia alkalmazása. Ezt a két módszert próbáljuk meg valamilyen módon kombinálni.

A fa topológiában minden csomópontnak (a gyökeret kivéve) volt egy szülőcsomópontja, és lehetett néhány gyermekcsomópontja. A gyűrűhierarchia hasonlít a fa topológiára. Tulajdonképpen egy fa topológiáról van szó, ahol a csomópontokat gyűrűkkel helyettesítjük, és többszörös összeköttetést alkalmazunk. Minden gyűrűnek (a gyökérgyűrűt kivéve) van egy szülőgyűrűje, és minden gyűrűnek lehetnek gyermekgyűrűi. A gyűrűhierarchia pontosan egy gyökérgyűrűt tartalmaz, és az összes gyűrű öngyógyító gyűrű. Az összeköttetések kétirányúak, az egyik irányú kapacitást teljes egészében tartalékként használjuk, tehát a normális forgalom a gyűrűkön az irányban halad.

Ezen topológia segítségével egyesíthetjük a fa és a gyűrű topológiák előnyét. Olyan hálózati topológiát kapunk, amely a fánál sokkal megbízhatóbb, de hasonlít a fára, így sok, a fánál jól bevált ötlet alkalmazható itt is (mint például útvonalválasztó algoritmusok, cellaváltó algoritmusok).

### Csomóponttípusok

Nézzük, milyen fajta csomópontokból épül fel a gyűrűhierarchia:

- **átjáró + router:** A router továbbítja a csomagokat a gyűrű két szomszédos csomópontja és az átjáró között. Az átjáró küldi ki a csomagokat az internetre, és fogadja az onnan érkezőket. Ilyen típusú csomópontok csak a gyökérgyűrűben vannak, számuk egy tipikus hálózatban kettő-három.
- **bázisállomás + router:** A router továbbítja a csomagokat a gyűrűben két szomszédos csomópont és a bázisállomás között. A bázisállomás a rádiós interfészen keresztül küldi és fogadja a mobilegységek csomagjait.



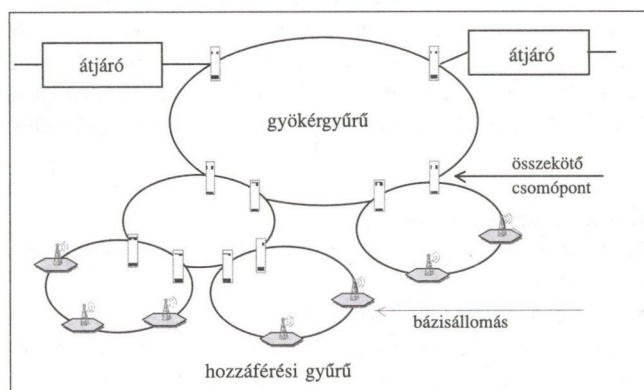
- összekötő csomópont (interconnection node): ezek a csomópontok kötik a gyűrűket a szülőgyűrűkhöz és a gyermekgyűrűkhöz. Két funkciót különíthetünk el az összekötő csomópontokban: átjárószerű funkciót a gyermekgyűrűben és bázisállomásszerű funkciót a szülőgyűrűben. Ezt a két funkciót betöltő hardvert fizikailag is különválaszthatjuk.
- router + speciális funkció: A gyűrűhierarchia tartalmazhat olyan csomópontokat is, amelyek sem átjáróként, sem bázisállomásként, sem összekötő csomópontként nem funkcionálnak, hanem valami egyéb célt szolgálnak (például csomaghitelességvizsgálat vagy forgalomanalízis).
- kombinált: a fent említett csomópontok tetszőlegesen kombinálhatóak.

### Gyűrűtípusok

Mikromobilitási hálózatunkban egy gyűrűnek vagy bázisállomásai, vagy gyermekgyűrűi vannak, a kettőt egyszerre nem engedjük meg. Ennek oka, hogy így jobban strukturált hálózatot kapunk. Tehát hálózatunk kétféle gyűrűből épül fel: hozzáférési gyűrűből (access ring), melynek bázisállomásai vannak, de gyermekgyűrűi nem, és transzportgyűrűből (transport ring), melynek gyermekgyűrűi vannak, de bázisállomásai nincsenek.

A hozzáférési gyűrűk tulajdonképpen gyűrű topológiára épülő mikromobilitási hálózatok egy kicsit több funkcionalitással. Az összekötő csomópontok, amelyek a hozzáférési gyűrűt a szülőgyűrűjéhez kötik, úgy viselkednek, mintha egy egyszerű gyűrű topológiájú hálózat átjárói lennének. A hozzáférési gyűrűhöz kapcsolódó összes mobilegységről információval rendelkeznek.

A 3. ábrán egy gyűrűhierarchia topológiájú mikromobilitási hálózat látható. Ez a példahálózat három hozzáférési gyűrűből, két transzportgyűrűből és a gyökérgyűrűből áll. A gyökérgyűrűben két átjáró található.



3. ábra Gyűrűhierarchia topológiájú hálózat

Az összes alkalmazott gyűrű öngyógyító gyűrű, tehát gyűrűként egy hiba az IP-szint alatt javítható. Minden gyűrűnek (a gyökérgyűrűt kivéve) van egy szülőgyűrűje, és minden transzportgyűrűnek vannak gyermekgyűrűi. Hogy hálózatunk megbízható legyen, min-

den gyűrűt több összekötő csomópontnak kell a szülőgyűrűjéhez kötnie, és a gyökérgyűrűben több átjárót kell alkalmazni. A többszörös kapcsolatoknak fizikailag is függetleneknek kell lenniük.

### Megbízhatóság

Megbízhatósági vizsgálatokhoz gráfmodellt használunk. A csomópontok a gráf csúcsai, az összeköttetések az élek. A csomópontoknak és az éleknek két állapota van: tökéletesen jó és tökéletesen rossz, és legalább az első meghibásodásig függetlenek, a meghibásodás valószínűsége kicsi. Meg fogjuk mutatni, hogy a gyűrűhierarchia topológia egy meghibásodást teljes mértékben tolerál a fa topológiával szemben. A fent leírt modellben ez jelentősen nagyobb megbízhatóságot jelent.

A modellünkben egy csomópont meghibásodása ekvivalens a csomópontba futó összes összeköttetés meghibásodásával. Tehát a csomópont-meghibásodás „súlyosabb”, mint az összeköttetés-meghibásodás. A következőkben megmutatjuk, hogy a gyűrűhierarchia bármely csomópontjának meghibásodását tolerálja.

Ha egy bázisállomás hibásodik meg, a hozzáférési gyűrű gyógyítja magát, így magasabb szinten észre sem vesszük a hibát. Azoknak a mobilegységeknek a kapcsolata, amelyek éppen a meghibásodott bázisállomáshoz kapcsolódtak, megszakadhat, de a hálózat normálisan működik tovább.

Ha egy összekötő csomópont hibásodik meg, a felső és az alsó gyűrű is gyógyítja magát, a topológia tehát annyiban változik, hogy a két gyűrűt összekötő csomópontok száma eggyel csökken. Így is marad összeköttetés, mert kezdetben minden gyűrűt legalább két összekötő csomópont kötött a szülőgyűrűhöz. Ha egy átjáró hibásodik meg, a gyökérgyűrű gyógyítja magát, és minden működik tovább, csak az átjárók száma csökkent eggyel. Biztosan maradt még működő átjáró, mert kezdetben legalább két átjáró volt a gyökérgyűrűben, lásd gyűrűtípusok.

Tehát a gyűrűhierarchia topológia egy összeköttetés vagy csomópont meghibásodását mindenképpen elviseli. Lehet, hogy egynél több meghibásodás esetén is működik tovább a hálózat. Az összes átjáró együttes meghibásodását például nyilván nem képes elviselni, de ha gyűrűként legfeljebb egy hiba történik, a gyűrűk gyógyítják magukat, és a hálózat működik tovább.

A gyűrűhierarchia topológián alkalmazott mikromobilitási protokollnak természetesen kezelnie kell az esetleges meghibásodások miatt történt topológiaváltozásokat. A felfelé irányú (tehát átjáró felé küldött) csomagokat minden gyűrűből az első összekötő csomópont továbbítja a szülőgyűrűjébe, amíg el nem érkezik a gyökérgyűrűbe. A lefelé irányú (bázisállomás felé küldött) csomagokat mindig az első megfelelő csomópont továbbítja a gyermekgyűrű felé. Megfelelő alatt azt értjük, hogy természetesen csak olyan gyermekgyűrű felé továbbítjuk a csomagot, ahol a címzett elérhető. Ez az útvonalválasztás a routerek adatbázisa alapján történik. A mobilegység időről időre útvonalfrissítő



(route update) üzeneteket küld fel egészen a gyökérig. Ezek az üzenetek az összes érintett gyűrűn teljesen körbemennek, hogy az összes router periodikusan aktualizálni tudja az adatbázisát.

Mivel a topológia csak a meghibásodások alkalmával változik meg és akkor sem nagyon, a fa topológiánál alkalmazott algoritmusok, ötletek közül sok átültethető a gyűrűhierarchia topológiára.

### Forgalomirányítás

Nézzük meg, mi történik a csomagokkal, melyeket a mobilegység elküldött a bázisállomásnak. A bázisállomás továbbítja a csomagot a csomópont routerének. A router pedig útjára indítja a csomagot a gyűrűn. A csomag routertől routerig halad a hozzáférési gyűrűn, amíg egy összekötő csomóponthoz nem érkezik. Az összekötő csomópont felismeri, hogy egy felfelé irányú csomagról van szó, ezért a hozzáférési gyűrűn való továbbítás helyett felfelé továbbítja a csomagot, vagyis a szülőgyűrűn indítja útjára. A routerek így továbbítják a csomagot gyűrűről gyűrűre, amíg el nem érkezik a gyökérgyűrűbe, ahol az első átjáró kifelé továbbítja az IP-gerinchálózat felé.

Az IP – gerinchálózat felől érkező csomagot az átjáróhoz tartozó router bocsátja útjára a gyökérgyűrűn. A csomag addig megy körbe, amíg egy olyan összekötő csomóponthoz nem ér, amelyik megtalálja adatbázisában a címzett mobilegységet. Ez az összekötő csomópont nem a gyökérgyűrűn továbbítja a csomagot, hanem a hozzá tartozó gyermekgyűrűn. A csomag így halad lefelé a transzportgyűrűkön, amíg el nem jut a megfelelő hozzáférési gyűrűbe, ahol is a bázisállomás továbbítja a mobilegységhez.

A csomagok megfelelő továbbítása tehát egyszerű feladat, ha minden összekötő csomópont ismeri az összes mobilegységet, amely az alatta lévő részben kapcsolódik a hozzáférési hálózathoz. Vizsgáljuk meg, hogyan kezelhetők ezek az adatbázisok.

### Regisztráció

Nézzük meg, mi történik, amikor a mobilegység belép a hálózatba vagy bekapcsolják a hálózaton belül. Először regisztrálnia kell magát a hálózat felé. A regisztrációs üzenet a hozzáférési gyűrűtől a gyökérgyűrűig halad felfelé. A hozzáférési gyűrűn, az összes útba eső transzportgyűrűn és a gyökérgyűrűn is teljesen körbemeny, hogy az összekötő csomópontok és az átjárók bejegyezhesék a mobilegységet az adatbázisukba. A regisztrációs üzenetet vagy az összes összekötő csomópont feljebb küldi, vagy csak minden gyűrűből az első. Ha az összes feljebb küldi, a szülőgyűrűben kezelni kell a többszörös regisztrációs üzenetet. Ha csak az első küldi feljebb, akkor valahogy jelölnie kell a csomagon, hogy már fel lett küldve, nehogy egy másik összekötő csomópont is feljebb küldje.

### Cellaváltás (Handover)

Ha a mobilegység egyszerre csak egy bázisállomáshoz tud kapcsolódni, akkor egy Cellular IP-hez [5] hasonló

„hard” cellaváltás alkalmazható. Itt a „soft” cellaváltást mutatjuk be. A cellaváltási kérdésekkel részletesen a [3] foglalkozik.

Amikor a mobilegység megváltoztatja kapcsolódási pontját a hálózathoz, cellaváltásról beszélünk. Az a bázisállomás, amelyet a mobilegység elhagy, a régi bázisállomás, amelyikhez átcsatlakozik, azt új bázisállomásnak hívjuk. Vegyük a két útvonalat: a régi bázisállomástól az átjáróig és az új bázisállomástól az átjáróig. Az utolsó gyűrű, amely mindkét útnak része, az ún. crossover-gyűrű. Tehát a két út a crossover-gyűrűnél válik szét.

A soft cellaváltás sokban hasonlít a regisztrációra. A mobilegység cellaváltás-üzenetet küld az új bázisállomáson keresztül. Ez az üzenet a crossover-gyűrűig halad felfelé. A crossover-gyűrűtől regisztrációs üzenet mehet tovább a gyökérgyűrűbe, hogy a routerek ne töröljék az adatbázisból a mobilegységre vonatkozó információkat. Azok az összekötő csomópontok pedig, amelyek a crossover-gyűrűt ahhoz a gyermek gyűrűhöz kapcsolják, amelyek a régi bázisállomás felé esik, kitörlik a vonatkozó információt az adatbázisukból, így azok a továbbiakban nem továbbítják a mobilegységnek érkező csomagokat lefelé. Esetleg egy üzenet mehet le gyűrűről gyűrűre a régi bázisállomásig, és útközben minden router törölheti a mobilegységre vonatkozó információt, de azok egy idő után maguktól törlődnek amúgy is. A cellaváltás ideje alatt a mobilegység az új és a régi bázisállomáson keresztül is küldhet üzenetet, és szintén mindkét bázisállomástól érkehetnek csomagok.

### Paging

A mobilegységek, amelyek éppen nem adnak vagy vesznek semmilyen adatot, pihenő módba (idle state) válhatnak, hogy az akkumulátort kíméljék. A pihenő állapotban lévő egységeknek a hálózat nem ismeri a pontos helyét, viszont nem kell értesíteni a hálózatot, ha a mobilegység eltávolodik a bázisállomástól. A hálózatot keresési területekre (paging areas) osztjuk, és a mobilegységnek csak akkor kell értesítenie a hálózatot, ha új keresési területre lép. Tehát a hálózat csak arról rendelkezik információval, hogy a pihenő módban lévő mobilegység melyik keresési területen tartózkodik.

A gyűrűhierarchia topológiájú hálózatban magától értetődő, hogy a hozzáférési gyűrűk legyenek a keresési területek. Amikor egy mobilegység pihenő módba kapcsol, egy üzenet megy körbe a hozzáférési gyűrűn, így az összes összekötő csomópont tudni fogja, hogy az egység pihenő módban van.

Mikor egy éppen pihenő módban lévő mobilegységhez érkezik csomag, kereső üzenet (paging message) megy körbe a gyűrűn, és az összes bázisállomás fel szólítja a mobilegységet, hogy kapcsoljon aktív módba.

Ha a mobilegység egy új hozzáférési gyűrűbe lép át, értesítenie kell a hálózatot. Ez a pihenő módú cellaváltás nagyon hasonlít a rendes, aktív módú cellaváltáshoz. A mobilegység egy pihenő módú regisztrációs



üzenetet küld az új bázisállomásnak. Ez az üzenet körbemegy az új hozzáférési gyűrűn, így az összes összekötő csomópont tudja, hogy egy új, pihenő módban lévő mobilegység érkezett a gyűrűbe. A cellaváltás a továbbiakban olyan, mint egy aktív módú cellaváltás, egy cellaváltás üzenet megy a fel a crossover-gyűrűig.

A [3] részletesen ismerteti a pihenő módú cellaváltást.

## Összefoglalás

Cikkünkben egy nagy megbízhatóságú mikromobilitási hálózati megoldást mutattunk be. Topológiai kérdésekre koncentrálna a klasszikus fa struktúra egy alternatíváját mutattuk be. Ez az új topológia, a gyűrűhierarchia a fából származtatható olyan módon, hogy a fa csomópontjait gyűrűkkel helyettesítjük. Bemutattuk, hogy a mikromobilitás különböző helyzetei, problémái hogyan kezelhetők egy gyűrűhierarchia topológiájú hálózatban.

A bemutatott topológia a fától örökölte jó skálázhatóságát és az útvonalválasztás egyszerűségét, azonban sokkal jobb megbízhatósági tulajdonságokkal rendelkezik.

## Köszönetnyilvánítás

Kutatásainkat az OTKA F032268 és az ETIK támogatta.

## Irodalom

1. S. Imre–M. Szalay: "Reliability Considerations of IP Micro Mobility Networks". DRCN 2001, Budapest, 7–10 October, 2001. pp. 72–77.
2. S. Imre–M. Szalay: "Ring Based Reliable IP Micro Mobility Network". ConTEL 2001, Zagreb, Croatia, 13–15 June, 2001. pp. 113–120.

3. M. Szalay–S. Imre: "Handover Support in Ring Based IP Micro Mobility Networks". SoftCOM 2001, Split, Dubrovnik, Croatia, Ancona, Bari, Italy, 9–12 October, 2001.
4. C. Perkins: "IP Mobility Support". IETF RFC 2002, <http://www.ietf.org/rfc/rfc2002.txt>, 1996.
5. A. T. Campbell–J. Gomez–C. Y. Wan–S. Kim–Z. Turanyi–A. Valko: "Cellular IP". Draft-ietf-mobileip-cellularip-00.txt, IETF Internet Draft, 1999.
6. R. Ramjee–T. La Porta–S. Thuel–K. Varadhan–L. Salgarelli: "IP micro-mobility support using HAWAII". Draft-ietf-mobileip-hawaii-01.txt, IETF Internet Draft, 1999.
7. B. Gloss–C. Hauser: "The IP Micro Mobility Approach". EUNICE 2000, September 2000, Eschende. pp. 195–202.
8. IETW Working Group, Context and Micro-mobility Routing (seamoby), <http://www.ietf.org/html.charters/seamoby-charter.html>
9. C. Huitema: "IPv6–The New Internet Protocol". Prentice Hall, 1999.
10. C. E. Perkins: "Mobile IP -Design Principles and Practices". Addison-Wesley, May 1998.

## Rövidítések

|      |                                     |
|------|-------------------------------------|
| BS   | Base Station                        |
| FA   | (Mobile IP) Foreign Agent           |
| HA   | (Mobile IP) Home Agent              |
| IETF | Internet Engineering Task Force     |
| IP   | Internet Protocol                   |
| MN   | Mobile Node                         |
| MSSP | Multiplex Section Shared Protection |
| PA   | Paging Area                         |
| SAP  | Service Access Point                |
| SDH  | Synchronous Digital Hierarchy       |



# Meddig terhelhető egy torony? Esettanulmány: egy magyarországi TV-torony története

FÖLDI ANDRÁS

okleveles mérnök, acélszerkezeti szakmérnök, az MSc Kft. igazgatója

CSEH SÁNDOR

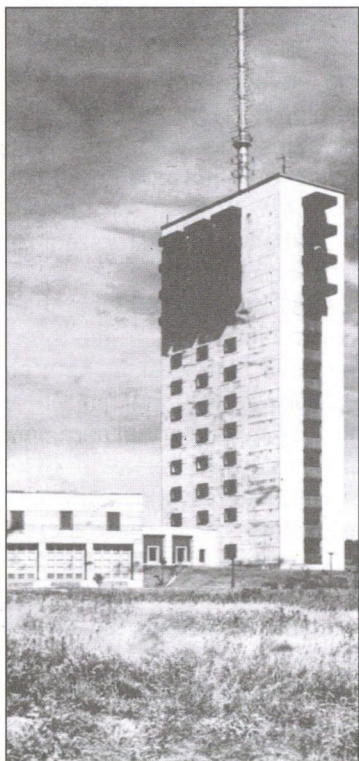
okleveles mérnök, ipari formatervezési szakmérnök, az MSc Kft. szakfőmérnöke

A távközlési infrastruktúra egyik kritikus eleme a torony, mely különböző vezeték nélküli szolgáltatásoknál nélkülözhetetlen. Ezek tervezésével sok tanulmány foglalkozott, karbantartásuk azonban eddig nem került az érdeklődés előterébe. A következőkben egy 40 éves torony története során kiderül a fenntartás fontossága.

A XX. századot szokás az információ, a telekommunikáció századának nevezni. Toronyjellegű szerkezetek már az őskortól épültek, de a hírközlési tornyok jellegzetesen e századhoz, a hírközlés rohamos fejlődéséhez kötődnek.

A hírközlési tornyok iránti igény hozta létre ennek a különleges mérnöki szerkezetnek a tudományát. A hírközlés technológiájának rohamos fejlődése a tornyok számának és típusának növekedését vonta maga után, majd a múlt század 80-as, 90-es éveit követően egyre inkább a meglévő szerkezetekkel való ésszerű „gazdálkodás” került előtérbe. A tornyok száma ma már korlátlanul nem növelhető, ki kell használni a meglévő toronyállomány összes tartalékát. A tervezőknek egyre gyakrabban kell szembenézniük a problémával: vannak-e és mik ezek a tartalékok?

A szerkezetek nagy része már túl van tervezett életkoruk felén, állapotuk a karbantartás függvényében változó. A tornyok az eredetileg tervezett antennákon kívül más méretű, más elrendezésű antennarendszereket hordoznak, sokszor az üzemeltetők sem tudják,



1. ábra 1958 januárjában Budapesten átadott adóépület

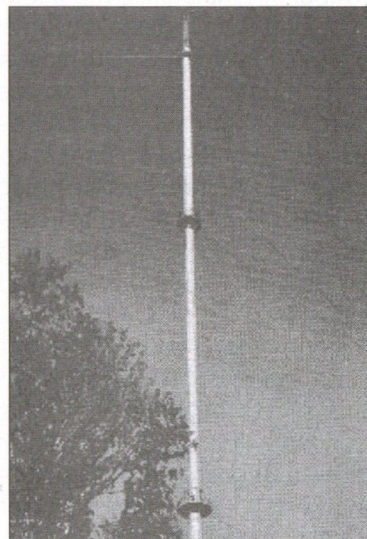
melyik antenna mire szolgál, jellemző a tápkábelek kuszasága. A tervezés óta számos szabvány, előírás megváltozott. Tehát a megválaszolandó kérdés az, hogyan foglalkozunk a régi tornyokkal?

Jelen ismertetésünkben egy magyarországi torony életéről számolunk be. Abban a szerencsés helyzetben vagyunk, hogy szinte a kezdetektől végig tudtunk követni minden eseményt, mely a toronnyal volt kapcsolatos.

## A szentesi TV-torony története és jövője

Magyarországon a televíziózás az ötvenes évek végén kezdődött. Először 1958-ban Budapesten épült egy adóépület<sup>3</sup> (1. ábra), rajta antennarendszerrel, majd ezt követte két, csaknem egyforma kikötött torony, melyek közül az 1960-ban Szentesen épült történetével foglalkozunk. (2. ábra)<sup>4</sup>

A 218 m magas, 1,9 m külső átmérőjű csőkeresztmetszetű toronytörzs 3 szinten, szintenként 3-3 irányban párhuzamos szálú acélkötelekkel volt kikötve. A kikötési szinteken erkélyek voltak a mikrohullámú sugárzók számára, TV-antennák csupán a felső, 20 m-es konzolon voltak.<sup>5</sup> (3. ábra) Ha figyelembe vesszük, hogy azok-

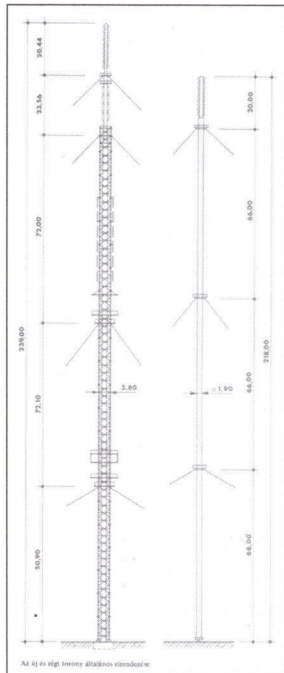


2. ábra Az 1960-ban épült első szentesi TV-torony

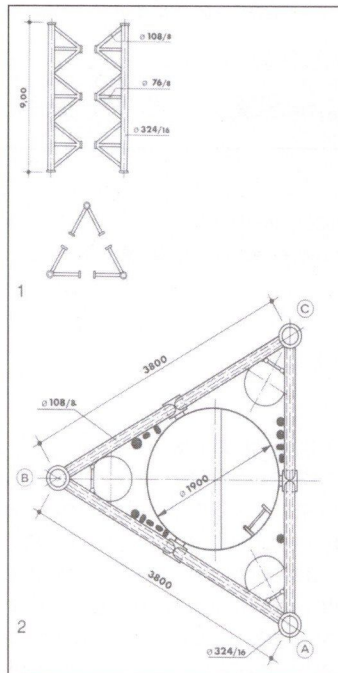


ban az években Magyarország tökéletesen el volt zárva a nyugati technológiák elől, szakirodalom nem volt beszerezhető, csak óriási elismeréssel adózhatunk az akkori tervezőknek, **dr. Petúr Alajosnak és Reiner Endrének**.

A televíziózás és a távközlés rohamos fejlődése rövid időn belül nyilvánvalóvá tette, hogy a torony a megnövekedett igényeknek már nem felel meg. A műsorsu-



3. ábra Szentesi régi és új torony



4. ábra A szentesi régi torony körbeépítése

gárzó vállalat ezért tervbe vette a torony lerobbantását és a közelben új, vasbeton torony építését. Mindez a 70-es évek elején történt, érthető, hogy a tervezők nem fogadták kitörő örömmel a viszonylag új szerkezet elpusztítását. Így hát – ezért mérnökök – kidolgozták a torony megmentésének, megerősítésének és további használatának módját oly módon, hogy az átépítés alatt is zavartalan legyen a sugárzás.

A régi csőtoronyt 3 övű rácsos tartóval vették körül, mely átvette a toronytörzs szerepét, és a régi csőszerkezet már csak a felvonó és a tápvonalak elhelyezésére szolgált. (3-4. ábra) A körbeépítés 6 m-es szakaszokban történt: amikor elértek egy kikötési pontot, elkészítették az új kikötést, majd a régit elbontották. Az „új” torony 240 m magas, ugyancsak 3 szinten, de már pászmaspirális kötelekkel merevített szerkezet.

A toronytörzs a 197 m-es magasságig 3,8 m oldalhosszúságú, csőszelvényű rudakból álló, háromövű rácsos szerkezet, (4. ábra) e fölött 1,4 m átmérőjű csőszerkezet, felette 80 cm oldalhosszúságú, négyszög keresztmetszetű árboc volt. A szerkezeti kialakítás lehetővé tette nagyszámú mikrohullámú antenna elhelyezését, valamint URH, TV III. és TV IV. sávú antennarendszerek telepítését. (5. ábra) A szerkezet **1974**-ben készült el.<sup>6</sup>

A torony életébe az első jelentős beavatkozás **1978**-ban volt, amikor a legfelső, a TV IV. sávú antennáit tartó, négyszög keresztmetszetű toronyszakaszt kicserélték Rhode-Schwartz típusú, hengeres időjárás-védelemmel ellátott antennarendszerre. Ez alapvetően nem befolyásolta a szerkezet erőjátékát, de beépítettek egy további, ún. „lengésgátló” kikötést, mely az R&S antenna-rendszer talppontját merevítette.

A 90-es évek elejéig lényeges antennatelepítések nem történtek. Ezt követően felgyorsultak az események, ami a tornyon lévő antennák rohamos gyarodásában mutatkozott meg. Ebben nyilván közrejátszott az akkori technológiaváltás, és nem utolsósorban a magyarországi rendszerváltás utáni privatizációs hullám.

**1991**-ben és **1993**-ban jelentős mennyiségű mikrohullámú antenna került a toronyra, majd **1994**-ben a TV III. sávú antennákat Kathrein típusúakra cserélték. Ezeknek az antennáknak, antennarendszereknek a mérete és száma még nem haladta meg a tervezettet, ezért külön vizsgálatok nem készültek.

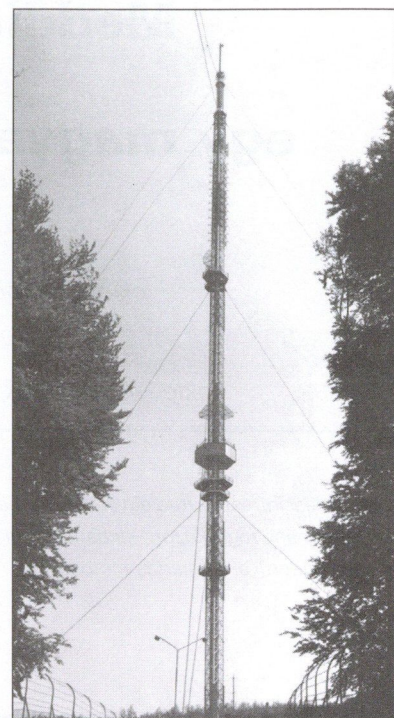
**1995**-ben az egész országra kiterjedő mikrohullámú hálózat (Országos Transzport Hálózat – OTH) kiépítésének keretében több, nagy átmérőjű antennát kellett a toronyra telepíteni. Ez alkalommal már készült statikai vizsgálat, mely az alábbiakat állapította meg:

- a torony acélszerkezete a **teherbírési határ**hoz érkezett,
- a **kihorgonyzó tömböket** meg kell **erősíteni**, valamint
- a kötélbekötő szerelvényeknél **lokális teherbírasi túllépés** észlelhető, de – mérlegelve a kötélcsera kockázat – a túllépést még elviselhetőnek ítéltük.

A számítást követően elkészült a kihorgonyzó tömbök megerősítésének terve (1995).

**1996**-ban újabb igény jelentkezett. A torony 180 és 198 m-es szintjei közé

100 MHz-es antennarendszert kellett telepíteni. Az ehhez készült szakvélemény megerősítette az 1995-ben készültet, ahhoz képest számottevő túllépés nem jelentkezett. Mivel a 100 MHz-es antennarendszer te-



5. ábra Szentesi „új” torony



lepítése sürgős volt, és a kihorgonyzások megerősítése még nem készült el, vizsgálni kellett, hogy a **kihorgonyzás megerősítése nélkül** is elhelyezhető-e ez az antennarendszer. Mivel a megerősítést igénylő OTH-mikroantennák telepítése még nem történt meg, az antennarendszer felszerelhető volt.

**1997**-ben elkészült a kihorgonyzó tömbök megerősítése, majd ezt követően megtörtént a mikrohullámú antennák telepítése is.

**1999** tavaszán újabb antennatelepítéshez készült számítás megint csak kimutatta a szerkezet továbbterhelhetőségének a határát.

**1999** novemberében az OTH bővítésének keretében további nagy átmérőjű antennák telepítésére kellett lehetőséget találni. Mivel 1999 elején jelzések érkeztek a torony „rendellenes” viselkedésére utaló jelenségekről, ezért a szakvélemény elkészítése előtt ezeket is megvizsgáltuk.

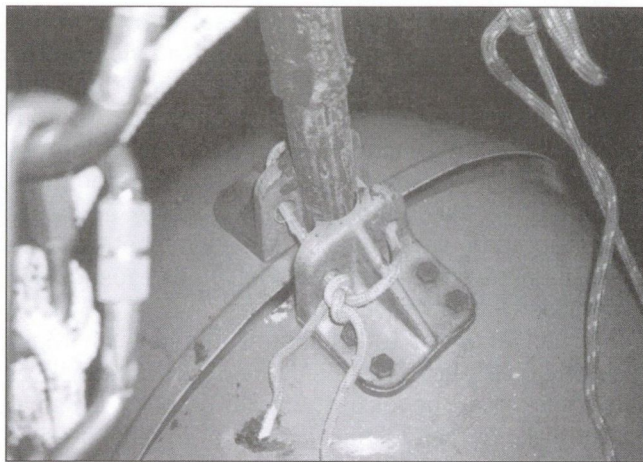
1998–99-ben az állomás dolgozói ritmikus hangokat hallottak a kötéltetről és állítólagos lengéseket is megfigyeltek. Erről 1999 januárjában értesített bennünket az üzemeltető, jelezve, hogy ez a jelenség a 100 MHz-es antennarendszer felszerelése óta jelentkezett. A helyszínen dolgozók tájékoztatása alapján hangjelenségek már régebben is voltak, de kötéllengést nem figyeltek meg. Többszöri helyszíni szemlén mi sem tapasztaltunk rendellenességeket, viszont szemmel látható volt a kötelek különböző mértékű belógása, gyaníthatóan a kötelek különböző mértékben kilazultak.

Javaslatot tettünk a szerkezet alapos átvizsgálására, különös tekintettel az alábbiakra:

- meg kell határozni a kötélfeszültségeket vagy kötél-erőt,
- fel kell mérni a torony alakját,
- végig kell vizsgálni a gyanúsak vélt köteleket teljes hosszukon,
- meg kell vizsgálni a kötélbekötő szerelvényeket, különös tekintettel a varratokra.

A torony üzemeltetője **2000** elején döntött a javasolt vizsgálatok ügyében, ugyanakkor 1999 novemberében – a korábban említett OTH bővítése miatt – el kellett végezni a statikai vizsgálatot. A számítást – mivel a valós állapotra vonatkozó mérések még nem álltak rendelkezésre – továbbra is a tervezett állapotra készítettük el. Eszerint a torony alsó részén (9,0–18,0 m között) a sarokszlopokat meg kellett erősíteni, a torony többi részére a korábbi szakvélemények voltak a mértékadók. Mindez azzal a kockázattal járt, hogy a kötelek lazasága vagy esetleges befeszülése miatt a torony más részei is kritikus állapotba kerülhettek (ez a későbbiek során be is bizonyosodott). Az erősítést és az antennák telepítését a 2000. év elején elvégezték.

Végül **2000** tavaszán került sor a torony javasolt átvizsgálására. Először a kötelek és a varratok szemrevételezése történt meg alpinisták segítségével. A kötelek átvizsgálása rögtön eredménnyel járt. A legfelső kötelekre pirosra festett gömbök lettek felerősítve légaka-



6. ábra A légakadályjelző gömb „felerősítése”

dály jelzése céljából (6. ábra). Közelről szemlélve a gömböket láthatóvá vált, hogy azok csak kötélrészletek lettek felerősítve, ezek tették lehetővé a gömbök mozgását, zörgését, és ez okozta a „furcsa hangot”. A csavarkapcsolatok elkészülte után „gyanús” zöreje már nem volt. A köteleken semmilyen károsodásra utaló nyomot nem találtak, ugyanez mondható el a varratokról is. Elkészült a torony geodéziai mérése is. Ennek során megmérték a torony függőlegestől való eltérését, valamint valamennyi kötélt alakját. Ezt felrajzolva és előzetesen értékelve látható volt a tervezett állapottól való eltérés, a kötelek helyenkénti befeszülése, helyenkénti – különböző mértékű – lazulása.

Úgy döntöttünk, hogy a különféle erőmérő technológiák alkalmazása helyett a kötéltben lévő kötélrészleteket a jól bevált, a kötéltől leválasztott számítással határozzuk meg.

Végül a vizsgálat az alábbi főbb megállapításokat eredményezte.

- A toronytengely függőlegestől való eltérése nem lépi túl a nemzetközi irodalomban található határértékeket, kivéve a felső toronyszakaszt (R&S henger)<sup>7</sup>, melynek viszonylag nagy ferdesége valószínűleg szerelési hiba.
- Az alsó kötelekben a feszültségek a tervezett **felett** vannak, míg a többi kötélt jelentősen **kilazult**. A legfelső, úgynevezett „lengésgátló” kikötés különösen lazának mutatkozott.
- A vizsgálat során meghatározott kötélrészletek mellett a toronytörzs alsó 42 m-es szakaszát is meg kellene erősíteni, ezt nem javasoltuk.
- Javasoltuk a kötelek besabályozását azzal az engedménnyel, hogy – mivel a legfelső kötéltnek alapjában véve statikai szerepe nincs – annak teljes megfeszítése nem követelmény (a feszítő szerelvény sem engedi).

Fontosnak tartjuk külön hangsúlyozni, és ezt az üzemeltetővel nyomatékosan közöltük, hogy ezekkel a be-

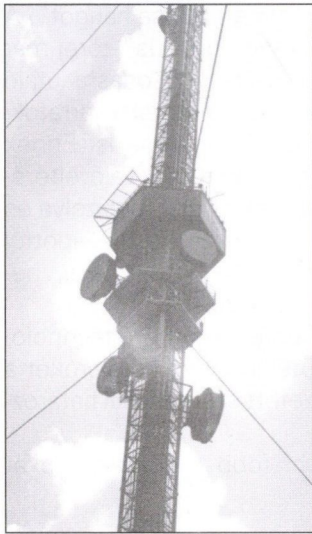


avatkodásokkal **a torony teherbírása nem fog növekedni, csupán a terv szerinti állapot fog visszaállni!**

A beszállítás a **2000.** év őszén megtörtént, magát a műveletet a későbbiekben ismertetjük. A torony ezáltal a tervezett állapotba került, a kötélerők, a torony függőlegessége a megengedhető hibahatáron belül vannak. Ugyanakkor a torony szerkezetének egy része határállapotban van, tovább nem terhelhető, illetve minden egyes antennatelepítésnél, áthelyezésnél, sőt, eltávolításnál is vizsgálat szükséges.

Hogyan lehetne a teherbírást ezután növelni? Maga a toronytörzs nem erősíthető. Felül, az antennák és tápvonalak miatt hegesztett erősítő bordák nem alkalmazhatóak. A másik kritikus pont a kötélbekötés viszonylagos gyengesége, mely egy kötélcserével megoldható lenne.

Az egyetlen ésszerű megoldás a szélnek kitett felület csökkentése, melyet a tápvonalakban, antennákban történő rendcsinálással, a felesleges védőkosaras lét-



7. ábra Szentes TV-torony  
Antenna-elrendezés  
1998. augusztus



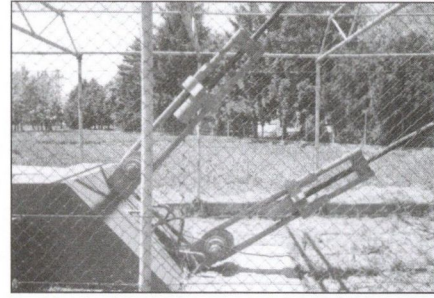
8. ábra Szentes TV-torony  
Antenna-elrendezés  
2000. november

rak leszerelésével el lehetne érni. Mivel mindez tetemes ráfordítással járna, az üzemeltető egyelőre ettől a megoldástól elzárkózik. Feltételezhetően más lesz az álláspont, amikor a terhelések miatti túllépéseket a tervező már nem tudja felelősséggel vállalni, és további antennák elhelyezéséhez nem járul hozzá.

## A szentesi TV-torony köteleinek beszállítása 2000-ben

Az alábbiakban röviden beszámolunk a kötelek beszállításának menetéről.

A képeken látható (9.–10. ábrák) a lehorgonyzó szerelvények kialakítása. A négy kötéllehorgonyzás közül három azonos kialakítású, míg a negyedik, az ún. „lengésgátló” más. Ez utóbbinál a feszítés különös műszaki problémát nem jelent, az az orsó csavarásával törté-



9. ábra Alsó két lehorgonyzó kötel feszítő  
szerelvénye



10. ábra Felső két lehorgonyzó kötel feszítő  
szerelvénye

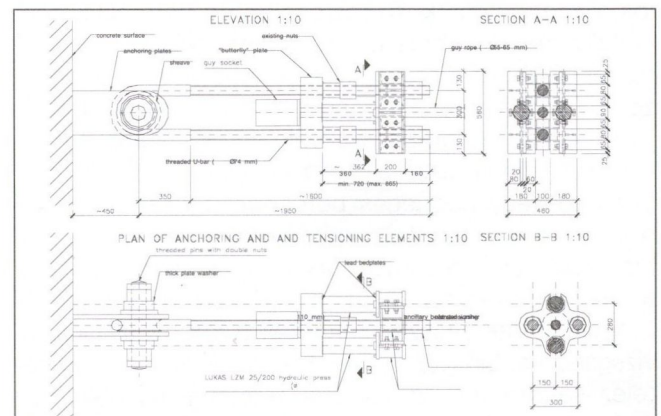
részletebben foglalkozni. A torony tervezői – akár tudatosan, akár tudattalanul – olyan szerkezetet terveztek, mely viszonylag egyszerűen lehetőséget tett az utólagos feszítés végrehajtására. A

képeken látható, hogy a kötélfej egy kovácsoltvas elemre támaszkodik, mely elem két nagyméretű csavaranyával van a menetes orsóhoz erősítve, és ezáltal adja át a lehorgonyzó erőt. Az is látható, hogy a lehorgonyzó elem felett még hosszú menetorsó van szabadon, és ez adta a viszonylag egyszerű megoldást.

Egy olyan, két elemből álló tartószerkezetet tervezünk, mely a kötelet közrefogja.

A szerkezet és a lehorgonyzó elem közé két hidraulikus sajtó (maximális erő 500 kN) kerül, és a szerkezet az orsóra felcsavart anyákra támaszkodik. A sajtó működtetésével a lehorgonyzó elem a kihorgonyzó tömb felé elmozdul, a kötel megfeszül, és a csavaranyák utánhúzásával rögzítve, lépésről lépésre a beszállítás megtörténhet. (11. ábra)

A beszállítás egyszerre egy szint feszítésével történt (3x2 db sajtó – 12. ábra) miközben mind a kötel-



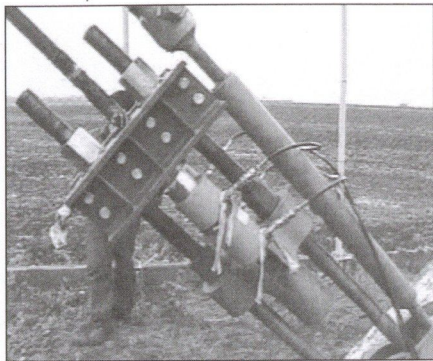
11. ábra Feszítőszerelvény elrendezése

nik, melynek határt a szerkezet hossza szab.

A beszállítás nehézségét itt a nehéz hozzáférés és a berendezésodott menet okozta.

A többi kötel beszállításával érdemes





12. ábra A feszítés végrehajtása

belógásokat, mind pedig a torony függőlegességét geodéziai úton mérték. Mivel az alsó kötelek az előzetes mérések szerint túl voltak feszítve, először úgy gondoltuk, hogy nem nyúlunk hozzá, a besza-

bályozást a második szintnél kezdtük. Az első lépésben azonos mértékűre hoztuk a kötélérőket, majd a három feszítési hely sajtóinak szinkron működtetésével a köteleket a terv szerinti állapotba hoztuk. Ugyanezt a műveletet elvégeztük a 3. szint köteleivel is, amikor a mérési eredmények alapján úgy döntöttünk, hogy a legalsó szint köteleit visszaengedjük a tervezett mértékre. Ezután még egyszer megismételtük a 2. és 3. szint köteleinek szabályozását. A toronyalak függőlegestől való eltérése és a kötélérők tervezettől való eltérése már a megengedett határon belül volt, a szabályozást befejeztük.

Igen fontosnak tartottuk a besabályozott állapot pontos rögzítését és dokumentálását, mivel a további számítások már ennek alapján történnek. Rendkívül sajnálatos, hogy az építéskor ezeket az adatokat nem őrizték meg, így ma már nem állapítható meg, hogy pl. az alsó szintek túlfeszítettsége, a felsők lazasága mennyiben építési hiba és mennyiben a használat következménye.

## Összefoglalás

Magyarországon két, a szentesi toronnyal megegyező kialakítású és korú torony található, melyeknél hasonló jelenségek várhatók. Ezek közül az egyik a Budapest Széchenyi-hegyi torony, melynek ez év szeptemberé-

ben lezajlott geodéziai mérése igazolta ezt a feltevést. Ennél a toronynál is szükséges a mielőbbi besabályozás, mivel a szerkezet egyes részeinek túlterhelése számottevő.

Feltehetően hasonló eredménnyel járna az országban lévő kikötött rádió- és TV-tornyok vizsgálata. Önmagában a kötélérők meghatározása még nem elegendő.

A teljes körű állapotfelméréshez hozzátartozik a szerkezet korróziós helyzetének felmérése, különös tekintettel a kötelekre – mint a szerkezet legérzékenyebb részére – valamint a kötélbekötések varrataira, kötőelemekre. Nem kétséges, hogy mindezen vizsgálatok és a szükséges besabályozások tetemes költségekkel járnak, de az ésszerű „toronygazdálkodás” során ezek a ráfordítások megtérülnek. Különösen megtérülnek akkor, ha új torony építése helyett, annál jóval olcsóbban rendet lehet teremteni a toronyon lévő antennák és tápvonalak között. A szélnek kitett felület csökkentésével újabb antennák elhelyezésére nyílnak lehetőségek.

Mi, tervezők, mivel egyéb eszközünk nincs, nem tehetünk mást, mint hogy az üzemeltetők figyelmét rendszeresen felhívjuk erre a lehetőségre, illetve a folyamatos karbantartás, ellenőrzés szükségességére.

## Irodalom

1. Az IASS Working Group No. 4 for Masts and Towers 2001. szept. 10–13. között tartott ülésén elhangzott előadás szerkesztett változata.
2. MSc Magyar Scetauroute Mérnöki Tervező és Tanácsadó Kft. 1143 Budapest, Hungária krt. 113.
3. Postaépítészeti Magyarországon. Budapest, 1992, Távközlési Könyvkiadó. 88. oldal.
4. Reiner Endre: A szentesi TV-torony átépítése. UVATERV Műszaki Közlemények, 76/1.
5. Dr. Petúr Alajos: 218 m magas csőtorony televízió részére. Mélyépítéstudományi Szemle XI. évfolyam. (1961) 7. szám.
6. Reiner Endre: A szentesi TV torony átépítése. UVATERV Műszaki Közlemények, 76/1.
7. ENV 1993-3-1. Eurocode 3: Design of steel structures – Part 3-1: Towers, masts and chimneys



# Hír

## Veszélyes kalandok a távközlésben

A neves szakmai folyóiratok szerkesztői vezércikkeikben ismételten figyelmeztetnek arra, hogy a műszaki fejlesztésnek gyakran nagy hűhóval beharangozott eredményei egyre gyakrabban vallanak kudarcot, vagy legalábbis nem váltják be a hozzájuk fűzött reményeket. Emellett az eddigi műszaki és gazdasági fejlődés bővületében olyan üzleti fogásokhoz folyamodnak a szolgáltatók, amelyek ügyes alkalmazása konjunktúrában általában sikeres, de a világgazdasági válság körülményei között a szakmai közvélemény által szilárdnak hitt gazdasági alapok inognak meg. Két ilyen időszerű eset szolgálat tanulságot.

## GPRS

A nagy hűhóban a GPRS-t úgy tüntették fel, mint ami félúton van a GSM-től a – minden gond megoldásának látszó – 3G technika felé („2.5G technika”). Kiemelték, hogy csekély beruházással már nagyot lehet lépni a nem túl olcsó 3G irányában, éppen a GSM-ből hiányzó olyan szolgáltatásokkal, amelyekre a nagyvállalatoknak van szükségük. Most, a piacravitel időszakában meglepően kevés érdeklődés mutatkozik a GPRS iránt. Előtérbe kerül a felhasználók szemlélete, akiket nem az út szélén álló kilométerkövek érdekelnek, hanem az, hogy mekkora ráfordításért mit kapnak. Áttekintve a kínálatot, gondos számolással rájönnek, hogy a 2,5G-vel kapcsolatos költségeiket (kezdeti beruházás + a szolgáltatás folyamatosan fizetendő díja) aligha tudják megkeresni a 2G szolgáltatásainak kihasználásával. E szolgáltatások egyelőre csak a WAP-ot és az állandó internetkapcsolatot jelentik. Ehhez járul, hogy a technika ugyan megengedi max. 8 csatorna összefogásával a sáv szélesség jelentős bővülését, de a GSM számára rendelkezésre álló frekvenciasáv egyre telítettebb. Erre való tekintettel kevés szolgáltató vállalja végkészülékenként több mint egy csatorna átvitelét. Ezen a tömörítés sem segít eleget.

Kiábrándító a díjszabás is. Európában legdrágább az osztrák Max Mobile Start Max csomag havi 9 \$-ért, de az adatátvitel Mbájonként 46 \$-ba kerül. Ez például azt jelenti, hogy egy üzleti használatnak 4600 \$-t kell költenie csupán arra, hogy villámleveleit és mellékleteit letöltse laptopjára. Ez tetemesen meghaladja azt az összeget, amit GSM-modem használatkor, időmérésen alapuló díjszabás esetén fizetnie kell. A Vodafone előfizetése havi 26 \$-ba kerül, a forgalmi díj pedig 5 \$ Mbájonként. Az Egyesült Királyságban egy foglalkozásszerűen úton tartózkodó munkatárs (kereskedelmi utazó, szerviz dolgozója stb.) havonta 500 \$-ért csak az üzleti villámleveleihez jut hozzá.

Végül tehát az a következtetés adódik, hogy a szolgáltatóknak óvatosaknak kell lenniük, amikor a potenciális használatok számát felbecsülik.

## Deutsche Telekom

Nem kellemes az, ha egy céget olyan övön aluli ütés ér, mint amikor a Deutsche Bank előzetes tájékoztatás nélkül eladta a Deutsche Telekom részvényeinek 44%-át. Különösen, ha mindez azután történik, hogy a várható versenytársakat eleve kizáró, a DT a 3G frekvenciák licencéért csillagászati összeget fizetett, majd kiderült, hogy az előzetesen terjesztett hírekkel ellentétben csak 2-3 év múlva indíthatja a 3G működését.

A DT piaci megítélése megrendült: részvényeinek árfolyama a tőzsdén egy hét alatt 20%-kal esett, és több cég jelezte, hogy DT részvényeitől meg akar válni. Az idei közgyűlésen a részvényesek szigorú bírálatban részesítették az igazgatóságot, melynek elnöke most foggal-körömmel igyekszik lebeszélni azokat, akik ki akarnak válni a részvényesek közül. Ennek egyik része az, hogy hat banknak följánlotta, hogy számukra további törzsrészvényekre biztosít elsőbbségi jogot. További lépésként a DT meg kíván válni nem alaptévékenységeitől, és tőzsdére kívánja vinni a T-Mobilt (saját mobil leányvállalatát).

Úgy látszik, hogy a konjunktúra utolsó évében túl nagyra nőtt buborékok azért fenyegetnek kipattanással, mert nagyvállalatok különben józan vezetőit kalandokba sodorták.

*Horváth Gyula*



# Börsztmódusú, szintetikus apertúrájú radar (SAR) jelek feldolgozása momentán Fourier-transzformáció alkalmazásával

ALBRECHT SÁNDOR

Ericsson Magyarország  
Kutatás-fejlesztés

L

A jel- és képfeldolgozás általános technikája, hogy a jelfolyam egy részletét ablakozási technikával kinyerjük, majd végrehajtunk egy DFT-t az ablak tartalmán. A momentán Fourier-transzformáció (MFT) arra az egyedi esetre vonatkozik, amikor az ablak mintánként lép előre a jelfolyam mentén két egymást követő transzformáció között. Ebben a cikkben az általános mátrixtranszformációkból kiindulva az eddigiektől eltérő levezetést adjuk az MFT rekurzív formulájának. A börsztmódusú adat és a rövid IFFT (SIFFT) algoritmus részletes leírása után bemutatjuk, hogy a DFT-eket és IDFT-eket hogyan használják a SIFFT SAR jelfeldolgozó algoritmusban. Ebben az algoritmusban alkalmazzuk az MFT-t, illetve az inverz MFT-t (IMFT), és megmutatjuk, hogy milyen előnyökkel jár ezek alkalmazása az FFT- és IFFT-algoritmus alkalmazásával szemben.

## Bevezetés

A diszkrét Fourier-transzformáció (DFT) a jel- és képfeldolgozás széles körben használt eszköze, hatékonysága nagy jelentőséggel bír. Vannak olyan alkalmazások, ahol ajánlatos relatíven kicsi, egymást követő, átlapoló DFT-eket használni a spektrumkomponensek kiszámítására. A momentán Fourier-transzformáció (MFT) hatékony, rekurzív formában számolja ki egy diszkrét időfüggvény DTF-jét minden egyes új mintára. Az inverz MFT rekurzív és nem rekurzív formáival hatékony frekvenciamanipuláció (pl. szűrés) végezhető el. Ezeket követi az MFT és az IMFT hatékonysági vizsgálata. Az inkrementális DFT használatát Papoulis 1977-ben [1], Bitmead és Anderson 1981-ben [5] mutatták be. A momentán Fourier-transzformáció (MFT) részletes levezetését Dudás adta 1986-ban [6]. 1991-ben Lilly mutatott be egy hasonló levezetést, bevezetve a „mozgó Fourier-transzformáció” kifejezést, ahol az MFT-t egy időben változó rendszer modelljének a frissítésénél használta [7].

A szintetikus apertúrájú radar (SAR) a távérzékelés hatékony szenzora, amely képes a Föld vagy más bolygó geofizikai paramétereinek megfigyelésére függetlenül az időjárástól és napszakoktól [3, 10]. A SAR-rendszereket széles körben használják óceánfelszín, jégtakaró, mezőgazdasági termőterületek monitorozására, valamint katonai célokra, például mozgó céltárgyak követésére és azonosítására. A SAR radarjeleket bocsát ki egy repülőgépre vagy űreszközre (pl. műhold, űrsikló) szerelt, egyenletes sebességgel haladó, a haladási irányra (azimutirányra) merőleges antennából. Ugyanez az antenna fogja fel a visszavert jelet, amely „nyers” formában kerül tárolásra. Ezek után extenzív jelfeldolgozásra van szükség a kívánt radarkép előállítására.

Amikor egy SAR-rendszer börsztmódban működik, akkor az azimutirányban vett jel időtől függő spektru-

ma szegmentált a Doppler-(azimut) lenyomatban. A spektrum ezen tulajdonsága szükségessé teszi, hogy az inverz DFT-eket a frekvenciatartomány meghatározott helyein végezzük el azimut-jelfeldolgozás közben. Először részletes leírást adunk a börsztmódusú jelek tulajdonságairól, majd megmutatjuk, hogy a rövid IFFT (short IFFT – SIFFT) algoritmusnak miért van szüksége tetszőleges hosszúságú, nagyon átlapoló IDFT-kre a börsztmódusú jelek feldolgozásához, mely esetben az IMFT számítási előnyei jól kihasználhatók.

## A momentán mátrixtranszformáció

### A rekurzív momentán mátrixtranszformáció

Legyen  $x_i$  egy tetszőleges, komplex egyváltozós diszkrét függvény egy eleme. Vizsgáljuk a függvényt az  $N$  minta hosszú ablakon keresztül, amely az  $i$ -edik mintában végződik. Az analízis során lépjen az ablak előre egyszerre egy mintányit. Az  $i$ -edik mintához tartozó ablakba lép az  $x_i$  minta, míg az  $x_{i-N}$  elhagyja az ablakot. Az  $i-1$  és  $i$ -edik mintákban az ablakozott függvényt a következő két oszlopvektor reprezentálja:

$$\mathbf{x}_{i-1} = \begin{bmatrix} x_{i-N} \\ \vdots \\ \cdot \\ \vdots \\ x_{i-1} \end{bmatrix}, \quad \mathbf{x}_i = \begin{bmatrix} x_{i-(N-1)} \\ \vdots \\ \cdot \\ x_{i-1} \\ x_i \end{bmatrix} \quad (1)$$

Legyen  $\mathbf{T}$  egy  $N \times N$ -es mátrixtranszformáció, mely egy lineáris transzformációt reprezentál, és amelynek



létezik az inverze,  $\mathbf{T}^{-1}$ . Transzformáljuk az oszlopvektorokat minden egyes mintánál  $\mathbf{T}$ -vel:

$$\dots, \mathbf{y}_{i-1} = \mathbf{T}\mathbf{x}_{i-1}, \mathbf{y}_i = \mathbf{T}\mathbf{x}_i, \dots \quad (2)$$

Legyen  $\mathbf{P}$  az  $N \times N$ -es elemi ciklikus permutációmátrix:

$$\mathbf{P} = \begin{bmatrix} 0 & 1 & . & . & 0 \\ . & 0 & 1 & . & 0 \\ . & . & 0 & 1 & . \\ . & . & . & 0 & 1 \\ 1 & 0 & . & . & 0 \end{bmatrix} \quad (3)$$

$\mathbf{P}$  mátrixszal balról megszorozva az  $\mathbf{x}_{i-1}$  vektort, a vektor elemeinek indexe eggyel nő, és az első elemből utolsó lesz:

$$\mathbf{P}\mathbf{x}_{i-1} = \begin{bmatrix} x_{i-(N-1)} \\ . \\ . \\ x_{i-1} \\ x_{i-N} \end{bmatrix} \quad (4)$$

Az  $\mathbf{x}_i$  vektort kifejezhetjük az eltolt  $\mathbf{x}_{i-1}$  vektorral (4) és a  $\Delta\mathbf{x}_i$  különbségvektorral, amelynek utolsó eleme az ablakba belépő és kilépő minta különbségével egyenlő (a többi eleme nulla):

$$\mathbf{x}_i = \begin{bmatrix} x_{i-(N-1)} \\ . \\ . \\ x_{i-1} \\ x_{i-N} \end{bmatrix} + \begin{bmatrix} 0 \\ . \\ . \\ 0 \\ x_i - x_{i-N} \end{bmatrix} = \mathbf{P}\mathbf{x}_{i-1} + \Delta\mathbf{x}_i \quad (5)$$

Az (5) egyenletbe helyettesítve az  $i$ -edik ablakhoz tartozó transzformációba (2) és kihasználva, hogy  $\mathbf{x}_{i-1} = \mathbf{T}^{-1}\mathbf{y}_{i-1}$ , a következő adódik:

$$\dots, \mathbf{y}_{i-1} = \mathbf{T}\mathbf{x}_{i-1}, \mathbf{y}_i = \mathbf{T}\mathbf{x}_i, \dots \quad (6)$$

A (6) egyenlet fejezi ki a pillanatnyi (momentán) mátrixtranszformációk (MMT) rekurzivitását, mivel az újonnan transzformált indexvektor,  $\mathbf{y}_i$  kiszámolásához nem szükséges más, mint az előzőleg transzformált  $\mathbf{y}_{i-1}$  és az ablakba be- és kilépő minták különbsége.

### Az MMT diagonálformája

A momentán mátrixtranszformáció akkor különösen hatékony és  $\mathbf{y}$  elemeit csak akkor lehet komponensenként számolni, ha a  $\mathbf{TPT}^{-1}$  hasonlósági mátrixtranszformáció a (6) számú egyenletben diagonál. A  $\mathbf{P}$  mátrixnak  $N$  eltérő sajátértéke van ( $\lambda_0, \dots, \lambda_{N-1}$ ) melyek nem mások, mint az  $n$ -edik komplex egységgyökök:  $\lambda_k = w^k = e^{j2\pi k/N}$ ,  $k=0,1,2,\dots,N-1$ .  $N$  lineárisan független sajátvektor létezik az  $N$  sajátértékhez:

$$\begin{aligned} \lambda_0 = w^0 = 1 \Leftrightarrow \mathbf{s}_0 &= \begin{bmatrix} 1 \\ 1 \\ . \\ . \\ 1 \end{bmatrix}; \lambda_1 = w^{-1} \Leftrightarrow \mathbf{s}_1 = \begin{bmatrix} 1 \\ w^{-1} \\ w^{-2} \\ . \\ w^{-(N-1)} \end{bmatrix}; \dots \\ \lambda_0 = w^0 = 1 \Leftrightarrow \mathbf{s}_0 &= \begin{bmatrix} 1 \\ 1 \\ . \\ . \\ 1 \end{bmatrix}; \lambda_1 = w^{-1} \Leftrightarrow \mathbf{s}_1 = \begin{bmatrix} 1 \\ w^{-1} \\ w^{-2} \\ . \\ w^{-(N-1)} \end{bmatrix}; \dots \\ \lambda_0 = w^0 = 1 \Leftrightarrow \mathbf{s}_0 &= \begin{bmatrix} 1 \\ 1 \\ . \\ . \\ 1 \end{bmatrix}; \lambda_1 = w^{-1} \Leftrightarrow \mathbf{s}_1 = \begin{bmatrix} 1 \\ w^{-1} \\ w^{-2} \\ . \\ w^{-(N-1)} \end{bmatrix}; \dots \end{aligned} \quad (7)$$

Ha a  $\mathbf{T}$  mátrix inverzének oszlopai a sajátvektorok ( $\mathbf{s}_i$ ), akkor a  $\mathbf{TPT}^{-1}$  szorzat egy diagonálmátrixot eredményez  $\mathbf{P}$  sajátértékeivel a diagonál mentén:

$$\begin{aligned} \mathbf{TPT}^{-1} &= \mathbf{S}^{-1}\mathbf{P}\mathbf{S} = [\mathbf{s}_0^{-1} \mathbf{s}_1^{-1} \dots \mathbf{s}_{N-1}^{-1}] \mathbf{P} [\mathbf{s}_0 \mathbf{s}_1 \dots \mathbf{s}_{N-1}] = \\ &= \begin{bmatrix} \lambda_0 & 0 & . & . & 0 \\ 0 & \lambda_1 & 0 & . & 0 \\ . & . & \lambda_2 & 0 & . \\ . & . & . & . & 0 \\ 0 & 0 & . & . & \lambda_{N-1} \end{bmatrix} \end{aligned} \quad (8)$$

ahol  $\mathbf{S}$  a  $\mathbf{P}$  sajátvektor mátrixa (spektruma), amely a (7) egyenletben szereplő oszlopvektorokból keletkezett.



Az  $\mathbf{S}$  diagonalizáló mátrix nem egyedi. Az  $\mathbf{s}_k$  sajátvektort megszorozhatjuk egy állandóval, és sajátvektor marad [2]. Tehát az  $\mathbf{S}$  oszlopai megszorozva bármely nem nulla konstanssal egy új diagonalizáló mátrixot eredményeznek. Valamint, az  $\mathbf{S}$  mátrix oszlopainak (sajátvektoroknak) nincs preferált sorrendje [2]. A sajátvektorok sorrendje az  $\mathbf{S}$ -ben és a sajátértékek a diagonálmátrixban automatikusan azonosak. Tehát az összes olyan  $\mathbf{T}$  mátrix, amely rendelkezik a fent említett tulajdonságokkal, diagonalizálni fogja a momentán mátrixtranszformációt:

$$\mathbf{y}_i = \begin{bmatrix} \lambda_k & 0 & \dots & 0 \\ 0 & \lambda_l & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & 0 & \vdots \\ 0 & 0 & \dots & \lambda_m \end{bmatrix} \mathbf{y}_{i-1} + \mathbf{T}_{N-1}(\mathbf{x}_i - \mathbf{x}_{i-N}), \quad (9)$$

ahol  $k, l, m \in \{0, 1, \dots, N-1\}$  és  $\mathbf{T}_{N-1}$  a  $\mathbf{T}$  mátrix utolsó oszlopa.

### A diagonalizált MMT inverze

Ha  $\mathbf{y}_i$  létezik minden egyes időpillanatban és  $\mathbf{T}$  oszlopai  $\mathbf{P}$  sajátvektorai, akkor az inverz MMT-nek létezik egy hatékony számolási módja. Az inverz MMT (IMMT) az  $i$ -edik időpillanatban:

$$\mathbf{x}_i = \mathbf{T}^{-1} \mathbf{y}_i \quad (10)$$

$$\mathbf{x}_i = [\mathbf{s}_0 \ \mathbf{s}_1 \ \dots \ \mathbf{s}_{N-1}] \mathbf{y}_i \Leftrightarrow \begin{bmatrix} x_{i-(N-1)} \\ \vdots \\ x_{i-1} \\ x_i \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \end{bmatrix} \begin{bmatrix} y_{i,0} \\ y_{i,1} \\ \vdots \\ y_{i,N-1} \end{bmatrix} \quad (11)$$

A  $\mathbf{T}^{-1}$  első oszlopa csak egyeseket tartalmaz, így az  $\mathbf{x}_i$  legrégebbi eleme kiszámítható pusztán összeadásokkal:

$$x_{i-(N-1)} = \sum_{k=0}^{N-1} y_{i,k} \quad (12)$$

Tehát a bemenő jelsorozat ( $x_{i-(N-1)} \dots x_i$ ) elemei kiszámíthatók a transzformált jelsorozatból ( $\mathbf{y}_i$ ),  $N-1$  minta késéssel.

Ezidáig a rekurzív MMT általános alakjáról esett szó. A következő fejezet bemutatja, hogy a diszkrét Fourier-transzformáció és annak inverze az egyetlen olyan transzformáció, amely diagonalizálja az MMT-t.

### Momentán Fourier-transzformáció

A diszkrét Fourier-transzformáció (DFT), illetve az inverz diszkrét Fourier-transzformáció (IDFT) mátrixa rendelkezik a 2.2 fejezetben leírt jellemzőkkel, azaz oszlo-

paik a  $\mathbf{P}$  mátrix sajátvektorai.  $\mathbf{P}$  sajátvektorai ( $\mathbf{S}$  oszlopai) egy bizonyos, speciális sorrendben felírva a DFT/IDFT mátrixot adják:

$$\mathbf{DFT} = \mathbf{F} = \mathbf{S}^{-1} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & w & w^2 & \dots & \dots & w^{N-1} \\ 1 & w^2 & w^4 & \dots & \dots & w^{2(N-1)} \\ 1 & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & w^{N-1} & w^{2(N-1)} & \dots & \dots & w^{(N-1)(N-1)} \end{bmatrix} \quad (13)$$

$$\mathbf{IDFT} = \mathbf{F}^{-1} = \mathbf{S} = \frac{1}{N} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & w^{-1} & w^{-2} & \dots & \dots & w^{-(N-1)} \\ 1 & w^{-2} & w^{-4} & \dots & \dots & w^{-2(N-1)} \\ 1 & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & w^{-(N-1)} & w^{-2(N-1)} & \dots & \dots & w^{-(N-1)(N-1)} \end{bmatrix} =$$

$$\frac{1}{N} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & w^{N-1} & \dots & \dots & w^2 & w \\ 1 & w^{2(N-1)} & \dots & \dots & w^4 & w^2 \\ 1 & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & w^{(N-1)(N-1)} & \dots & \dots & w^{2(N-1)} & w^{N-1} \end{bmatrix} \quad (14)$$

Kihasználva az  $N$ -edik komplex egységgyök tulajdonságait (pl:  $w^k = w^{N-k}$ ), belátható, hogy az IDFT-mátrix oszlopai a második oszloptól kezdődően, fordított sorrendben megegyeznek a DFT-mátrix oszlopaival (14). Tehát, ha  $\mathbf{T}$  megegyezik a DFT (15), illetve az IDFT- (16) mátrixszal, akkor az MMT diagonalizálható:

$$\mathbf{y}_i = \mathbf{F} \mathbf{P} \mathbf{F}^{-1} \mathbf{y}_{i-1} + \mathbf{F} \Delta \mathbf{x}_i =$$

$$= \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & w^{-1} & 0 & \dots & 0 \\ \vdots & \vdots & w^{-2} & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \dots & w^{-(N-1)} \end{bmatrix} \mathbf{y}_{i-1} + \begin{bmatrix} 1 \\ w^{-1} \\ w^{-2} \\ \vdots \\ w^{-(N-1)} \end{bmatrix} (\mathbf{x}_i - \mathbf{x}_{i-N}) \quad (15)$$

$$\mathbf{x}_i = \mathbf{F}^{-1} \mathbf{P} \mathbf{F} \mathbf{x}_{i-1} + \mathbf{F}^{-1} \Delta \mathbf{y}_i =$$

$$= \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & w^1 & 0 & \dots & 0 \\ \vdots & \vdots & w^2 & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & 0 \\ 0 & 0 & \dots & w^{N-1} \end{bmatrix} \mathbf{x}_{i-1} +$$



$$\begin{aligned}
& + \begin{bmatrix} 1 \\ w^1 \\ w^2 \\ \vdots \\ w^{N-1} \end{bmatrix} (y_i - y_{i-N}) = \\
& = \begin{bmatrix} 1 & 0 & \cdot & \cdot & 0 \\ 0 & w^{-(N-1)} & 0 & \cdot & 0 \\ \cdot & \cdot & w^{-(N-2)} & 0 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 0 \\ 0 & 0 & \cdot & \cdot & w^{-1} \end{bmatrix} \mathbf{x}_{i-1} + \\
& + \begin{bmatrix} 1 \\ w^{-(N-1)} \\ w^{-(N-2)} \\ \cdot \\ w^{-1} \end{bmatrix} (y_i - y_{i-N})
\end{aligned} \quad (16)$$

A (15) egyenlet nem más, mint a momentán Fourier-transzformáció (MFT) rekurzív egyenlete [6, 7, 8, 9]. Az  $N$  elemű  $\mathbf{y}_i$  vektor tartalmazza az  $i$ -edik mintában végződő  $N$  hosszúságú  $\mathbf{x}_i$  függvényrészlet spektrumkomponenseit. Vegyük észre, hogy az  $y_{i,k}$  spektrumkomponensek egymástól függetlenül számíthatók,

$$y_{i,k} = w^{-k} (y_{i-1,k} + x_i - x_{i-N}) \quad (17)$$

mely növeli az MFT hatékonyságát ha csak néhány frekvenciakomponenst kell kiszámolni, mint például a spektrális zoom transzformációban.

A (16) egyenlet az MFT duál párja, az inverz momentán Fourier-transzformáció (IMFT).  $\mathbf{x}_i$  tartalmazza az  $N$  hosszúságú bemeneti függvényt, míg  $\mathbf{y}_i$   $N$  darab spektrumkoefficiens, melyek az  $i$ -ik frekvenciakomponensnél végződnek. Vegyük észre, hogy  $\mathbf{x}_i$  elemei is egymástól függetlenül számíthatók, valamint azt, hogy az MFT és az IMFT kiszámításánál is ugyanazokat a  $w$  konstansokat (twiddle faktorokat) használjuk, de más sorrendben.

Összegzésképpen elmondhatjuk, hogy ha a DFT vagy az IDFT szerepel a momentán mátrixtranszformációban, akkor a transzformált függvény értékei rekurzívan, egymástól függetlenül számíthatók  $N$  komplex szorzás és  $N+1$  komplex összeadás felhasználásával (a számítási igény csökken, ha a bemenő függvény valós).

### Nem rekurzív inverz MFT

A nem rekurzív inverz momentán Fourier-transzformáció [6] kifejezhető a (12) és (14) egyenletek felhasználásával:

$$x_{i-(N-1)} = \frac{1}{N} \sum_{k=0}^{N-1} y_{i,k} \quad (18)$$

A (18) egyenlet szerint a bemenő függvény ( $\mathbf{x}_i$ ) a kétdimenziós spektrum-idő függvényből ( $\mathbf{y}_i$ )  $N-1$  minta késszel szorzás nélkül, egyszerű szummázással visszanyerhető. Így az MFT/nem rekurzív IMFT-transzformációs pár ((15) és (18)) hatékonyan felhasználható spektrummanipulálásra (pl. szűrésre), különösen akkor, ha a DFT-koefficiensek nagy részére nincs szükség.

Ha az  $\mathbf{x}_i$  függvény valós, akkor ki lehet használni a spektrum konjugált komplex szimetriáját, és az ablak legrégebbi mintája kiszámítható a spektrumkomponensek valós részeinek összegéből:

$$x_{i-(N-1)} = \frac{1}{N} \sum_{k=0}^{N-1} \text{Re} \{y_{i,k}\} \quad (19)$$

Mint az már a [6]-ban levezetésre került, ha  $\mathbf{x}_i$  valós, akkor a spektrumkomponensek képzetes részének összegzésével kiszámítható az  $x_{i-(N-1)}$ -edik minta Hilbert-transzformáltja:

$$H\{x_{i-(N-1)}\} = \frac{1}{N} \sum_{k=0}^{N-1} \text{Im} \{y_{i,k}\} \quad (20)$$

Így tehát az MFT/nem rekurzív IMFT hasznos lehet különböző jelfeldolgozási eljárásoknál, ahol a jel és annak kvadraturakomponense szükséges (pl. távközlés vagy radarrendszerek).

### Az MFT számításigénye és hatékonysága

Ebben a fejezetben az MFT számításigényét és hatékonyságát vizsgáljuk, valamint összehasonlítjuk a különböző gyors Fourier- (FFT) algoritmusokkal. Bár a számításigény többféleképpen definiálható, azt fogjuk vizsgálni, hogy az egyes algoritmusok milyen valós műveletigénnyel (szorzás és összeadás) rendelkeznek.

Vizsgálatunkban egy  $M$  hosszúságú komplex adatsoron  $N$  hosszúságú DFT-ket hajtunk végre. Ha a DFT-k  $q$  ( $1 \leq q \leq N$ ) mintával vannak eltolva egymáshoz képest, és az FFT algoritmust használjuk, akkor  $\frac{M-N}{q} + 1$  DFT-re van szükségünk a teljes adatsor spektrumanalíziséhez. Az MFT-t  $M$ -szer kell használnunk ugyanerre a feladatra, mert a spektrumkoefficienseket minden mintában ki kell számolnunk, függetlenül  $q$  értékétől.

Tehát, ha radix-2 FFT-ket használunk, akkor

$$OPS_{FFT} = \left( \frac{M-N}{q} + 1 \right) [5N \log_2(N)] \quad (21)$$

valós műveletre van szükség, míg az MFT esetében

$$OPS_{MFT} = M [8N_c + 2] \quad (22)$$

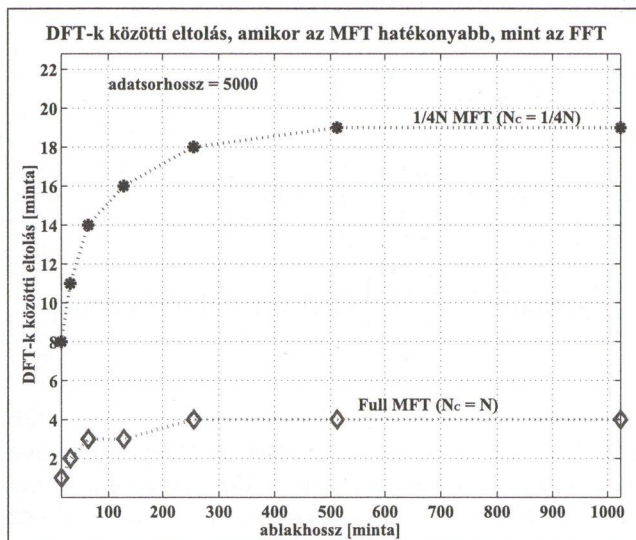
valós művelet kell a teljes adathalmaz analíziséhez. A fenti egyenletben  $N_c$  a kiszámított spektrumkomponensek száma, vagyis  $N_c = N$ , ha az összes kompo-



nens kiszámításra kerül. Az MFT hatékonyabb az FFT-nél, ha a DFT-k közötti eltolás  $q$  kicsi. A (21) és (22) egyenletből kifejezhető, hogy mely eltolások esetén hatékonyabb az MFT, mint a radix-2 FFT:

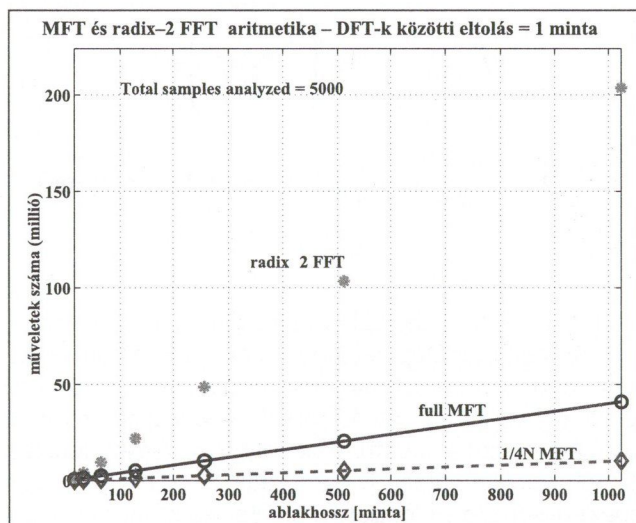
$$q_{MFT} < \frac{(M - N) [5 N \log_2(N)]}{M(8N_c - 1) - 5 N \log_2(N)} \quad (23)$$

Mint ahogy az a (23) egyenletből látható,  $q_{MFT}$  függ az adatsor méretétől ( $M$ ), az ablak méretétől ( $N$ ), valamint a kiszámolt spektrumkoefficiensok számától ( $N_c$ ). A 1. ábrán a DFT-k közötti eltolás látható az ablakméret függvényében, két különböző  $N_c$ -re, amikor az MFT hatékonyabb az FFT-nél.



1. ábra DFT-k közötti eltolás, amikor az MFT hatékonyabb

A teljes MFT hatékonyabb a radix-2 FFT-nél, ha az eltolás nagyon kicsi ( $q_{MFT} \leq 5$ ), míg a redukált MFT ( $N_c = N/4$ ), még akkor is hatékonyabb, ha az eltolás értékei nagyobbak. Vegyük észre, hogy ha a vizsgált adatsor nagyobb, akkor  $q_{MFT}$  értékei nagyobbak minden ablakmérethez. Az algoritmusok számításigénye  $q_{MFT} = 1$  esetben a 2. ábrán látható.



2. ábra Az MFT és a radix-2 FFT számításigénye, amikor  $q_{MFT} = 1$

Az MFT aritmetikája lineárisan függ a számított spektrumkoefficiensoktól ( $N_c$ ) és az analizálandó adat nagyságától ( $M$ ). Egy adott adatsorhosszra, változó eltolás mellett az MFT számításigénye nem változik, míg az FFT aritmetikája jelentősen csökken az eltolás mértékének a növekedésével.

Az MFT-nek  $N$  valós műveletre van szüksége ahhoz, hogy rekurzívan kiszámolja egy  $N$  hosszúságú DFT koefficiensait, ami  $\log_2 N$  javulást jelent a radix-2 FFT számításigényéhez képest. Ha a spektrumnak csak egy részére van szükség, akkor az MFT számításigénye továbbcsökkenthető azzal, hogy csak a szükséges koefficiensokat számoljuk ki. Az MFT hatékonysága, ellentétben a szabványos FFT-algoritmusokkal, nem függ attól, hogy az ablak mérete kettő hatványa-e. Így módon az MFT hatékonyan használható a DFT számításánál, ha a következő feltételek egyike vagy mindegyike teljesül:

- a DFT-k nagyon átlapoltak,
- csak néhány Fourier-koefficiensre van szükség vagy
- DFT hossza egy speciális, nem összetett szám (pl. prím).

Figyelembe véve a fent bemutatott MFT-jellemzőket, hogy az MFT jól felhasználható a jelfeldolgozás különböző területein, mint például

- a valós idejű spektrumanalízisben,
- a valós idejű jelfelismerésben és -detektálásban,
- a beszédfeldolgozásban vagy
- a radar- és a szonárjelfeldolgozásban.

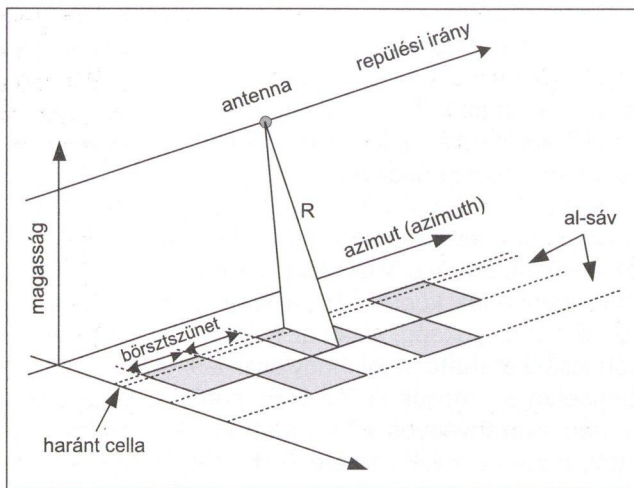
## Az MFT alkalmazása a börsztmódusú SAR-jelfeldolgozásnál

A börsztmódusú üzemmód azért használatos SAR-rendszereknél (pl. RADARSAT, ENVISAT), hogy szélesebb sávról (swath) készülhessen radarkép, hogy energiát takarítsunk meg a műholdon, illetve hogy az adatkapcsolat sáv szélességét csökkentsük a műhold és a földi állomás között. Ebben az üzemmódban a vett jel az azimut-időtartományban periodikusan ablakozott, ami egy szegmentált frekvenciaidő-struktúrát eredményez az azimutspektrumban (az azimutspektrum egy másik elterjedt neve a Doppler-spektrum). A spektrum szegmentált tulajdonsága miatt speciális jelfeldolgozásra van szükség a pontos fókuszálás, a konzisztens fázis és a hatékony számítás érdekében.

### A börsztmódusú SAR-rendszer rövid áttekintése

A börsztmódus általánosan használt a SAR-rendszerekben az úgynevezett ScanSAR üzemmódban, ahol a nyalábot két vagy több sáv között periodikusan kapcsolgatják, hogy minél nagyobb sávról tudjanak képet alkotni. A 3. ábrán a 2 nyalábos ScanSAR-mód sematikus rajza látható.





3. ábra Börsttmódusú 2 nyalábos ScanSAR

Ebben az üzemmódban a radarnyaláb letapogatja az egyik alsávot egy bizonyos időtartamig, majd átkapcsol a másik alsávra. A második alsáv letapogatása után a radar visszatér az elsőhöz, hogy elkezdje a következő börsttciklust. A börsttciklusnak elég hosszúnak kell lennie ahhoz, hogy minden céltárgy teljesen le legyen fedve legalább egy börsttel.

Egy alsávból származó adatot külön kell feldolgozni a többi alsávtól, mert a radarnyaláb különböző földterületet fed le az egyes alsávokban. Azimutirányban (pályairányban) a beérkezett adat diszkrét börsttökre szegmentálódik (szürke terület a 3. ábrán), míg haránt irányban az egyes alsávokban folytonosnak tekinthető.

### A börsttmódusú jelfeldolgozás tulajdonságai

16 egymást követő, a radarnyaláb által teljesen megvilágított és egy harántcellában lévő (3 ábra) ideális céltárgyból származó vett jel látható a 4. ábrán, ahol a börstthossz 20%-a az apertúrahossznak. Szaggatott vonal jelzi az egyes céltárgyak azimutmegvilágítási idejét, amikor a SAR folyamatos módban üzemel, míg a vonalak folytonos része a céltárgyak börsttmódban ténylegesen megvilágított részét jelzik. A teljesen megvilágított céltárgyak azok a céltárgyak, amelyek a folyamatos üzemmódban feldolgozásra kerülnek: teljes a frekvenciaidő-lenyomatuk, és teljes sávszélességű illesztett Doppler-szűrővel kerülhetnek feldolgozásra.

Az egy börsttben felfogott céltárgyrészletek különbözőek az egyes céltárgyaknál, ami jól látható a 4. ábra frekvenciaidő diagramján. Minden egymást követő céltárgy egy alacsonyabb Doppler-frekvencián helyezkedik el egy adott börsttön belül, ugyanakkor a következő börsttben egy magasabb frekvenciára kerülnek mindaddig, amíg a nyalábban található. Az impulzusismétlési frekvencia ( $PRF$  or  $F_a$ ) és az azimutidőben mért apertúrahossz ( $T_a$ ) között az azimut FM-ráta ( $K_a$ ) teremt kapcsolatot:

$$F_a = T_a K_a \text{ [Hz]} \quad (24)$$

Az általunk vizsgált példában  $T_a$  az időtartományban 5 börsttből áll (3 börstt és 2 szünet), így  $F_a$  a frekvenciaidőtartományban szintén 5 börstt sávszélességű (6 ábra). Felhasználva a (24) egyenletet, a szintetikus apertúrahossz azimut-időmintában kifejezve:

$$N_a = T_a F_a = \frac{F_a^2}{K_a} \quad (25)$$

A (24) egyenletben bemutatott idő- és frekvenciaidőtartományok közötti kapcsolatot felhasználva a két egymást követő céltárgy spektruma közötti eltolást ( $q_{tar}$ , a 6 ábrán) a következőképpen kaphatjuk meg:

$$\begin{aligned} q_{tar \text{ Hz}} &= T_{\text{sampl}} K_a = \frac{K_a}{F_a} \text{ [Hz]} \\ q_{tar \text{ bin}} &= \text{round} \left( \frac{q_{tar \text{ Hz}}}{\Delta f} \right) = \text{round} \left( q_{tar \text{ Hz}} \frac{N_{FFT}}{F_a} \right) = \\ &= \text{round} \left( \frac{K_a N_{FFT}}{F_a^2} \right) \text{ [frekvenciakomponens]} \end{aligned} \quad (26)$$

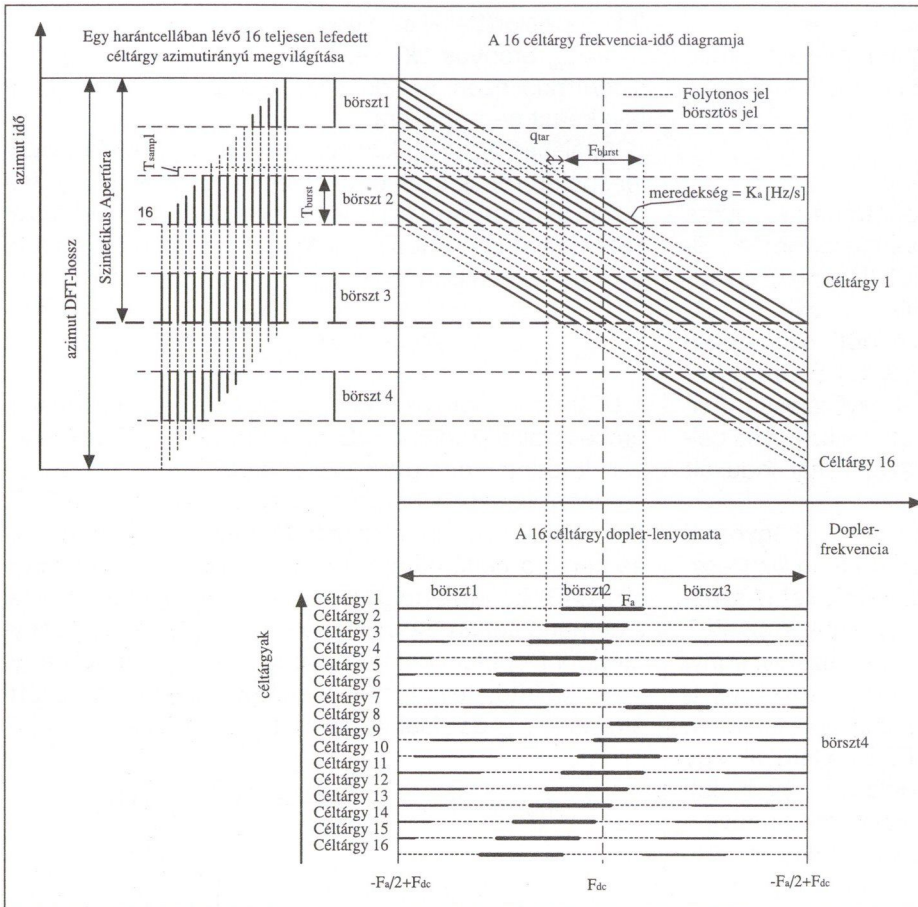
ahol  $T_{\text{sampl}}$  a mintavételi idő, vagyis a két egymást követő ideális céltárgy közötti azimutidő-különbség,  $\Delta f$  egy frekvenciakomponens sávszélessége Hz-ben kifejezve, míg  $N_{FFT}$  a azimut DFT hossza időmintákban kifejezve. Vegyük észre, hogy  $q_{tar}$  arányos  $K_a$ -val és  $N_{FFT}$ -vel, így az céltárgyak közti eltolás mértéke függ a harántiránytól (harántcellától), illetve a DFT hosszától. A börstt sávszélessége Hz-ben, illetve a spektrumkomponensek számában kifejezve szintén a (26) egyenlet felhasználásával kapható meg:

$$\begin{aligned} F_{burst \text{ Hz}} &= T_{burst} K_a = \frac{N_b K_a}{F_a} \text{ [Hz]} \\ F_{burst \text{ bin}} &= \text{ceil} \left( \frac{F_{burst \text{ Hz}}}{\Delta f} \right) = \\ &= \text{ceil} \left( \frac{N_b K_a N_{FFT}}{F_a^2} \right) \text{ [frekvenciakomponens]} \end{aligned} \quad (27)$$

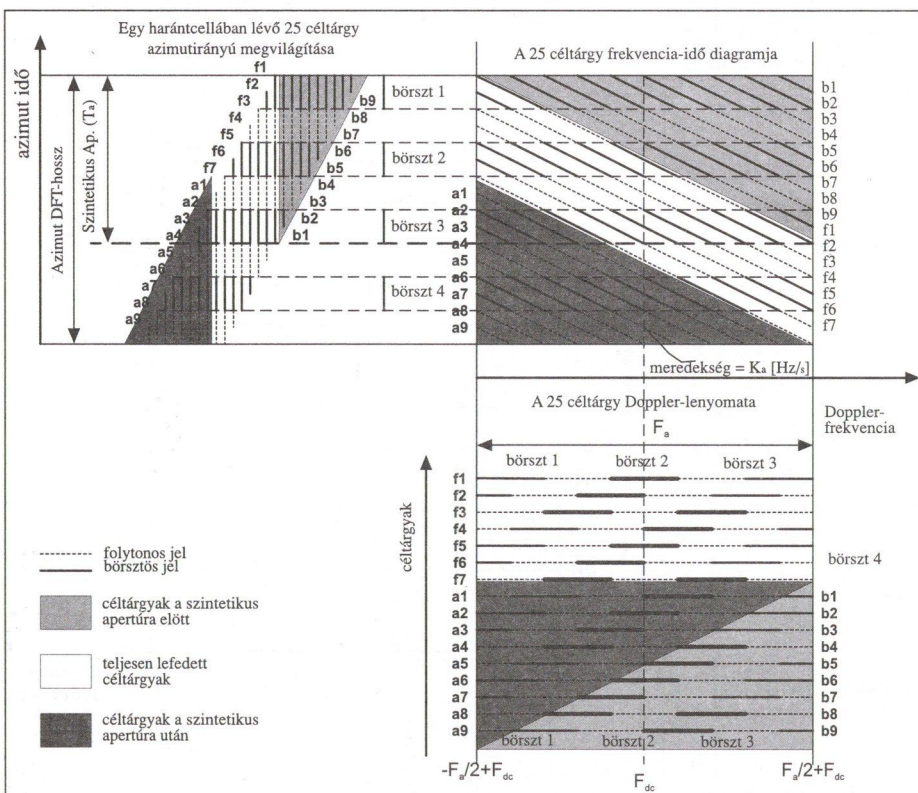
ahol  $N_b$  a börstthossz azimut-időmintákban kifejezve.

A 16 céltárgy Doppler-lenyomatán a 4. ábrán jól látható, hogy két börstt már elegendő az összes céltárgy lefedéséhez (pl a 2. és 4. börstt). A Doppler-lenyomat nem más, mint a spektrum dekompozíciója az illesztett szűrő szorzása után. Megmutatja a céltárgyak azon spektrálisenergia-eloszlását, amikor az azimut DFT a 4 börsttre és a 4 szünetre egyszerre vonatkozik, és a ka-





4. ábra Tizenhat, egymást követő, egy harántcellában, valamint egymástól egyenlő távolságra lévő, teljesen lefedett, ideális céltárgy börsztmódusú feldolgozása



5. ábra Huszonöt, egymást követő, egy harántcellában, valamint egymástól egyenlő távolságra lévő, teljesen és részlegesen lefedett, ideális céltárgy börsztmódusú feldolgozása

pott eredmény meg van szorozva az illesztett szűrővel. Vegyük figyelembe, hogy a céltárgyak spektrálisenergia-eloszlása ugyanaz illesztett szűrő szorzás előtt és után, mivel az illesztett szűrő az ideális céltárgy konjugált komplexe.

A Doppler-lenyomatban vannak olyan céltárgyak, amelyek 2 teljes börszttel lefedettek (pl. 6 céltárgy), vannak olyanok, amelyek 3-mal (pl. 11 céltárgy), míg a többiek 2 teljes és egy rész-börszttel vannak lefedve. Ebben az esetben az átlagos céltárgy-megvilágítás, azaz a börsztök száma egy apertúrában 2,5. Általában a börszt/apertúra arány a ScanSAR-rendszereknél 1,5 és 3 közötti.

Az azimut DFT által teljesen lefedett céltárgyakon kívül az ablak elejénél és végénél léteznek részlegesen lefedettek is. Ezen céltárgyak azimut-időlenyomata nem teljes, így a folytonos módosú jelfeldolgozásnál nincsenek figyelembe véve.

A részlegesen lefedett céltárgyak frekvencia-idő képe és Doppler-lenyomata az 5. ábrán látható. A világosszürke tartomány a DFT előtt kezdődő céltárgyak (b1-b9) időlenyomatát, míg a sötétszürke azon céltárgyak időlenyomatát jelzi, melyek a DFT-ablak után végződnek (a1-a9). Vegyük észre, hogy a részlegesen lefedett céltárgyak nagy részét egy vagy két börszt teljesen befogja. Tehát a spektrumukból egy börsztnyi felhasználva a képfeldolgozásban ők is szerepet játszanak. Így több céltárgyat kisebb felbontással lehet feldolgozni egy adott DFT-hossznál a szintetikus apertúrában, mint a folyamatos üzemmódban.

Az úgynevezett komplex egyszeri nézet (single-look complex – SLC) képfeldolgozásnál lehetőségünk van megválasztani, hogy melyik céltárgyat melyik börszt segítségével dolgozzuk fel. Általában a Doppler-centroidhoz ( $F_{dc}$ ) legközelebbi céltárgyspektrum-részletet vá-



lasztjuk, ahogy ezt a vastagabb vonalak jelzik a 4. és 5. ábra Doppler-lenyomataiban. Mindemellett más börsztök is felhasználhatók, ha például a jelfeldolgozás InSAR-célt szolgál.

### Az SIFFT algoritmus

A legtöbb SAR-jelfeldolgozó algoritmus a gyors konvolúció elvén alapul, ahol frekvenciatartományi illesztett szűrőt használnak az azimut (Doppler) spektrumban. Amikor ezt az eljárást alkalmazzák börszt-módusú adatokra, akkor a börsztök közötti szüneteket nullákkal töltik fel, és az összes börsztöt és szünetet egyszerre szorozzák meg egy teljes sáv szélességű illesztett szűrővel, amit egy IFFT követ. Így az egyes céltárgyakhoz tartozó képpontok börsztök által indukált modulációt fognak tartalmazni.

Az SIFFT-algoritmus abban különbözik a hagyományos gyors konvolúciós eljárásoktól, hogy itt az illesztett szűrő szorzása után rövid, átlapolt IFFT-t használunk a Doppler-tartományban [16]. Így, amikor az IFFT teljesen lefedi egy céltárgy egy börszt sáv szélességnyi részletét, akkor ugyanazon céltárgy következő börsztjéből kevés vagy nulla energia lesz jelen ugyanabban az IFFT-ablakban. Minden egyes IFFT a céltárgyak egy csoportját börsztinterferencia (moduláció) nélkül dolgozza fel, és ez pontos impulzusválaszt eredményez. Tulajdonképpen az IFFT úgy működik mint egy sávszűrő. A céltárgy szegmentált spektrumából egy adott részt használ fel a radarkép kinyeréséhez. A sávszűrő időfüggő abban az értelemben, hogy az egymást követő IFFT-k különböző frekvenciasávra vonatkoznak.

Az IFFT hosszának legalább akkorának kell lennie, mint egy börszt sáv szélessége, hogy a céltárgyakat megfelelő módon transzformáljuk. Felhasználva a (29) egyenletet, a minimális IFFT-ablak mérete:

$$N_{IFFT \min} = F_{burst \ bin} =$$

$$= \lceil \left( \frac{N_b K_a N_{FFT}}{F_a^2} \right) \rceil [\text{frekvenciakomponens}] \quad (28)$$

Az IFFT nem lehet nagyobb, mint egy börszt és egy szünet sáv szélessége, azaz az IFFT által lefedett céltárgyspektrum-részlet nem tartalmazhat egy másik frekvencián lévő, ugyanabból vagy egy másik céltárgyból származó részletet. Az általunk vizsgált esetben a szünet egyenlő hosszú a börszttel, így a maximális IFFT-hossz:

$$N_{IFFT \max} = 2F_{burst \ bin} =$$

$$= 2 \lceil \left( \frac{N_b K_a N_{FFT}}{F_a^2} \right) \rceil [\text{frekvenciakomponens}] \quad (29)$$

A gyakorlatban a fenti határértéken egy kicsit módosítanak a céltárgy spektrális energiájának szétterülése miatt, azaz védősávot alkalmaznak a spektrumon az

IFFT pozicionálásakor. Vegyük észre, hogy  $N_{IFFT \max}$  és  $N_{IFFT \min}$  arányos  $K_a$ -val és  $N_{FFT}$ -vel. Az SIFFT-algoritmus ezen tulajdonsága részletesebben a [18]-ban került bemutatásra.

Általában  $N_{IFFT \max}$  kisebb, mint az  $N_{FFT}$ , így a Doppler-spektrumnak csak egy részét használjuk fel a jelfeldolgozás alatt, ami azt jelenti, hogy az SIFFT-vel létrehozott radarkép felbontása  $N_{IFFT}/N_{FFT}$  faktorialább kisebb, mint a maximálisan lehetséges felbontás, azaz

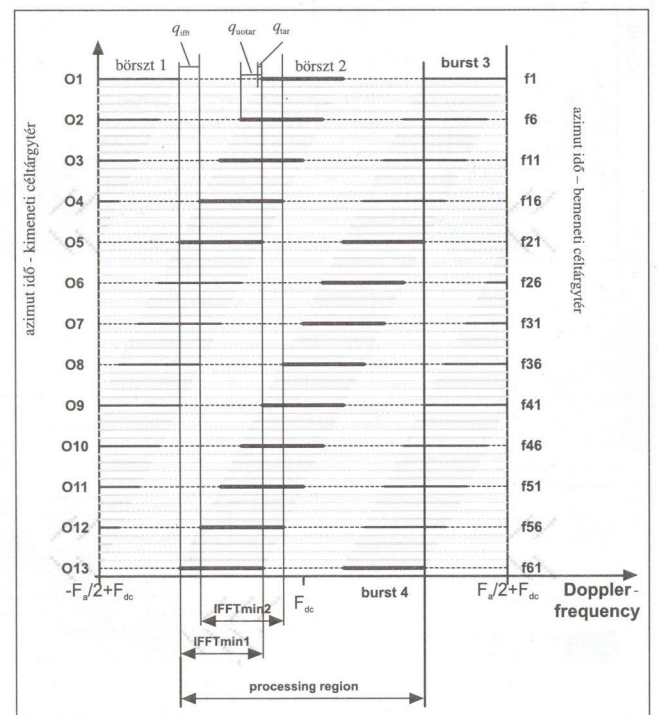
$$\rho_{SIFFT} = \rho_{\max} \frac{N_{IFFT}}{N_{FFT}} \quad (30)$$

A 6. ábrán láthatók az  $N_{IFFT \min}$  pozíciói (vastag vonal) a processzási régióban. Csak az azimut DFT-vel teljesen lefedett céltárgyak szerepelnek az ábrán, abban esetben, amikor 4 börszt és 4 szünet van azimut DFT-ben (4 ábra). Az ábrán szintén látható az algoritmus be- és kimenő céltárgytere. Csak minden ötödik céltárgy (O1-O13) kerül feldolgozásra az SIFFT-algoritmus által a bemenő céltárgytérből (f1-f61), mivel az  $N_{IFFT \min}$  egy-ötöde a Doppler-spektrumnak ( $\rho_{SIFFT} = 1/5$ ). Két egymást követő, feldolgozott céltárgy spektruma közötti eltolás ( $q_{outar}$ ) az alábbiak szerint vezethető le:

$$q_{outar \ Hz} = q_{tar \ Hz} \frac{N_{FFT}}{N_{IFFT}} = \frac{K_a N_{FFT}}{F_a N_{IFFT}} [\text{Hz}]$$

$$q_{outar \ bin} = \text{round} \left( \frac{q_{outar \ Hz}}{\Delta f} \right) = \text{round} \left( q_{outar \ Hz} \frac{N_{FFT}}{F_a} \right) =$$

$$= \text{round} \left( \frac{K_a N_{FFT}^2}{F_a^2 N_{IFFT}} \right) [\text{frequency bin}] \quad (31)$$



6. ábra A minimum IFFT-k pozíciója az SIFFT-algoritmusban a teljesen lefedett céltárgyak processzási régiójában



Látható, hogy *IFFT Min 1* teljesen lefedi az O5 (f21) és O13 (f61) céltárgy egy börsztnyi spektrumát. Ezeknél a céltárgyaknál az *IFFT Min 1* nem fed le másik börsztből vagy szünetből származó spektrumrészletet, így a hozzájuk tartozó radarképpontot nem zavarja meg moduláció. Hasonlóképpen, az *IFFT Min 2* teljesen lefedi az O5 (f21) és O13 (f61) céltárgy egy börsztnyi spektrumát. Annak érdekében, hogy folytonos legyen a radarkép, az egymást követő IFFT-kből származó eredmények össze vannak fűzve [16]. Ha csak a legnagyobb spektrális energiájú börsztöket használjuk fel a céltárgyak processzálásánál akkor a kimeneti eredmények különböző radarképpontot eredményeznek. Vegyük észre, hogy az első IFFT a legnagyobb indexű céltárgyakat (O5 és O13) dolgozza fel, és ahogy az IFFT a magasabb frekvenciák felé tolódik a Doppler-spektrumban, úgy alacsonyabb indexű céltárgyak kerülnek feldolgozásra.

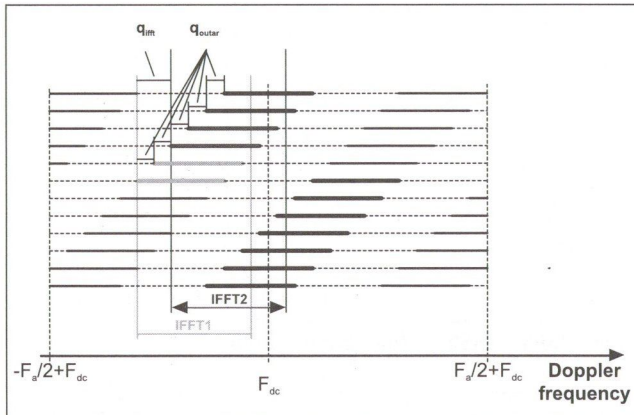
A két egymást követő IFFT közötti eltolás ( $q_{\text{ifft}}$ ) is szerepel a 6 ábrán, ami a következőképpen vezethető le. Minden IFFT egy céltárgy börsztspektrumának az elejénél kezdődik, így  $q_{\text{ifft}}$   $q_{\text{outar}}$  egész számú többszöröse (7 ábra). Két egymás utáni IFFT közötti eltolásban  $q_{\text{outar}}$  száma:

$$Q_{\text{outar}} = \text{floor}\left(\frac{N_{\text{IFFT}} - F_{\text{burst bin}}}{q_{\text{outar bin}}}\right) + 1 \quad (32)$$

A fenti egyenletet felhasználva kiszámítható két egymást követő IFFT közötti eltolás:

$$q_{\text{ifft}} = q_{\text{outar bin}} \left( \text{floor}\left(\frac{N_{\text{IFFT}} - F_{\text{burst bin}}}{q_{\text{outar bin}}}\right) + 1 \right) \quad [\text{frequency bin}] \quad (33)$$

Ha  $N_{\text{IFFT Min}}$ -t használjuk, akkor az eltolás két IFFT között egyenlő két kimenő céltárgy közötti eltolással ( $q_{\text{ifft}} = q_{\text{outar}}$ ). Ha  $N_{\text{IFFT}}$  nagyobb, akkor  $q_{\text{ifft}}$  nagyobb, vagyis kevesebb IFFT szükséges az összes céltárgy feldolgozásához (azaz egy IFFT több céltárgyat dolgoz fel egyszerre).



7. ábra Két egymást követő IFFT közötti eltolás

## Az SIFFT hatékonyságvizsgálata IMFT- és IFFT-algoritmus használatával

Az SIFFT-algoritmus feldolgozási területe három börszt sáv szélességű ( $3F_{\text{burst bin}}$ ) a Doppler-nyomatban (8 ábra). Így az IFFT és az IMFT csak ebben a régióban kerül felhasználásra. Az előző fejezetben megmutattuk, hogy  $q_{\text{ifft}}$  eltolás van két egymás utáni IFFT között, így a felhasznált IFFT-k száma a feldolgozási régióban:

$$NUM_{\text{IFFT}} = \text{ceil}\left(\frac{3F_{\text{burst bin}} - N_{\text{IFFT}}}{q_{\text{ifft}}} + 1\right) \quad (34)$$

Így tehát, ha az IFFT-algoritmust használjuk a céltárgyak feldolgozására, akkor

$$\begin{aligned} NOP_{\text{IFFT}} &= NUM_{\text{IFFT}} \cdot NOP_{N_{\text{IFFT}}} = \\ &= \text{ceil}\left(\frac{3F_{\text{burst bin}} - N_{\text{IFFT}}}{q_{\text{ifft}}} + 1\right) NOP_{N_{\text{IFFT}}} \end{aligned} \quad (35)$$

műveletre van szükség, ahol  $NOP_{N_{\text{IFFT}}}$  a valós műveletek száma egy  $N$  minta hosszúságú mixed-radix IFFT-nél. Ha  $N$  kettő hatványa (radix-2 IFFT), akkor  $NOP_{N_{\text{IFFT}}} = 5N \log_2(N)$ .

A 3.2 fejezetben bemutattuk, egy  $M$  hosszúságú komplex adatsor feldolgozására  $NOP_{N_{\text{IFFT}}} = M(8N_{\text{IMFT}} + 2)$  (22) valós műveletre van szükség, ha  $N_{\text{IMFT}}$  hosszú ablakkal használjuk a teljes IMFT-t. A két-nyalábos börsztmódusú adatfeldolgozásnál  $M = 3F_{\text{burst bin}}$  így az IMFT számításigénye ebben az esetben:

$$NOP_{\text{IMFT}} = 3F_{\text{burst bin}} (8N_{\text{IMFT}} + 2) \quad (36)$$

Vegyük észre, hogy a (35) és (36) egyenletben szereplő képlet függ az azimut DFT-hossztól ( $N_{\text{FFT}}$ ) a következőképpen:  $NOP_{\text{IFFT}}$  az  $N_{\text{IFFT}}$ -n és  $F_{\text{burst bin}}$ -en és a  $q_{\text{ifft}}$ -n keresztül, míg  $NOP_{\text{IMFT}}$   $N_{\text{IMFT}}$ -n és  $F_{\text{burst bin}}$ -en keresztül.

| Processzási paraméter                                    | Mennyiség | Mértékegység |
|----------------------------------------------------------|-----------|--------------|
| Azimut mintavételi frekvencia ( $F_a$ )                  | 1673.32   | Hz           |
| Azimut FM-ráta ( $K_a$ )                                 | -2000     | Hz/s         |
| Doppler Centroid ( $F_{dc}$ )                            | 447.1     | Hz           |
| Szintetikus apertúra-hossz – 3 börszt-2 szünet ( $N_a$ ) | 1400      | minta        |
| Börszthossz ( $N_b$ )                                    | 280       | minta        |
| Egyenlő távolságra lévő céltárgyak közti távolság        | 135       | minta        |

1. táblázat Feltételezett műholdas SAR-rendszerparaméterek az SIFFT aritmetikájának számításánál

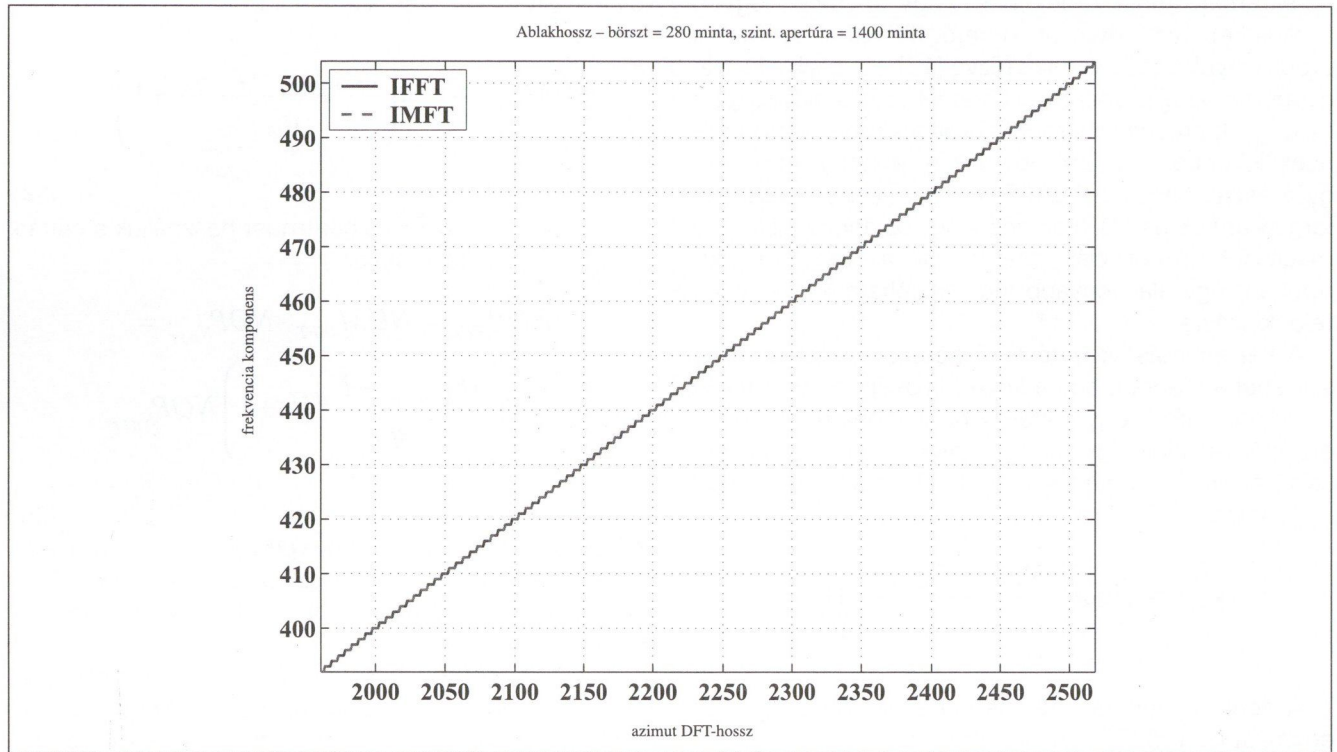
## Az SIFFT hatékonysága az azimut DFT hosszfüggvényében

A műveleti igény számításánál az 1. táblázatban megadott paraméterekkel rendelkező műholdas SAR-

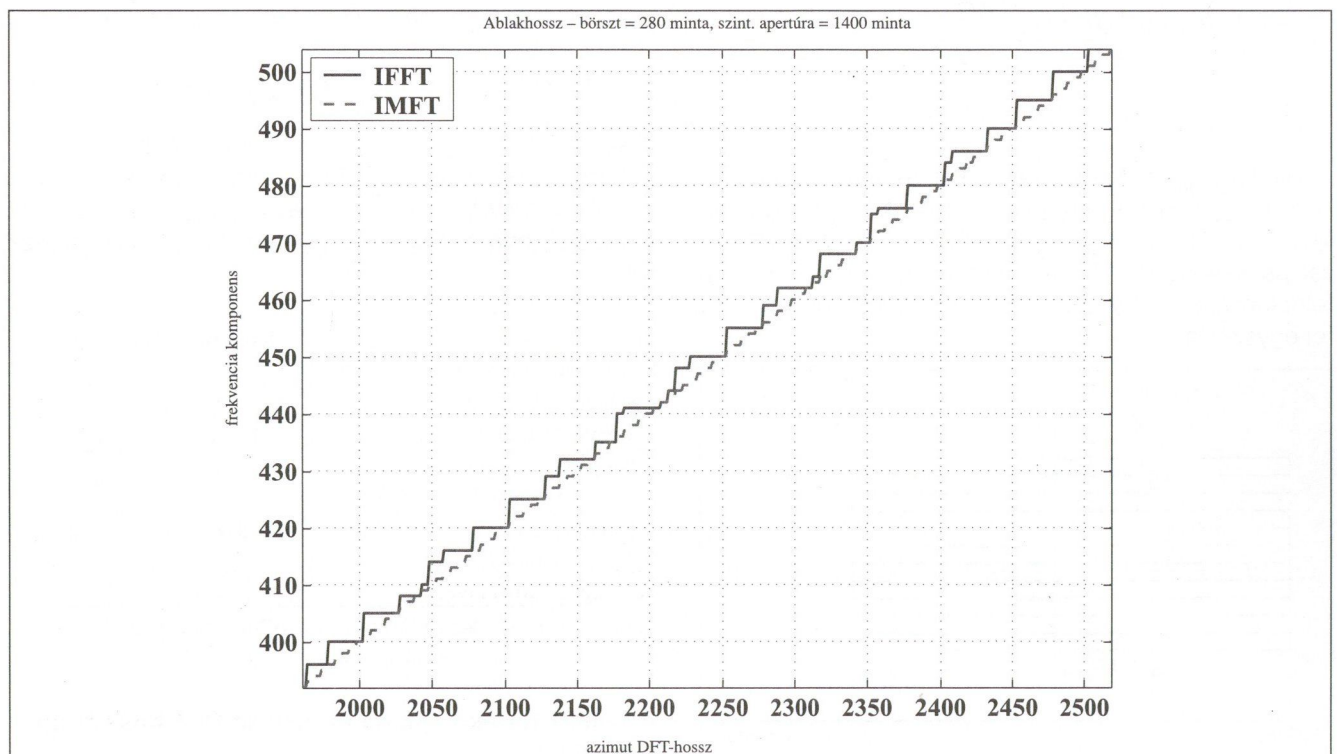


rendszert vettük alapul, ahol az azimut DFT hossza 1960 és 2519 minta között változott ( $1960 \leq N_{FFT} \leq 2519$ ). Először megmutatjuk, hogy milyen az SIFFT aritmetikája az azimut DFT függvényében, minimális IFFT-hossz mellett ( $N_{IFFT} = N_{IMFT} = F_{burst\ bin}$ ), majd megvizsgáljuk a számításigényt abban az esetben, amikor az IFFT-hossza 4 mintával nagyobb lehet a mini-

málisnál (i.e.  $F_{burst\ bin} \leq N_{IFFT} < F_{burst\ bin} + 4$  and  $N_{IMFT} = F_{burst\ bin}$ ). Az utóbbi esetben lehetőségünk van egy előnyösebb (hatékonyabb) IFFT hosszat választanunk 5 lehetséges ablakmérethől a jel-zaj viszony kis romlásának árán. A jel-zaj viszony és az IFFT-ablak méretének az összefüggését a [14] és [15] tárgyalja részletesebben.



(a) minimális IFFT-hossz



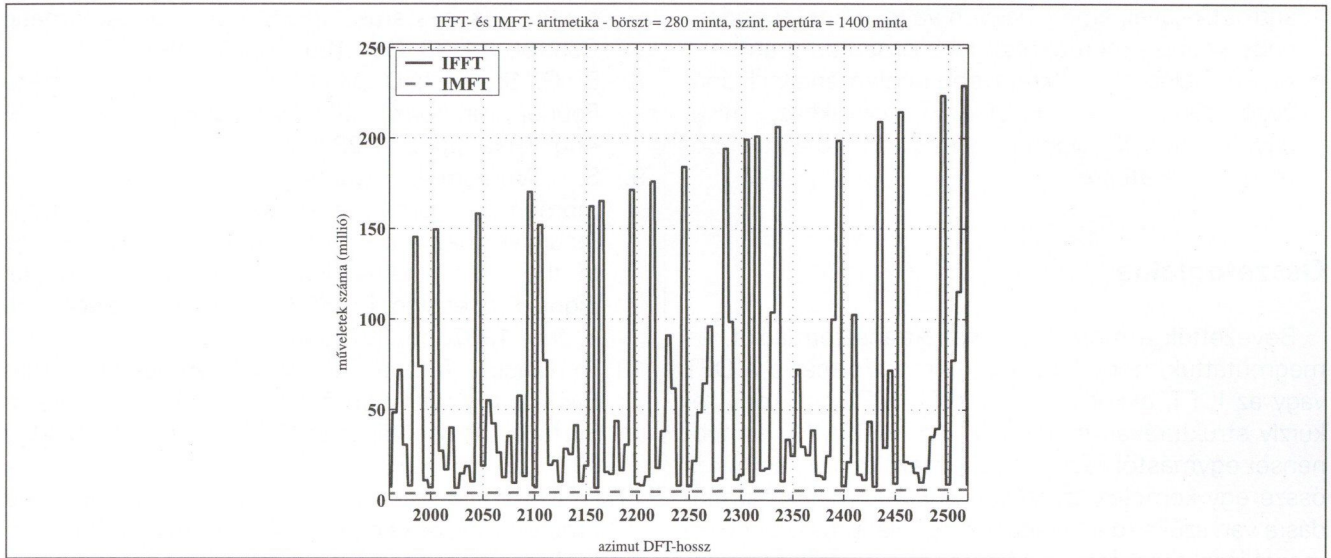
(b) lehetséges IFFT-hosszak száma öt

8. ábra IMFT- és az IFFT-ablakhossz az azimut DFT függvényében



A fentiekben megadott SAR-paramétereket behelyettesítve a (28) és (29) egyenletbe adódik, hogy az IMFT-és IFFT-ablak mérete 392 és 504 között változik. A 8 (a) ábrán jól látható, hogy az első esetben az IMFT és IFFT ablakok mérete egyenlő egymással (és a börsztsávszélességgel), és mind a 113 értéket felveszik a kiszámított intervallumban. A második esetben lehetőségünk van a minimális ablakméretnél nagyobb, 5 egymás melletti ablakhosszból választani. Az IMFT akkor hatékony, ha minél kisebb az ablakméret, míg az IFFT hatékonysága attól függ, hogy az ablak hossza mennyire összetett szám (pl. kettőnek hatványa-e). A

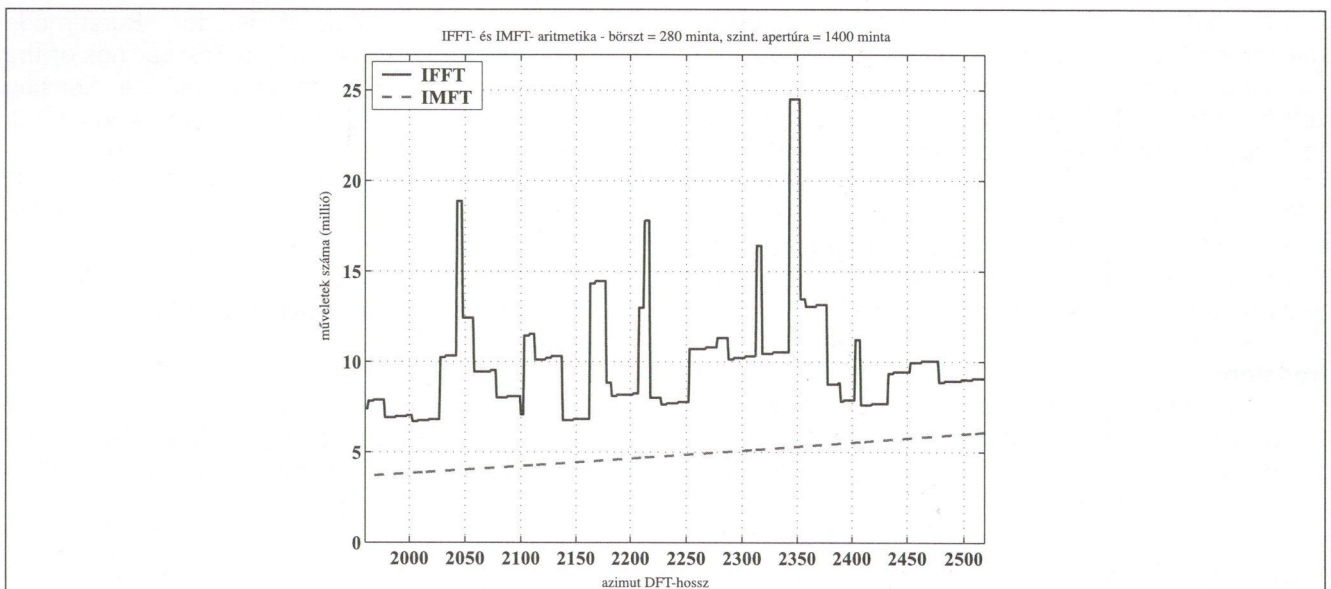
8 (b) ábrán látható, hogy az IFFT-ablak hossza általában nagyobb, mint a lehetséges minimális, tehát sikerült olyan ablakméretet találni, amelynél az IFFT-algoritmus hatékonyabb. Vegyük észre, hogy mindkét esetben nagyon összetett jelfeldolgozó rendszerre van szükség, ha az IFFT-algoritmusokat használjuk, valamint komoly feladatot jelent a különböző IFFT-algoritmusok implementálása. Ezzel ellentétben az IMFT-algoritmust könnyebb implementálni különböző börszt és azimut DFT-hosszakhoz, mivel ugyanaz az IMFT-algoritmus használható különböző ablakméretekre.



9. ábra Az IFFT és IMFT aritmetikája az azimut DFT függvényében, minimális IFFT-hossz

Az IMFT- és IFFT-algoritmusok számításigénye börsztmódusú jelek feldolgozásánál a 9. és 10. ábrán látható. Az IFFT aritmetikája nagyon változó, mivel nagyon függ attól, hogy az ablakméret mennyire összetett szám. Az IMFT aritmetikája sokkal egyenletesebb, és

négyzetesen függ az azimut DFT-hossztól [(38) egyenlet,  $N_{IMFT} = F_{burst}$ ]. Az ábrákból az is kitűnik, hogy az IMFT-algoritmus mindkét esetben hatékonyabb, még akkor is, amikor lehetőség van egy kedvezőbb ablak választására az IFFT-algoritmushoz (10 ábra).



10. ábra Az IFFT és IMFT aritmetikája az azimut DFT függvényében, lehetséges IFFT-hosszak száma öt



A fenti aritmetikai vizsgálat alapján elmondhatjuk, hogy az IMFT növelheti az SIFFT-algoritmus számítási hatékonyságát valamint az alábbi előnyökkel rendelkezik, amikor az SIFFT-algoritmusban kerül felhasználásra:

- Egy adott azimut DFT-hossznál az IMFT-algoritmus akkor a leghatékonyabb, ha az ablak mérete egyenlő a borszt sávszélességével ( $N_{IMFT\ min}$ ). Így a hatékonyság mellett a céltárgyak a legjobb jel-zaj viszonyra kerülnek feldolgozásra.
- Az IMFT aritmetikája egyenletes és négyzetesen függ az azimut DFT-hossztól, ellentétben az IFFT aritmetikájával, amely nagyon változó attól függően, hogy az ablak mérete mennyire összetett szám.
- Az IMFT-algoritmust könnyebb implementálni különböző borszt- és azimut DFT-hosszakhoz, mivel ugyanaz az IMFT-algoritmus használható a különböző ablakméretekre.

## Összefoglalás

Bevezettük a momentán mátrixtranszformációt, és megmutattuk, hogy ha a mátrixtranszformáció a DFT vagy az IDFT, akkor a kapott MFT/IMFT hatékony rekurzív struktúrával rendelkezik. Az MFT/IMFT komponensei egymástól függetlenül kiszámíthatók, és mindössze egy komplex szorzásra és két komplex összeadásra van szükség a frissítésükhöz. Ha az összes inkrementálisan számított DFT-komponensre szükség van, az MFT-nek  $N$  valós műveletre van szüksége ahhoz, hogy rekurzívan kiszámolja a komponenseket, ami  $\log_2 N$  javulást jelent a radix-2 FFT számításigényéhez képest. Az MFT/IMFT algoritmus hatékonyságához nem szükséges az ablakhossznak kétszeres hatványának lennie úgy, mint a radix-2 FFT algoritmusnál.

Borsztmódosú SAR-jelfeldolgozásnál az azimutirányban vett adatok időben változó spektrális tulajdonsága megkívánja, hogy nagymértékben átlapolt inverz DFT-ket használjunk a frekvenciatartomány jól meghatározott helyein ahhoz, hogy az azimut-jelfeldolgozás pontos legyen. Részletes leírást adtunk az SIFFT-algoritmus jellemzőiről, és megmutattuk, hogy az IMFT hatékonyabb lehet, mint az IFFT, amikor az SIFFT borsztmódosú jelfeldolgozó algoritmusban kerül felhasználásra, különösen akkor, amikor a lehető legjobb jel-zaj viszonyra van szükség.

## Irodalom

1. A. Papoulis: Signal Analysis. 1977, McGraw-Hill.
2. G. Strang: Linear Algebra and Its Applications. Third Edition. 1988, Saunders College Publishing.
3. J. Curlander–R. McDonough, Synthetic Aperture Radar: System and Signal Processing. New York, 1991, Wiley.
4. J. G. Proakis–D.G. Manolakis, Digital Signal Processing. Third Edition. 1996, Prentice Hall.
5. R. R. Bitmead–B. D. O. Anderson: "Adaptive frequency sampling filters." IEEE Trans. On Circuits and Systems, vol. CAS-28, June 1981. pp. 524–534.
6. J. Dudás: The Momentary Fourier Transform. Ph.D. thesis, Technical University of Budapest, 1986.
7. H. Lilly: "Efficient DFT-based model reduction for continuous systems". IEEE Trans. on Automatic Control, vol. 36, Oct. 1991. pp. 1188–1193.
8. B. G. Sherlock–D. M. Monro: "Moving discrete Fourier transform". IEE Proceedings-F, vol. 139, Aug. 1992. pp. 279–282.
9. S. Albrecht–I. Cumming–J. Dudás: "The momentary Fourier transformation derived from recursive matrix transformations". In Proceedings of the 13th International Conference on Digital Signal Processing, DSP'97, (Santorini, Greece) vol. 1, July, 1997. pp. 337–340.
10. Tomiyasu: "Tutorial Review of Synthetic-Aperture Radar (SAR) with Applications to Imaging of Ocean Surface." Proceedings of IEEE, Vol. 66, No. 5, May 1978. pp. 563–583.
11. I. Cumming–Y. Guo–F. Wong: "Analysis and Precision Processing of Radarsat ScanSAR Data". In Geomatics in the Era of Radarsat, GER'97, (Ottawa, Canada), May 25-30, 1997.
12. F. Wong–D. Stevens–I. Cumming: "Phase-Preserving Processing of ScanSAR Data with Modified Range Doppler Algorithm". In Proceedings of the International Geoscience and Remote Sensing Symposium, IGARSS'97, (Singapore), August 3-8, 1997. pp.725–727.
13. I. Cumming–Y. Guo–F. Wong: "A Comparison of Phase-Preserving Algorithms for Burst-mode ScanSAR Data Processing". In Proceedings of the International Geoscience and Remote Sensing Symposium, IGARSS'97, (Singapore), August 3-8, 1997. pp.731–733.
14. I. Cumming–Y. Guo–F. Wong: "Modifying the RD Algorithm for Burst-mode SAR Processing". In Proceedings of the European Conference on Synthetic Aperture Radar, EUSAR'98, (Friedrichshafen, Germany), May 25-27, 1998. pp. 477–480.
15. S. Albrecht–I. Cumming: "Application of Momentary Fourier Transform to SAR Processing". IEE Proceedings: Radar, Sonar and Navigation, 146(6), December 1999. pp. 285–297.



# Újszerű számítási eljárások a megbízhatósági analízisben

VESZTERGOMBI GYÖRGY–DR. LEVENDOVSKY JÁNOS–ELEK ZSOMBOR

Budapesti Műszaki és Gazdaságtudományi Egyetem (BME)  
Híradástechnikai Tanszék

L

Távközlési hálózatok megbízhatóságvizsgálatánál a megbízhatóságot jellemző mérték kiszámítása jelenti az elsődleges kihívást, ugyanis ezt a mértéket egy hatalmas állapottér fölötti összegzéssel lehet csak meghatározni. Annak ellenére, hogy az állapottér óriási, rövid idő leforgása alatt kell ezt a mértéket kiszámítani. Célunk tehát olyan statisztikai módszerek kidolgozása, amelyek a hibákat leíró állapottér fölötti véletlen mintavételezéssel működnek, és minél kevesebb mintából adnak jó becslést. Cikkünkben több módszert mutatunk be az átlagos veszteség (Average Loss: AL) és kiesési valószínűség (Probability of Outage: PO) meghatározására. Ezek az új módszerek a fontossági mintavételezés technikáján (Importance Sampling: IS) és közelítő eljárásokon, nevezetesen neurális hálózatokon, illetve lineáris közelítésen alapszanak. A módszerek hatékonyságát nemcsak elméleti elemzéssel vizsgáljuk, hanem numerikus szimulációkkal is alátámasztjuk.

## Bevezetés

A telekommunikációban távközlési hálózatok megbízhatóságának jellemzésére használatos két mérték az átlagos veszteség (AL), amely a meghibásodás esetén maradó sáv szélességet írja le, és a kiesési valószínűség (PO). AL és PO ismeretében megelőző lépésekre nyílik mód, amelyekkel a hálózat teljesítményének romlása mérsékelhető. Ezért AL gyors meghatározása alapvető fontosságú QoS-t biztosító szolgáltatásoknál, IP over ATM hálózatoknál.

A feladat szabatos megfogalmazásához, tételezzük fel, hogy ismertek a következő mennyiségek:

- A hálózati elemek száma  $M$ ;
- A hálózat állapotát jellemző bináris vektor

$$\mathbf{y} = (y^{(1)}, y^{(2)}, \dots, y^{(M)}),$$

ahol

$$y^{(j)} = \begin{cases} 0 & \text{ha a } j\text{-edik elem nem hibásodott meg} \\ 1 & \text{ha a } j\text{-edik elem hibásodott meg} \end{cases}$$

$$\text{és } \mathbf{y} \in Y = \{0, 1\}^M;$$

- Minden  $\mathbf{y}$  vektornál az adott hiba konfiguráció  $p(\mathbf{y})$  valószínűsége;
- A veszteséget jellemző mérték  $g: Y \rightarrow \mathbb{R}$ , ahol  $g(\mathbf{y})$  a rendszer teljesítőképességének a veszteségét jellemzi adott  $\mathbf{y}$  mellett.

A két legfontosabb jellemző mértéket a következő módon határozzuk meg [6]:

1. Az átlagos veszteség (AL), ami úgy írható fel, hogy

$$Eg(\mathbf{y}) = \sum_{\mathbf{y} \in Y} g(\mathbf{y}) p(\mathbf{y}).$$

2. A hálózatkiesés, illetve a kiesési valószínűség (PO)

$$PO = P(g(\mathbf{y}) > C) = \sum_{g(\mathbf{y}) > C} p(\mathbf{y}),$$

ahol  $C \in \{0, 1\}$  egy adott teljesítményküszöb. Látható, hogy

$$P(g(\mathbf{y}) > C) = \sum_{g(\mathbf{y}) > C} p(\mathbf{y})$$

a  $C$  paraméter függvénye, tehát elsődleges célunk a

$$\varphi(C) = P(g(\mathbf{y}) > C) = \sum_{g(\mathbf{y}) > C} p(\mathbf{y})$$

függvény meghatározása.

Mivel az állapottér rendkívül nagy ( $|Y| = 2^M$ ), ezért AL és PO nem számolható ki az összes állapot bejárásával. A hagyományos módszercsaládok kétfajta megközelítéssel élnek, az egyik determinisztikus úton (pl. L–Sylvester-korlát [2,3]), míg a másik statisztikai becsléssel történik (pl. Monte-Carlo rétegelt mintavételezés és fontossági mintavételezés [4]). Mindkét esetben jelentős méretű  $\{\mathbf{y}_k, g(\mathbf{y}_k), k=1, \dots, N\}$  mintahalmazt kell előállítani AL és PO pontos becslésére. A megbízhatósági analízisbeli módszereink egyrészt fontossági mintavételezés segítségével, másrészt adaptív módszerek alkalmazásával próbálnak meg jobban illeszkedni a feladathoz és nagyobb becslési pontosságot elérni.

A fontossági mintavételezést oly módon alkalmazzuk PO becslésére, hogy a minták eloszlásának módosításával a minták a kritikus kiesési tartományba esnek, ezzel jelentősen javítva a hatékonyságot. Ez a hatás úgy érhető el, hogy a teljes kiesés állapotából indulunk ki, és a mintákat súlyozott Bernoulli-eloszlásból származtatjuk. Be fogjuk látni, hogy ez a módszer hatékonyabb a Monte-Carlo-mintavételezésnél.



Rátérve az adaptív approximációs módszercsaládra,  $AL$  kiszámítását tekinthetjük approximációs, más szóval függvényközelítési feladatnak. Az alapvető ötlet az, hogy közelítsük a  $g(\mathbf{y})$  függvényt  $f(\mathbf{y}, \mathbf{w})$ -vel, ahol a  $\mathbf{w}$  vektor a közelítő függvény szabad paramétereit tartalmazza. Ezek hangolásával lehet  $f(\mathbf{y}, \mathbf{w})$ -t úgy beállítani, hogy tetszőleges  $g(\mathbf{y})$ -t adott pontossággal közelítsen. Továbbá a közelítés rendelkezzen az alábbi tulajdonságokkal:

- $f(\mathbf{y}, \mathbf{w})$  nagy reprezentációs képességgel rendelkezzen, vagyis legyen univerzális approximátor a  $G$  térben, ami az össze lehetséges  $g(\mathbf{y})$  függvényt tartalmazza (pl. előnyös, ha  $f(\mathbf{y}, \mathbf{w})$  univerzális approximátor az  $L^p$  térben);
  - a várható érték  $m' = E(f(\mathbf{y}, \mathbf{w}))$  legyen könnyen számítható analitikus formában, vagyis ne kelljen kiértékeléséhez bejárni az egész állapotteret (pl. álljon elő szorzat és összeg alakban).
- Ezen feltételek teljesülése mellett  $AL$  könnyedén kiadódik. Vegyük észre, hogy

$$Eg(\mathbf{y}) = \sum_{\mathbf{y} \in Y} g(\mathbf{y})p(\mathbf{y})$$

kiszámításáról áttolódik a hangsúly egy közelítési problémára. Mivel a neurális hálózatokról bebizonyosodott, hogy univerzális approximátorok, és léteznek gyors algoritmusok a várható négyzetes hiba minimalizálására, ezért a neurális alapú módszerek fontos eszközökké válnak  $AL$  valós idejű meghatározására.

## Hagyományos eljárások $AL$ meghatározására

Ebben a fejezetben röviden összefoglalunk néhány hagyományos módszert a megbízhatósági analízisből. Ezek viszonyítási alapként fognak szolgálni elkövetkező vizsgálataink során. Az egyik legrégebben használt módszer a Monte-Carlo mintavételezés [1], ahol az

$$\tilde{m} = \frac{1}{N} \sum_{i=1}^N g(\mathbf{y}_i)$$

becslést a mintaátlag szolgáltatja. A módszer hiányosságai, mint például a lassú konvergencia és a rossz hatékonyság jól ismertek. Szintén ismeretes a fontossági mintavételezési [6] algoritmus:

$$P(g(\mathbf{y}) > C) = \sum_{\mathbf{y} \in Y} p(\mathbf{y}) I(g(\mathbf{y}) > C) =$$

$$\sum_{\mathbf{y} \in Y} \frac{p(\mathbf{y})}{h(\mathbf{y})} I(g(\mathbf{y}) > C) h(\mathbf{y}) = E_{h(\mathbf{y})} \left[ I(g(\mathbf{y}) > C) \frac{p(\mathbf{y})}{h(\mathbf{y})} \right]$$

Ahol az indikátorfüggvényt jelöli, amely

$$I(x) = \begin{cases} 1 & \text{ha } x \geq 0 \\ 0 & \text{ha } x < 0 \end{cases}, \quad h(\mathbf{y})$$

pedig egy eloszlás, amire teljesül, hogy  $h(\mathbf{y}) \neq 0 \forall \mathbf{y} \in Y'$ , ahol  $Y' = \{\mathbf{y} : g(\mathbf{y}) > C\}$  megfelelő meg-

választásával a becslés szórása jelentősen csökkenthető. Másrészt viszont a megbízhatósági analízis felfogható determinisztikus számítási feladatként, meghozzá úgy, hogy a

$$Eg(\mathbf{y}) = \sum_{\mathbf{y} \in Y} g(\mathbf{y})p(\mathbf{y})$$

összegben a tagok számát próbáljuk csökkenteni. Ennek egy alkalmas módja a következő:

Rendezzük az állapotvalószínűségeket csökkenő sorrendbe  $p(\mathbf{y}_1) \geq p(\mathbf{y}_2) \geq \dots \geq p(\mathbf{y}_N)$ , és gyűjtsük a legvalószínűbb hibaállapotokat az  $Y_1 = \{\mathbf{y}_k, k=1, \dots, N\}$  halmazba. Ez  $Y$ -t két részre osztja,  $Y_1$  és  $Y_2 = Y \setminus Y_1$ -re.

Ezek segítségével becslést adhatunk  $AL$ -re, a

$$\sum_{\mathbf{y} \in Y_1} g(\mathbf{y})p(\mathbf{y}) \leq \sum_{\mathbf{y} \in Y} g(\mathbf{y})p(\mathbf{y}) \leq \sum_{\mathbf{y} \in Y_1} g(\mathbf{y})p(\mathbf{y}) + P(Y_2)$$

korláttal, a

$$P(Y_2) = \sum_{\mathbf{y} \in Y_2} p(\mathbf{y})$$

jelölést használva. Ezek az egyenlőtlenségek Li–Sylvester ( $LS$ ) korlátként ismertek [3].

## Javított fontossági mintavételezés (IIS)

Ez az eljárás a kiesési valószínűség ( $PO$ ) becslését végzi, az IIS rövidítés az angol „Improved Importance Sampling” elnevezésből származik. A módszer fontossági mintavételezés segítségével becsüli  $PO$  értékét a következő módon:

Minden minta előállítását az  $\hat{\mathbf{y}} = (1 \ 1 \dots 1)$  vektorból indul ki, ami a teljes kiesés állapotát jelképezi, vagyis azt az eseményt, hogy minden hálózati komponens meghibásodott. Ebben az esetben  $g(\hat{\mathbf{y}}) > C$  nyilvánvalóan teljesül. Válasszuk meg tehát a módosított  $h(\mathbf{y})$  eloszlást úgy, hogy a minták nagyjából  $\hat{\mathbf{y}}$  közelébe essenek. Ezzel jelentősen javítható a hatékonyság, ugyanis

$$PO = P(g(\mathbf{y}) > C) = \sum_{\mathbf{y} \in Y} p(\mathbf{y}) I(g(\mathbf{y}) > C)$$

kiszámítása a cél, és ha olyan  $\mathbf{y}_k$  mintát generálunk, amire  $g(\mathbf{y}_k) < C$ , akkor  $I(g(\mathbf{y}_k) < C) = 0$ -t kapunk, ami semmivel nem járul hozzá  $PO$  becsléséhez. Így tehát  $\mathbf{y}_k$  számunkra egy „elvesztett” minta, ami csökkenti a hatékonyságot.  $h(\mathbf{y})$  helyes megválasztásával az  $I(g(\mathbf{y}_k) < C) = 0$  esemény valószínűsége csökkenthető, ami végül pontosabb becslést eredményez.

Az IIS-algoritmus pontos meghatározása a következő:

1. Állítsunk elő egy  $\mathbf{u}$  maszk vektort  $q$  paraméterű Bernoulli valószínűségi változók segítségével, a

$$P(u_i = 1) = 1 - q, \quad P(u_i = 0) = q$$

eloszlás szerint, az  $\mathbf{y} = (0, 0, \dots, 0)$  esemény kizárásával.

2. Az  $i : u_i = 0$  komponenseken végezzünk újabb Bernoulli-sorsolást, ezúttal a megfelelő meghibásodási valószínűségek szerint, vagyis

$$P(y_i = 0) = 1 - p_i, \quad P(y_i = 1) = p_i \quad \forall i : u_i = 0.$$

3.  $N$  minta sorsolása után becsüljük  $PO$ -t az



$$\frac{1}{N} \sum_{k=1}^N I(g(\mathbf{y}_k) > C) \frac{p(\mathbf{y}_k)}{h(\mathbf{y}_k)}$$

formulával. Belátható, hogy a módosított mintavételi eloszlás

$$h(\mathbf{y}) = \frac{1}{1 - (1-q)^L} q^l (1-q)^{L-l} \prod_{j \in A} p_j \prod_{i \in B} (1-p_i),$$

ahol  $L$  az  $\mathbf{y}$  vektordimenziója,  $l$   $\mathbf{y}$  súlya,

$$A = \{i: y_i = 1 \cap u_i = 0\} \text{ és } B = \{i: y_i = 0 \cap u_i = 0\}.$$

Ehhez az algoritmushoz levezethető a következő tétel [5]:

**Tétel 1:**

Az IIS-algoritmus hatékonyabb az MC-bebecslésnél, vagyis az IIS-algoritmus becslésének alacsonyabb a szórása az MC algoritmusénál

$$(Var(\tilde{m}_{IIS}) < Var(\tilde{m}_{MC})) , \text{ ha}$$

$$(1 - (1-q)^L) \frac{p_{\max}^{L-k}}{q^k (1-q)^{L-k}} < 1$$

teljesül minden  $1 < k < L$  esetén.

Megjegyzés: Egy 22 elemű gyakorlati hálózatban  $p_{\max} = 1,86e-4$  és  $q = 0,1$  választása teljesíti a feltételt. A bizonyítás a két módszer második momentumának

$$E \left[ I^2 \frac{p(\mathbf{y})^2}{h(\mathbf{y})^2} \right]$$

összehasonlításával vezethető le.

## Neurális módszerek alkalmazása megbízhatóságanalízisben

Ennél a módszercsaládnál  $AL$  meghatározása három lépésben történik:

1.  $\tau^{(N)} = \{(\mathbf{y}_k, g(\mathbf{y}_k)), k = 1, 2, \dots, N\}$  mintahalmaz sorsolása;
2. a  $\mathbf{w}_{opt}$  vektor kiszámítása, amelyik minimalizálja a közelítés hibáját a tanító halmaz fölött, ahol a közelítés hibáját a következő kifejezés adja meg:

$$\mathbf{w}_{opt} : \min_{\mathbf{w}} \sum_{k=1}^N (g(\mathbf{y}_k) - f(\mathbf{y}_k, \mathbf{w}))^2;$$

3. az  $E(f(\mathbf{y}, \mathbf{w}))$  várható érték analitikus úton történő meghatározása.

## Radiális bázisfüggvény alapú neurális hálózatok (RBF)

Ebben a bekezdésben a hagyományos Li-Sylvester-korlát élesítését adjuk meg radiális bázisfüggvényű neurális hálók (RBF) segítségével. Ebben az esetben rendezett mintát használunk, azaz nem véletlen sorsolás alapján áll elő, hanem a legnagyobb valószínűségű minták kiválasztása során. Az algoritmus bemutatása előtt még be kell vezetni a következő fogalmat:

**Definíció:**

Egy bináris  $\tilde{\mathbf{y}}$  vektor a bináris  $\mathbf{y}$  vektor „leszármazottja”, amit  $\mathbf{y} < \tilde{\mathbf{y}}$ -al jelölünk, ha teljesül a következő feltétel:

ha  $y_i = 1$ , akkor  $\tilde{y}_i = 1$  és  $r(\tilde{\mathbf{y}}) \supset r(\mathbf{y})$ ,

ahol  $r(\mathbf{y})$  az  $\mathbf{y}$  súlyát adja meg. A továbbiakban feltételezzük, hogy ha  $\mathbf{y} < \tilde{\mathbf{y}}$ , akkor  $g(\tilde{\mathbf{y}}) \geq g(\mathbf{y})$ . Ez a feltételezés a rendszerek túlnyomó többségére igaz, mivel azt mondja ki, hogy ha adott esetben nő a meghibásodott komponensek száma, akkor a veszteség vagy ugyanakkora marad, vagy növekszik. Az előbb vázolt kikötések mellett a következő algoritmus felhasználható  $AL$  becslésére:

A javított Li-Sylvester-eljárás:

1. A  $g(\mathbf{y})$  függvényt  $N$ -szer számoljuk ki, és  $N$  úgy van megválasztva, hogy létezik hozzá egy  $k$ , amire

$$N = \sum_{i=1}^k \frac{2^L!}{i!(2^L-i)!}$$

( $k$  értékét az  $1, \dots, 3$  intervallumból lehet választani.)

2. Rendezzük az állapotokat valószínűségük szerint csökkenő sorrendbe, és válasszuk ki az első  $N$  darabot:

$$(\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_N) \longrightarrow p(\mathbf{y}_1) > p(\mathbf{y}_2) > \dots > p(\mathbf{y}_N).$$

3. Az  $Y$  állapotteret osszuk fel két halmazra,  $Y_1$  és  $Y_2$ -re,  $Y_1 \cup Y_2 = Y$ ,  $Y_1 \cap Y_2 = \emptyset$ . A két halmazt a következő módon adjuk meg:

$$Y_1 := \{\mathbf{y}_1, \mathbf{y}_2, \dots, \mathbf{y}_N\},$$

$$Y_2 := Y \setminus Y_1.$$

4. Számítsuk ki a következő tanítóminta halmazt

$$\tau^{(N)} := \{(\mathbf{y}_i, g(\mathbf{y}_i)), i = 1, \dots, N\},$$

ahol  $\mathbf{y}_i \in Y_1 \quad \forall i = 1, \dots, N$ .

5. Készítsünk RBF-hálózatot, amit az

$$f(\mathbf{y}) = \sum_{k=1}^K w_k \varphi(\|\mathbf{y} - \mathbf{y}_k\|)$$

egyenlet ír le, ahol hasonlít a Gauss-i eloszlásfüggvényhez:

$$\varphi(x) = \exp \left( -\frac{\sum_{i=1}^L (y_i - y_i^{(k)})^2}{2\sigma} \right)$$

(Itt az  $y_i^{(k)}$ -edik elemét jelöli a  $k$ -adik mintavektornak.)

6. Állítsuk be az RBF-hálózat súlyait a következő lineáris egyenletrendszer megoldásával a  $\tau^{(N)}$  tanítóhalmaz fölött.

$$\sum_{k=1}^K w_k \varphi(\|\mathbf{y}_i - \mathbf{y}_k\|) = g(\mathbf{y}_i) \quad \forall \mathbf{y}_i \in Y_1$$

7. Az RBF-alapú becslés pedig legyen a következő:

$$RBFB = E(f(\mathbf{y}, \mathbf{w}_{kopt})) =$$



$$= \sum_{k=1}^K w_{\text{kopt}} \prod_{i=1}^L \left( p_i \exp \left( -\frac{(1 - y_i^{(k)})^2}{2\sigma} \right) + (1 - p_i) \exp \left( -\frac{(y_i^{(k)})^2}{2\sigma} \right) \right)$$

**Tétel 2:**

Az RBF-hálózat élesebb alsó becslést ad, mint a Li-Silvester alsó korlát

$$LS < RBF < AL$$

**Bizonyítás**

Először kimondjuk az  $Y_1$  és  $Y_2$  halmaz néhány alapvető tulajdonságát.

**Tulajdonság 1**

Minden  $y \in Y_1$  vektorhoz létezik olyan  $\hat{y} \in Y_2$ , amire  $y < \hat{y}$  teljesül. Mint azt korábban láttuk, ebből  $g(\hat{y}) > g(y)$  következik.

**Tulajdonság 2**

A Gauss-i sűrűségfüggvények lineáris kombinációja

$$\sum_{k=1}^N w_k \varphi(\|y - y_k\|)$$

a maximumát az  $(y_1, y_2, \dots, y_N)$  halmaz fölött veszi föl, azaz

$$\sum_{k=1}^N w_k \varphi(\|y - y_k\|) < f(y_i) = g(y_i) \quad \forall i = 1, \dots, N.$$

Először is fejezzük ki a tényleges várható értéket:

$$m = E(g(y)) = \sum_{y \in Y} p(y) g(y) = \sum_{y \in Y_1} p(y) g(y) + \sum_{y \in Y_2} p(y) g(y).$$

Az RBF-alapú becslés is felírható hasonló alakban, ahol

$$RBF = E(f(y)) = \sum_{y \in Y} p(y) f(y) = \sum_{y \in Y_1} p(y) f(y) + \sum_{y \in Y_2} p(y) f(y).$$

Egyrészt az algoritmus hatodik lépése miatt teljesül, hogy  $g(y) = f(y) \quad \forall y \in Y_1$ . Másrészt viszont vissza-

emlékezhettünk az LS alsó korlátra, ami

$$\sum_{y \in Y_1} g(y) p(y) \leq \sum_{y \in Y} g(y) p(y) \leq \sum_{y \in Y_1} g(y) p(y) + P(Y_2).$$

Így elegendő a

$$0 < \sum_{y \in Y_2} f(y) p(y) < \sum_{y \in Y_2} g(y) p(y)$$

állítás belátnunk. Ez viszont belátható az előzőleg kimondott két tulajdonság alapján. Mivel  $Y_2$  minden  $\hat{y}$  eleme leszármazottja valamilyen  $y_i \in Y_1$  elemnek, ezért  $g(\hat{y}) > g(y_i) = f(y_i) > f(\hat{y}) \quad \forall \hat{y} \in Y_2, y_i \in Y_1$ .

Amiből következik, hogy

$$0 < \sum_{y \in Y_2} f(y) p(y) < \sum_{y \in Y_2} g(y) p(y).$$

**Lineáris approximáció**

Ha a lehető legegyszerűbb formájú lineáris approximációt szeretnénk előállítani, akkor tételezzük föl, hogy  $g(y)$  jól közelíthető az  $f(y, w) = w^T y$  lineáris kifejezéssel.

**Lineáris közelítés**

Adott  $N$ , az összesen felhasználható minták száma mellett a következő lépéseket kell megtenni:

1.  $\tau^{(N)} = \{(y_k, g(y_k)), k = 1, 2, \dots, N\}$  mintahalmaz sorso-lása;
2. a  $w_{\text{opt}}$  vektor kiszámítása, amely minimalizálja a közelítés hibáját a tanítóhalmaz fölött, ahol a közelítés hibáját a következő kifejezés adja meg:

$$w_{\text{opt}} : \min_w \sum_{k=1}^N \left( g(y_k) - \sum_i w_i y_i^{(k)} \right)^2;$$

3. A várható érték kiszámítása, ahol

$$E(f(y, w)) = \sum_i w_i p_i.$$

Abban az esetben, ha ez az eljárás nem ad elég pontos eredményt, szakaszosan lineáris közelítéssel lehet javítani a pontosságot. Ebben az esetben az  $Y$  teret felosztjuk  $Y_i$  alterekre, ahol  $i = 1, \dots, L$  a meghibásodások számát jelenti, azaz  $w(y) = i$ , ha  $y \in Y_i$ . Ezután minden részhalmazon  $g(y)$  különböző lineáris közelítésével élünk. Ezzel a szakaszosan lineáris megközelítéssel nagyon jó hatékonyságot érhetünk el.

**Szakaszosan lineáris közelítés**

Adott  $N$ , az összesen felhasználható minták száma; egy adott elosztása a mintáknak a különböző halmazok között, azaz  $\sum_{i=1}^L N_i = N$ ; egy felosztása a térnek a meghibásodások száma szerint  $Y_i, i = 1, \dots, L$ , ahol

$$\bigcup_{i=1}^L Y_i = Y, Y_i \cap Y_j = \emptyset, \quad \forall i, j = 1, \dots, L, i \neq j:$$

1.  $\tau^{(N)} = \{(y_k, g(y_k)), k = 1, 2, \dots, N\}$  mintahalmaz sorso-lása;
2. a  $w_{\text{opt}}$  vektor kiszámítása, amely minimalizálja a közelítés hibáját a tanítóhalmaz fölött, ahol a közelítés hibáját a következő kifejezés adja meg:

$$w_{\text{opt}}^j : \min_{w, y_k \in Y_j} \sum_{k=1}^{N_j} \left( g(y_k) - \sum_i w_i y_i^{(k)} \right)^2;$$

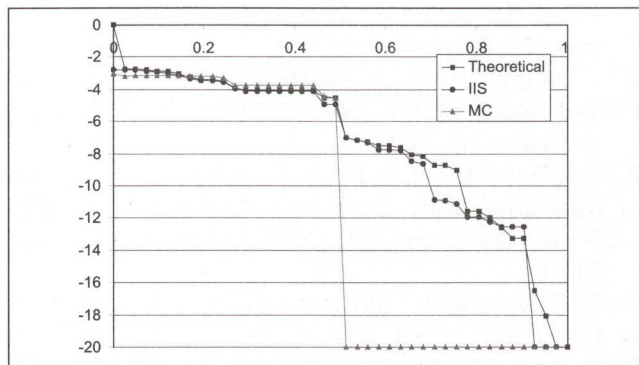
3. A várható érték kiszámítása, ahol

$$E(f(y, w_{\text{opt}})) = \sum_{i=1}^L \left( \sum_j w_{\text{opt}}^{j,i} p_i \right) P(Y_i)$$

Ezzel a módszerrel AL jobban becsülhető, mivel  $g(y)$  a szakaszos közelítés miatt jobban reprezentálható.



## Numerikus eredmények



1. ábra  $\varphi(C)$  különböző módszerekhez

### PO meghatározása

A módszerek hatékonyságának felméréséhez a következő minta SDH-hálózatot vizsgáltuk, amely a magyar nemzeti gerinchálózat (ld. 2-es ábra) egyszerűsített modellje. Ez a hálózat 22 elemből áll (9 csomópontot és 13 élt), ami  $2^{22} = 4\,194\,304$  állapotot tartalmazó teret eredményez. A hálózat hatékonyságának romlását a  $g(y)$  függvény írja le, amely megadja az  $y$  hibavektorhoz tartozó teljesítményjellemzőt. Ennél a példánál  $g(y)$  a kieső kapacitás és a maximálisan elérhető kapacitás hányadosát adja meg. Az algoritmusok összevetéséhez először az elméleti

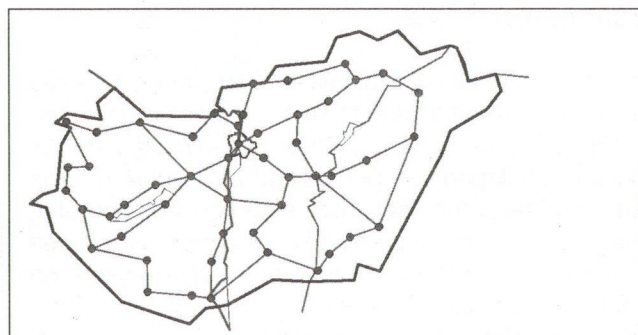
$$\varphi(C) = P(g(y) > C) \quad \varphi(C)$$

függvényt számoltuk ki. Utána PO-t és a hozzá tartozó  $\varphi(C)$  függvényt meghatároztuk az MC és IIS-módszerekre; ennek menetét az 1-es ábrán mutatjuk be.

Jól látható, hogy az új módszer jobban használható  $\varphi(C)$  becslésére, hiszen nagyobb  $C$  értéknél is tudja közelíteni az elméleti értéket, míg az MC-becslés ott már hasznavehetetlen. A görbék meghatározásához  $N = 100\,000$  mintát használtunk.

### AL-számítási eljárások

Ebben a fejezetben összehasonlítjuk az előzőekben tárgyalt algoritmusok hatékonyságát. A mintahálózat, amelyen AL értékét meghatároztuk, a 2-es ábrán látható, és a magyar nemzeti gerinchálózat egy egyszerűsített modellje. A hálózat 111 elemből áll, ebből 52 csomópont, 59 pedig összekötő kábel. (Vagyis az egyhibás  $y$  vektorok száma 111.)

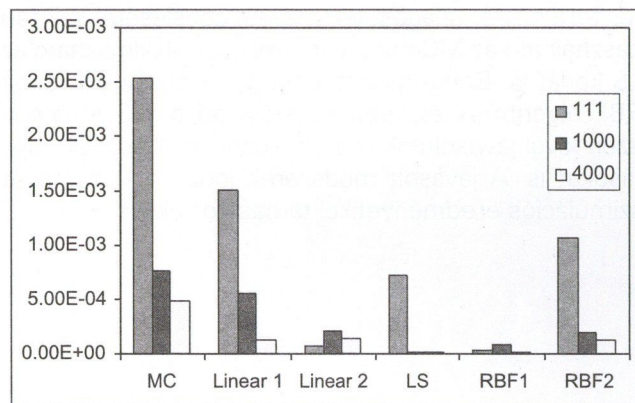


2. ábra Egy lehetséges magyar gerinchálózati topológia

Az egyes módszerekhez tartozó szórások, illetve determinisztikus módszereknél a négyzetes hibák a 3-as ábrán találhatók. Az ábrán használt címkék a következőket jelölik:

- MC: a hagyományos Monte-Carlo-algoritmus;
- Linear 1: lineáris közelítés;
- Linear 2: szakaszosan lineáris közelítés;
- LS: Li–Silvester-becslés;
- RBF1: az RBF-hálózat alkalmazásával élesített LS-becslés;
- RBF2: az RBF1-módszer, véletlenszerűen generált mintahalmazzal.

Mindegyik módszerhez három oszlop tartozik, mely három különböző mintaszám esetén adja meg a szórásokat. A szórásokat 111, 1000 és 4000 mintára határoztuk meg.



3. ábra AL-becslő eljárások sora

Ahogy az ábráról leolvasható, az adaptív közelítő eljárásokkal jó hatékonyságot lehet elérni, különösen az RBF-módszer esetében. Látható, hogy az RBF módszer jobb az LS-becslésnél 111 minta esetében. Ebben az esetben a tanítóhalmaz tartalmazza az összes egyhibás esetet, és ezért teljesül az

$$N = \sum_{i=1}^M \frac{2^L!}{i!(2^L - i)!}$$

feltétel. A következő mintahalmaz, amelyre a feltétel teljesül, azaz tartalmazza az egyhibásokon kívül az összes kéthibás állapotot, már 12 210 elemből állna. A rendelkezésre álló kapacitások korlátozott volta miatt csak az 1000 és 4000 mintaszámra tudtuk a szimulációt lefuttatni. Bár itt nem bizonyított, hogy az RBF-módszer jobb LS-nél, mégis jobb eredmények figyelhetők meg.

Szintén figyelemreméltó, hogy a lineáris módszerek jó hatásfokkal működnek, vagyis ha alacsony számítási kapacitás áll rendelkezésre, akkor ezek az algoritmusok jól használhatóak AL becslésére. A komplexitás növekedésével tovább javítható a becslés pontossága szakaszosan lineáris törtfüggvények alkalmazásával. A tárgyalt módszerek közül a legnagyobb komplexitásúak az RBF-típusú hálózatok, általában ezek jobb approximátorok, mint a lineáris függvények, azonban a rész-



halmazok számának növelésével egyre pontosabb becslés érhető el a szakaszosan lineáris függvényes közelítéssel.

## Összefoglalás

Távközlési hálózatok megbízhatóságvizsgálatánál a hálózatok jellemzésére két fontos mértéket vizsgáltunk, az átlagos elérhetőséget és a kiesési valószínűséget. Számba vettük a hagyományosan használt módszereket ezek meghatározására, és bemutattunk új algoritmusokat. A kiesési valószínűség meghatározására a fontossági mintavételezésen alapuló IIS-algoritmust tárgyaltuk, és elméleti megfontolások alapján bizonyítottuk, hogy hatékonyabb a hagyományos MC-algoritmusnál. Az elméleti eredményt szimulációval is megerősítettük. Az átlagos veszteség becslésére szintén használható az MC-mintavételezés, de alkalmazható az LS korlát is. Bebizonyítottuk, hogy az általunk javasolt RBF algoritmus élesebb becslést ad az LS-korlátnál, ezen kívül javasoltunk lineáris közelítést használó eljárásokat is. A javasolt módszerek jobb hatékonyságát szimulációs eredményekkel támasztottuk alá.

## Irodalom

1. W. E. Deming: "Some Theory of Sampling". New York, 1966, Dover Publ., Inc.
2. L. Jereb: "Network Reliability: Models, Measures and Analysis" 6th IFIP ATM'98 Workshop, Ilkley, UK, 1998. pp. T02/1-10.
3. J. A. Silvester-V. O. K. Li: "Performance Analysis of Networks with Unreliable Components". IEEE Trans. Commun, Vol. COM-32 (1984) pp. 1105-1110.
4. R. E. Melchers: "Structural Reliability Analysis and Prediction". 1999, John Wiley.
5. J. Levendovszky-Gy. Vesztergombi-T. Dávid-L. Jereb: "Improved importance sampling based reliability analysis for communication networks" Proceedings of the 8th IFIP ATM & IP 2000 Workshop, Ilkley, UK, 2000. pp. 46/1-13.
6. R. E. Melchers: "Structural Reliability Analysis and Prediction". 1999, John Wiley.
7. K. I. Funahashi: "On the Approximate Realization of Continuous Mappings by Neural Networks". Neural Networks, VOL. 2. (1989) pp.183-192.

## Hír

A hazai távközlés küszöbön álló liberalizációja hatással lehet a Voice over IP szolgáltatásra. Az 1999-ben indult internetalapú telefónia lendülete töretlen, a VoIP-szolgáltatók száma évente 30-40 százalékkal nő, a forgalmi díjakból származó bevételt az elemzők hétmilliárd forintra becsülik. Az igényeket felismerve – PhoNet márkanévvel október elejétől a PSINet Magyarország is megkezdte VoIP – szolgáltatását, elsősorban az üzleti távközlés eszköztárát használó, virtuális magánhálózattal (VPN, Virtual Private Network) rendelkező partnerei számára.

A PhoNet szolgáltatásnak nincs külön alapdíja, a megrendelőt csak a szolgáltatás igénybevételéhez szükséges internetkapcsolati díj és a beszélgetések másodperc alapon számlázott költsége terheli. A nemzetközi hívások díja átlagosan 30-40 százalékkal alacsonyabb, de a belföldi vezetékes és mobilhívások tarifái is kedvezőbbek, mint a hagyományos telefondíjak.

A VoIP lehetőségeit eddig elsősorban a főváros és az észak-magyarországi régió üzleti vállalkozásai vették igénybe. Várhatóan mind több pénzügyi-gazdasági vezető fogja támogatni az internetalapú telefon bevezetését. A szakértők szerint év végére 4000 fölé nőhet az üzleti ügyfelek száma.

A Bluetooth HBH-20 fülhallgató-mikrofon kihasználja a vezeték nélküli technológia előnyeit, nincs szükség fizikai összeköttetésre a telefonnal, viszont megőrzi a hagyományos fülhallgató-mikrofon megszokott felépítését. Kialakítása lehetővé teszi, hogy akár egész nap viselhető legyen: a kicsiny Bluetooth egység a mikrofont is tartalmazó, rövid vezetékkel kapcsolódik a különálló fülhallgatóhoz. A Bluetooth készülék nyakba akasztva hordható vagy blúzra, ingre csíptethető; ráadásul cserélhető fedőlapja révén harmonizál napi ruházatunk stílusával is. A készülék kis méretű gombjaival mind a bejövő, mind pedig a kimenő hívásokat kezelhetjük anélkül, hogy hozzáérnénk a telefonhoz. Újhívás elutasító gombbal rendelkezik, tehát szükség esetén a készülék tulajdonosa közvetlenül a fülhallgató – mikrofonról utasíthatja el a hívást.

Mérete 68 x 35 x 22 mm, súlya (összesen) 26 g, beszélgetési ideje 4 óra, készenléti ideje 60 óra.



# Nanocsövektől a nanomérnökökig

HORVÁTH GYULA

tanácsadó mérnök

## A folyamat kezdetei

A történet azzal kezdődött, hogy a szén fullerénnek nevezett (hagyományos jelöléssel  $C_{60}$ ) molekuláját 1985-ben felfedezte az angol Kroto és a texasi Smalley, akik ezért 1990-ben Nobel-díjat kaptak. Ugyanekkor német és amerikai tudósok bejelentették a fullerén nagyobb mennyiségben való készítésére kidolgozott eljárásukat.<sup>1</sup>

Iijima japán tudós a szénszálak atomi tulajdonságait már évek óta tanulmányozta, amikor 1991-ben az említett sikerek nyomán felfigyelt a nanovilág kutatásában végzett korábbi munkájának indokoltságát. Két, egymáshoz nagyon közel lévő grafitrúd között vilamos szikrát keltett, az ennek hatására elgőzölgött, majd lecsapódott „szemétben” (amiben más kutatók csak fullerénmolekulákat láttak) pedig igen kicsi csövecskéket talált. Ezek voltak az első, henger alakú, egymásba ágyazott szén-nanocsövek [1]. Az elméleti fizikusok megjósolták a nanocsövek tulajdonságait, aminek hatására a fullerénkutatók közül sokan a forradalmian új kutatási terület, a nanotechnológia felé fordultak.

A biológusok élő sejtekben is felfedeztek szerves anyagokból álló nanocsövecskéket, amelyekben a sokféle szerepet ellátó proteinek [2] mozognak. Ennek kutatásakor új távlatok nyílnak arra, hogy a természetől tanuljunk.

## A nanovilág alapjelenségei

Mint neve mutatja, a nanotechnológia a nanométeres mérettartományba sorolható tárgyak előállításával, mérésével és hasznosításával foglalkozik. Ebbe, a gyakorlatban 1–100 nm mérettartományba esik számos molekula, atom és az elektron (utóbbi kb. 1 nm). Például a baktériumok mérete 1–10  $\mu$ ; a vírusokat már a nanométeres tartományban találjuk. A genetikai in-

formációt hordozó DNS-molekula néhány nanométer „átmérőjű”.

A fullerén molekulastruktúrája kristályos, kb. 1 nm átmérőjű üreg, futball-labdához hasonló. Vannak magassabb rendű, 84, 280 és még több atomból álló, nagyobb fullerének is, de a kutatók már 20 szénatomból álló fullerénről is beszámoltak [3].

Távközlési és számítástechnikai alkalmazások egyelőre a szénatomokból fölépülő nanocsövekre alapozva várhatók, ezért ez a cikk elsősorban a szénalapú (karbon) nanocsövekkel foglalkozik.

A kristályos szerkezetű grafit atomjai lemez formában helyezkednek el, szigorú sorban, közöttük igen erős kötésekkel. Ennél tökéletesebb atomi struktúra felfigyelhető meg a nanocsöveknél. A lemezes szerkezet meggörbül, és csúcsban végződő hengerré záródik össze. Az így keletkező nanocsövek sokszor egymásban helyezkednek el.

A nanocsövek rendkívül szilárd és merev testek, mert nemcsak az atomok, hanem a molekulák közötti kötések is igen erősek. Falvastagságuk egy szénatom-méval megegyező, szakítószilárdságuk és keménységük a gyémántét meghaladja. A gyémánton kívül ez az egyetlen anyag, amely az „úrlift”, vagyis a tudományos-fantasztikus írók agyában megszületett és már a NASA által is tanulmányozott torony anyagaként szóba jöhet. A torony magassága a geostacionárius műholdpálya magasságának nagyságrendjébe esik. A tudósok szerint nem megvalósíthatatlan, hogy a torony tetejére az űrhajókat rakéták helyett úrlift juttatná föl.

A nanocsövek vezetőképességét a grafit gyenge vezetőképessége határozza meg, de adalékokkal a közel fémekre jellemző vezetőképességtől a félvezetőkén át a szigetelőkéig beállítható. Érdekes jelenség az „alagútcsatlakozás” egymással érintkező nanocsövek között. E jelenség során a másik nanocsőbe alagútáram szivárog át, ami meglehetősen rossz érintkezésnek felel meg, viszonyítva két egymásra fektetett, makroszkopikus méretű vezető közötti átmenethez.

<sup>1</sup> Az anyagok fullerén csoportját Richard Buckminster Fullerről nevezték el. Fuller amerikai feltaláló, építész és filozófus 1895 és 1993 között élt. Építési munkásságában öt- és hatszögekből álló konstrukciókat tervezett. Ezek egyike az 1967. évi montreali világkiállítás amerikai pavilonja. Erre hasonlít a fullerén atomszerkezete. – A leggyakrabban előforduló  $C_{60}$  fullerént sokszor buckminsterfullerén néven említik.



## A nanovilág szerszáma és mérőműszere

A nanotechnológiai termékek és atomok megtekintése és kezelése hagyományos eszközökkel nem lehetséges. A fénytörvényei szerint elektromágneses hullámokkal működő mikroszkóppal a fél hullámhossznál kisebb tárgyak már csak elmosódott foltnak látszanak. A röntgen- és gammasugarak nem használhatók, mert az anyagon áthatolnak, arról nem verődnek vissza. Az elektronnak megfelelő hullám hosszúsága a fényénél tízszer, százszor rövidebb, de még elektronmikroszkóppal sem lehet látni a legnagyobb atomokat sem. Egészen új ötletre volt szükség.

A pásztázó alagútmikroszkópban (Scanning Tunneling Microscope, STM [4], más néven Atomic Force Microscope, AFM) az alagúthatást használják ki. Ha egy igen hegyes, ideálisan egyetlen atomban végződő tűt a tárgy felületéhez atomi méretekben közel viszünk, akkor villamos feszültség hatására köztük alagútáram folyik. Ennek erőssége a tű és a tárgy közötti távolságtól függ. A kivitelezett műszerben a tűt, piezoelektromos kristállyal mozgatták úgy, hogy az alagútáram állandó legyen. Ily módon a tárgy fölött sűrű sorokban elmozgatott, pásztázó tű helyzete a kristályt mozgó feszültségből könnyen levezethető. A pásztázást egyébként az elektronmikroszkópnál is alkalmazzák. A műszert 3 év alatt kidolgozó *Binnig* (német) és *Rohrer* (svájci) 1986-ban Nobel-díjat kaptak.

Később kiderült, hogy a pásztázó alagútmikroszkóppal az atomok közötti kötések is láthatóvá lehet tenni, sőt tüje arra is alkalmas, hogy enyhe lökésekkel az atomok helyzetét megváltoztassák vele. Utóbbi módon nagy fáradsággal ugyan, de tárgyak rakhatók össze, melyek atomi struktúráját és anyagi összetételét csak a kémia törvényei korlátozzák.

## Nanocsövek alkalmazási lehetőségei

A nanocsövek segítségével megoldható műszaki feladatok listája állandóan bővül. Ionsugarakkal szilárd, nem szerves anyagokból nanocsöveket lehet húzni, kívánt átmérővel. Ha ezek egyforma átmérőjűek, a lemez szitához hasonló szűrővé alakul, melynek lyukain csak meghatározott méretű molekulák vagy atomok férnek át. Ezen az elven alapuló szűrőket használnak például egyedülálló DNS-molekulák folyadékból történő kiszűrésére, de kéményekre is ezzel terveznek füstgázsűrőket kifejleszteni.[5]

A nanocsövekből a fenti módon membrán is kialakítható, ami például a PEM-típusú üzemanyagcellákban hasznosítható. Létezik már elgondolás arra is, hogy a járműveken alkalmazott üzemanyagcellák táplálásához szükséges hidrogént az igen szilárd nanocsövekből készített tartályokban tárolják.

A nanocsövek a mikroelektronikai áramkörök közötti vezetékként is használhatók. Hajlíthatók és egymással összeforrasztathatók. A forrasztást a nanocsövek érintkezési helyére irányított elektronsugárral végzik.

A nanocsövek levegőnek kitéve szénttartalmú szennyezéseket vesznek föl. A speciális elektronsugár a hulladékot az elektromosságot jól vezető grafit-szerű szénréteggé alakítja át, ami a két nanocsövet egymáshoz rögzíti. [6]

Könyvekben hajlított nanocsöveknél diódahatás érhető el, aminek kihasználásával tranzisztor is felépíthető (2. ábra.). Hír érkezett már arról, hogy ezzel a lehetőséggel élve az IBM kutatói egyetlen molekulát tettek logikai műveletek ellátására alkalmassá [7].

A biológusok abban bíznak, hogy a tudományos fantáziában már megjelent nanoméretű készüléket, amely a vérkeringés egész rendszerét bejárja információk gyűjtése vagy gyógyszerek célzott elhelyezése céljából, a nanotechnológia eszközeivel meg lehet alkotni (a hajszálerek átmérője kb. 1  $\mu$ ).

Egy Leonardo-freskó restaurálásakor a pigmentréteg lepattogni készülő darabkáit alkoholban oldott olajjal megmentették, majd a darabkákat alkoholos oldatba mártva visszahelyezték a freskó helyükre. Az oldatban szuszpendált 200-250 nm méretű szemcsék a legkisebb repedésbe is behatoltak, majd az alkohol elpárolgása után mészkővé szilárdultak [8].

## Még sok megoldandó részletkérdés maradt

Minden nanoméretű alkalmazásnál figyelembe kell venni azonban a hőmozgás hatását és a kvantummechanika törvényeinek érvényesülését. Előbbi esetben a hőmozgás rendezetlensége okoz gondot, ami a makroszkopikus tárgyaknál legfeljebb söréztáj formájában érzékelhető, de pl. tranzisztor kicsinyítésekor a néhány ezernél kevesebb atomból készített tranzisztor stabilitása már nem kielégítő.

A hőmozgás következtében rezgő atomok és elektronok nehezen nézhetők és fényképezhetők, mert pontok helyett foltok látszanak. Ezen és más nem kívánatos jelenségeken a tárgy lehűtésével lehet segíteni, mert az a hőmozgás amplitúdóját csökkenti (az abszolút nulla fok hőmérséklet nem érhető el). Az STM is csak lehűtött eszközökkel és tárggyal használható.

Kvantummechanikai jelenség a nanotechnikában például az, hogy az 1 nm belső átmérőjű csőben az elektronok méreteiknél fogva már csak egyenként férnek el, vagyis csak egymás után haladhatnak, és emiatt összetorlódnak. A jelenséget blokkolásnak nevezik, ami abból áll, hogy a feszültség növelésekor bizonyos áramerősségnél az áram megszakad, és csak a feszültség megfelelő emelésével indul újra. Eme jelenség által okozott nehézségekről, azok kiküszöböléséről vagy ellenkezőleg, a jelenség felhasználásáról nem érkezett még hír.

## Érdekes lehetőségek

A nanotechnológiában jelenleg remélhető lehetőségek, amelyek kihasználása és megvalósítása, gyakorla-



ti bevezetése hosszú és sikeres kutató-fejlesztő munka után várható, a következők:

Egy bit – egy atom [9], nanoprocesszor, energiatárolás egy molekulán, energiaátalakító molekula, elektronikai eszközeink kisebbitése tized- vagy talán százszázred részükre.

A legnagyobb kihívást tárgyak összerakása jelenti atomokból. Alkalmazásának nélkülözhetetlen gazdasági feltétele az, hogy az egyszer nagy költséggel összerakott minta gépi úton sokszorosítható legyen. Csodálatos gépeket várhatunk a nanoelektronikától, csak egy alapvető gond van: még nem tudjuk, hogy élő szervezetünk hogyan másolja sejtjeinket, pedig gépünknek ezt kellene utánoznia.

## Nanométernökök

A feladat jövőbeni megoldóit – és joggal mai elődeiket is – nanométernököknek nevezhetjük, akikre a gazdaságos előállítás útjának-módjának kidolgozása is vár. Az előttük álló, még ismeretlen nehézségekről, a piacképes termékek megjelenésének várható időszakáról még jóslatok sincsenek. A világszerte dolgozó tudósok és nanométernökök sincsenek viszont tőlünk messze, mert egyik kutató-

helyük az MTA Műszaki Fizikai és Anyagtudományi Kutató Intézet Nanoszerkezetek Kutatása Osztálya [3, 4], ahol már hagyomány műszerek készítése üreszközökhöz.

## Irodalom

1. Philip Ball: Focus on carbon nanotubes, nature science update. 1999.11.26
2. Mark Haw: Arrows point to nanotech's future, nature science update. 2001.09.19
3. dr. Bíró László Péter: Nanoforradalom, avagy a természet ajándéka. Népszava, 2000.03.11
4. dr. Barna József: A nanotechnológia. <http://supernova.ake.hu/bolygo/ds1/nano1.htm>
5. Tersoff, J.: Nanotechnology: Less is more. Nature 412 (2001) pp.135–136.
6. Philip Ball: Nanotechnology solders on. <http://www.nature.com/nsu/010628/010628-2.html>
7. Egymolekulás áramkör (szerző nélkül) <http://www.korridor.hu/cikk/php?-100000014266>
8. Philip Ball: Nanotechnology restores flaking frescos. <http://www.nature.com/nsu.010712/010712-8.html>
9. Philip Ball: Turning on the nanoworld. <http://www.nature.com/nsu.001102/001102-10.html>



# Könyvet ajánlunk

*„A titok ajtaját nem olyan nehéz kinyitni, mint ahogy azt  
a tudatlan emberek gondolják.  
Ellenkezőleg, az a szörnyű, milyen nehéz bezárni.”*

*Akutagava Rjunosuke (1892–1927) japán író*

Nos, pontosan erről szól ez a könyv. A titok elrejtésének, „bezárásának” módszereiről, amely az emberrel talán egyidős vágy, és lassan az információs társadalom hétköznapi szükségszerűségévé válik. Céлом e könyvvel (és további folytatásával) az, hogy a kedves Olvasót könnyed, játékos formában, mégis együttgondolkodásra készítve vezessem be abba a misztikusnak tartott világba, amelyről ma még azt gondolja, hogy az csupán a James Bondok és a matematikusok, informatikusok, kriptográfusok kiváltsága.

A Titok Tan, mint alcíme, a „Kódtörő ABZ” is jelzi, igyekszik a Titok természetét és általános törvényeit A-tól Z-ig, azaz az alapoktól a mai és a jövőbeli titkosítási lehetőségekig körüljárni, követve a kriptográfiai gondolkodás fejlődését. Nem felejtkeztem el arról sem, aki ennél mélyebben szeretne belelátni ebbe az érdekes világba. Sok ábra, illusztráció, történelmi példa és részletes irodalomjegyzék segíti a gyakorlati és elméleti eligazodást a témákban.

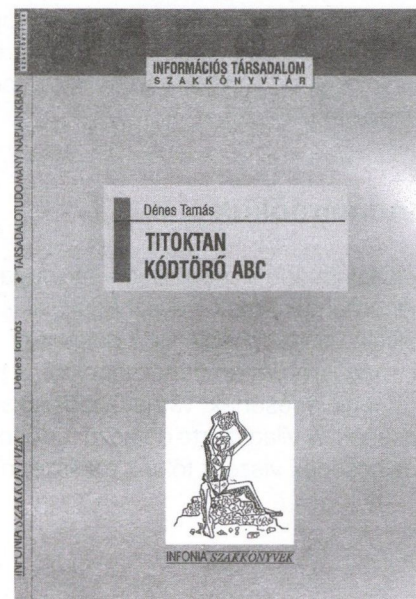
A könyvben szereplő számos Titok Próbá feladvány jó megoldói egy mások számára láthatatlan könyvrészt fedezhetnek fel ugyanebben a könyvben.

A könyv igen aktuális ma, amikor az információs társadalom küszöbén egész életünket egyre jobban át-  
szövi a titkosítás és a biztonság igénye, illetve a privát információk veszélyeztetettségének réme. A magyar könyvpiacra több mint 20 éve jelent meg utoljára a titok egy speciális területét, a titkosítások történetét bemutató, nem informatikai szakkönyv (Révay Zoltán: Titkosírások). Átfogó, a titok természetét, annak hétköznapi, játékos (rejtvény), profi (kriptográfia), szépirodalmi stb. vonatkozásait tárgyaló mű a hazai könyvpiacra eddig nem jelent meg, ezért a Titok Tan széles olvasóközönségre számít („10–100 éves korig”).

Tartalmát tekintve sem „egyszeri olvasás után eldobható” kategóriába sorolható a könyv, mivel számtalan enciklopédikus információt tartalmaz (naprakész formában), valamint az alcímbeli ígéretéhez híven sok-sok konkrét módszer, rejtjelező eszköz, valamint játék és fejtörő leírását, amelyek segédeszközként a későbbiekben is felhasználhatók. Ezen kívül több olyan információblokk van a könyvben, amelyet először e kötet gyűjt össze.

A könyv mottójául választott Karinthy Frigyes-idézet („Nem mondhatom el senkinek, elmondom hát mindenkinek”) szellemét reményeim szerint közösen engedjük ki a palackból, így nem marad TITOK-ban.

*Dénes Tamás*





# Kis lépésekkel az infotársadalom felé

PÁTI BRIGITTA

Napjainkban a sajtó tele van a vezetékes és a mobiltáv-  
közlési szolgáltatók, az internetszolgáltatók hirdetéseivel. Kinek szólnak ezek a hirdetések?

Tendencia, hogy egyre fiatalabb korosztályt céloznak meg a szolgáltatók. A mobiltelefon szolgáltatás mint termék még igen fiatal, nem ismertek hosszú távú társadalmi, gazdasági hatásai. A hatóságok nem korlátozzák a felhasználói réteget, mesterséges korlát nincs a piacon.

A mai gyerekek már a számítógép mellett nőnek fel, használják játéka és iskolai munkavégzésre egyaránt. A telefon, mint az információáramlás gyors és kiemelt eszköze a következő lépcsőfok. Kényes az egyensúly: ha tiltjuk, kimaradhat egy fontos lépés a fejlődésben, az információs társadalomhoz való alkalmazkodásban, az új életritmus felvételében. A korai használat viszont torzíthatja az értékrendet, a gyermek egészséges fejlődését.

A társadalom különböző korosztályai nem egyformán élnek meg az információs társadalomba való átmenetet.

Az Európai Unió eEurope programja tartalmazza az EU tagállamai információs társadalommá való átalakulásának stratégiáját és akcióit. Ennek kiterjesztése az eEurope+, mely arra törekszik, hogy összhangba hozza az EU valamennyi ilyen programját. Az információs program a következő célokat tartja elsőrendűnek:

## **1. Az információs társadalom megalapozása**

- megfizethető árú távközlési szolgáltatás hozzáférhetővé tétele mindenki számára
- a közösségi joganyag információs társadalommal kapcsolatos részének átvétele

## **2. Olcsóbb, gyorsabb és biztonságosabb internet**

## **3. Befektetés az emberekbe és az információs jártasság megszerzésébe**

- az európai fiatalok beléptetése a digitális korszakba
- munka a tudásalapú gazdaságban
- mindenki bevonása a tudásalapú gazdaságba

## **4. Az internethasználat elősegítése**

- az e-kereskedelem terjedésének felgyorsítása
- elektronikus kormányzat: on-line hozzáférés a közösségi szolgáltatásokhoz

- on-line egészségügy
- európai digitális tartalom a globális hálózatok számára
- intelligens közlekedési rendszerek, irányítás
- on-line környezet(védelem)
- távoktatás

Az EU a csatlakozó országok fejlődéséhez nem látja elegendő garanciának csupán a program átvételét, szükséges a gazdaság általános modernizálása, a piaci folyamatok átalakítása, a kormányzat átlátható funkcionalizálása és a polgárok kapcsolatrendszerének átalakulása. Nézzük meg, hogy az egyes pontok mennyiben valósultak meg hazánkban, és ezzel hol tartunk Európában és a világon.

## **Az internet ára Magyarországon**

Az OECD 2000-es összesített adatai alapján az összes tag közül hazánkban a legdrágább havi 20 órányi internetezés. Az internet használók száma tekintetében az EU-csatlakozásra várók között középen helyezkedünk el. Utánuk a sorban Lengyelország, Portugália, Csehország és Görögország következik. Ezen felmérést erősíti, hogy nem állunk kiemelkedő helyen az internethasználói statisztikában sem: A Netsurvey által végzett felmérés szerint a lakosság 14 százaléka tudja használni az internetet, otthoni eléréssel azonban csak 8 százaléknak rendelkezik. A világhálózathoz hozzájutók valamivel több mint 70 százaléka a vagyon szerinti társadalmi hierarchia két legfelsőbb rétegéhez tartozik, többségben vannak az egyetemi és főiskolai diplomával rendelkezők. A felhasználók legnagyobb része 30 év alatti, 57 százalék a férfiak, 43 százalék a nők aránya.

A magyar internetpiacon – a nemzetközi tendenciáknak megfelelően – az utóbbi években több ingyenes hozzáférést biztosító internetszolgáltató cég is megjelent, erősítve ezzel a versenyt az egyelőre korlátozott számú előfizetőkért, valamint lefelé mozdítva az árakat. Hosszú távon nem tartható fenn az igen költséges internetszolgáltatás kizárólag a reklámokból – ezt számos .com vállalat látványos bukása is mutatta külföldön –, de a próbálkozások jótékonyan hatnak az árakra.



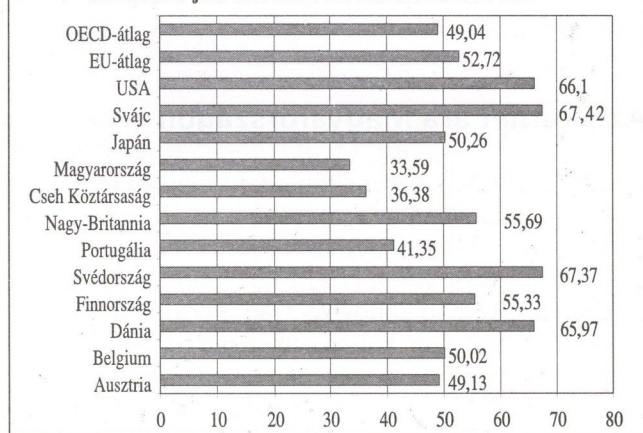
**100 lakosra jutó internethasználók száma** (a 14 évesnél idősebb lakosság körében) 2000-ben

|     |               |    |
|-----|---------------|----|
| 1.  | Szlovénia     | 37 |
| 2.  | Észtország    | 25 |
| 3.  | Csehország    | 16 |
| 4.  | Horvátország  | 14 |
| 5.  | Bulgária      | 13 |
| 6.  | Szlovákia     | 11 |
| 7.  | Lettország    | 10 |
| 8.  | Magyarország  | 9  |
| 9.  | Lengyelország | 8  |
| 10. | Románia       | 7  |
| 11. | Litvánia      | 7  |
| 12. | Macedónia     | 6  |
| 13. | Jugoszlávia   | 4  |
| 14. | Oroszország   | 3  |
| 15. | Ukrajna       | 2  |

Forrás: www.ittk.hu/infinet

**A távközlési szolgáltatások hozzáférhetővé tétele mindenki számára**

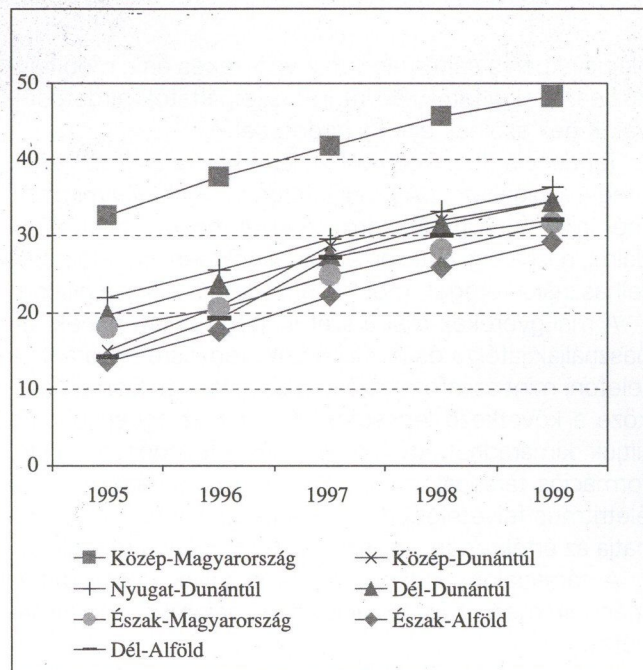
A távközlési szolgáltatások alapterméke a fix telefonszolgáltatás. Érdemes megvizsgálni, hogyan alakul ez más országokhoz viszonyítva és hazánk egyes régióiban.

**100 lakosra jutó távbeszélő-fővonal száma 1998-ban**

A táblából látható, hogy hazánk egyelőre elmarad az EU átlagos szintjétől. A jelenlegi árakon a piac nem igényli e szolgáltatást, a fix bekötések száma évről évre csökken, a fogyasztók a mobiltelefont választják helyettesítő termékként. Ez nem könnyíti meg az internet használatának elterjesztését, mivel Magyarországon igen szűk réteg használja a WAP szolgáltatást. Európai szinten a mobilfelhasználók közül 2000-ben mindössze 5% vette igénybe. A WAP Európában a szolgáltatóknak egyelőre csalódást és igen tetemes veszteségeket okozott ezidáig. A médiakampányok következtében a fogyasztók arra számítottak, hogy a vezetékes interneten megszokott szolgáltatásokat érhetik el, változatlan minőségben – ehelyett magas díjakért tudják csak igénybe venni a korlátozott szolgáltatást. Ezért egyelőre csak egy szűk réteg érdeklődik iránta.

Az EU távközlési miniszterei támogatják azt a javaslatot, amely szerint az operátoroknak funkcionális internet-hozzáférést kell garantálni. Ezáltal az internethasználat alanyi joggá válna minden állampolgár számára, és az elzárt vidékeken élők; továbbá az alacsonyabb jövedelemmel rendelkező réteg is esélyt kapna az új társadalomba való bekapcsolódásra, a felzárkózásra. Amennyiben csatlakozni akarunk az EU-hoz, ez komoly feladatot jelenthet a jövőben a vezetékes szolgáltatóknak és az államnak egyaránt.

Hazánk egyes régióiban eltérőek a meglévő telekommunikációs feltételek. Az alábbi ábra jól mutatja a nagyságbeli és trendbeli különbségeket:



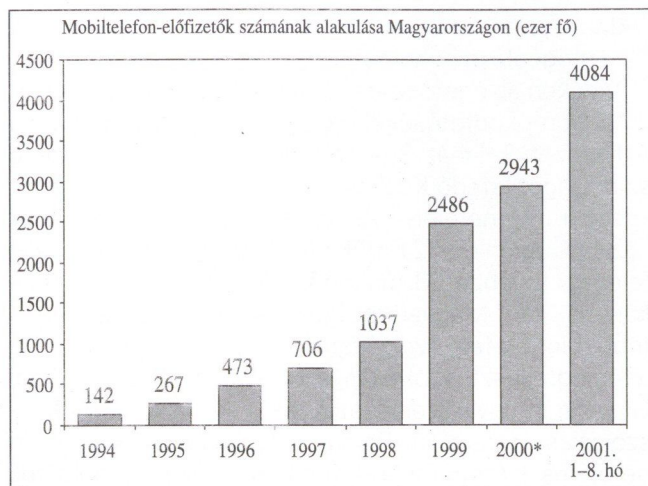
Forrás: Hírközlés-statisztikai évkönyv 1999, HIF.

Közép-Magyarország (Budapest és Pest megye) kiemelkedik a régiók közül, a lakosság 30%-a lakik ebben a régióban, és a jövedelmi helyzete is ennek a régióknak a legjobb. A rangsor tükrözi a régiók egymáshoz képesti jövedelmi helyzetét. Az EU-átlagot a legjobb ellátottságú régió sem éri el. Az elmaradott területek felzárkóztatására ezidáig nem tapasztalhatóak érzékelhető lépések, a csatlakozáshoz szükség lesz mind hatalmi, mind anyagi támogatásra a jövőben.

A vezetékes telefon helyettesítő terméke a mobiltelefon. Jelenleg Magyarországon 3 szolgáltató közül választhat a fogyasztó. A mobilpiacon óriási fejlődés tapasztalható az elmúlt évtizedben, az alábbi ábra jól mutatja a növekedést:

A felhasználók száma nem egyezik meg az előfizetők számával. Az előfizetők száma valamennyivel kevesebb, mivel az egyes szolgáltatók tarifáinak kedvezőbb kihasználásának érdekében előfordul, hogy egy vásárló több szolgáltatótól is igénybe veszi a szolgáltatást, és mindig a számára legkedvezőbb hálózaton telefonál. Másrészt sokan nem fizetnek elő, hanem előre fizetett kártyával használják mobilkészüléküket.





Forrás: Hírközlés-statisztikai évkönyv 1999, HIF.

\*becsült adat

A mobilcégek egyre fiatalabb vevőket céloznak meg, és kapcsolatot teremteni politikájuk azt sugallja, hogy akinek nincs telefonja, az nem is teljes értékű ember, nem tud megfelelően kommunikálni sem a magán, sem az üzleti életben. Az eddig megcélzott 15–35 éves korosztály piaca a felmérések szerint 100%-ban telített, ezért próbálják a terméket a 10–15 éveseknek eladni. A következő lépés valószínűleg az idősebbek bevonása lesz.

## Befektetés az emberekbe és az információs jártasság megszerzésébe

Ez talán a legösszetettebb terület, ahol számos feladat megoldásra vár. A szolgáltatók és a kormányzat részéről folyamatos és változatos kommunikációra lenne szükség, hogy az információs társadalom termékeit megismertessék a potenciális felhasználókkal. A termékeket nem elég megismerni, a használatukat is meg kell tanítani/tanulni, különben a termékeket nem lehet eladni, a felhasználókat nem lehet rendszerbe integrálni. A különálló felhasználók nem képeznek automatikusan hálózatot, a csatornákat működtetni kell.

A párbeszéd hatékony formája a média lenne, lehetne. Az újságok, a rádió, a televízió sokszínűen és változatos formában informálhatná a széles rétegeket. Megvizsgáltam Magyarországon legolvasottabb napilap-

ját, mely országosan hozzáférhető, valamint egy hetente megjelenő specifikáltabb gazdasági lapot, hogy mennyiben foglalkoznak a távközléssel, az internettel (2001. május havi lapszámok).

A Népszabadságban az újság terjedelméhez viszonyítva igen alacsony a távközléssel foglalkozó cikkek száma, ezeknek is több mint fele gazdasági tartalmú hír, ami nem sokban segíti elő a széles rétegek gyakorlati tájékozódását. A Figyelő c. lap jellegéből adódóan túlnyomó részt a gazdasági hírekről ad tájékoztatást.

A televíziós csatornák jelenlegi műsorrendjükből nem, vagy alig foglalkoznak információs témákkal, az országosan fogható TV-csatornákon a heti műsorrendben mindössze 150 perc jut infokommunikációs műsorokra.

A közszolgálati csatornák egyáltalán nem foglalkoznak a témával, ami érthetetlen, mivel ez a kormány egyik fő eszköze a tájékoztatásra. A távközlés jelenléte a médiában jellemzően a vezetékes és a mobilszolgáltató vállalatok reklámjaiban teljesedik ki.

A kormány információs stratégiája kiemelten fontos társadalompolitikai célnak tekinti a sérültek, a roma kisebbség és a munkanélküliek csoportját; az idősek és a kistelepülések lakosai a 2. csoportba tartoznak. A jelenlegi társadalomnak problémát jelent az idősebb korosztály hasznos foglalkoztatása. A nyugdíjas réteg eltartása egyre növekvő terhet jelent a társadalom aktív tagjai számára. Ha az idősebbeket nem vonjuk be az átalakulásba és nem vehetnek részt az újfajta kommunikációban, elszigetelődésük felgyorsul, a társadalom végleg kettészakad. Ma már minimális követelmény egy állás elnyeréséhez a felhasználói szintű PC-ismeret, számos helyen az internet ismerete is. Amennyiben lehetővé tesszük az otthoni számítógép-használatot az idősebb rétegek számára, alapot teremtünk a felzárkózásra, az újabb technológiák használatára is, mellyel megvalósulhatna mindenki részvétele-bevonása a tudásalapú gazdaságba.

A Mareco Piackutató Kft. Target Group Indexe (TGI) által a 14–69 éves magyar lakosság körében 1999-ben végzett mintavételes felmérés szerint 500 ezer háztartásban volt személyi számítógép, ami a kapcsolódó statisztikák szerint 1 395 000 ember számára tette lehetővé az otthoni számítógép-használatot (a lakosság 14%-a), s közülük mintegy 170 ezren interneteznek otthonról.

Az USA-ban 1995-ben a lakosság 29%-a, 1997-ben 42%-a, 1999-ben 54%-a rendelkezett otthon PC-vel. A

| Cikk témája                   |                       | Magyarország |             |           |             |
|-------------------------------|-----------------------|--------------|-------------|-----------|-------------|
|                               |                       | Népszabadság |             | Figyelő   |             |
|                               |                       | db           | %           | db        | %           |
| <b>Távközlés</b>              |                       | 16           |             | 33        |             |
| Ebből:                        | gazdaság, technológia | 8            | 32%         | 30        | 56%         |
|                               | egyéb                 | 8            | 32%         | 3         | 6%          |
| <b>Internet</b>               |                       | 7            |             | 20        |             |
| Ebből:                        | gazdaság, információ  | 5            | 20%         | 19        | 35%         |
|                               | oktatás               | 2            | 8%          | 1         | 2%          |
| <b>Információs társadalom</b> |                       | 2            | 8%          | 1         | 2%          |
|                               |                       | <b>25</b>    | <b>100%</b> | <b>54</b> | <b>100%</b> |



használat gyakorisága azonban a vizsgált időszakban rendre 26-30-29% volt, ami az aktivitás csökkenését jelenti.

## Az internethasználat elősegítése

Az információs társadalom fejlődésének egyik hordozója az elektronikus kereskedelem (e-kereskedelem), melynek használata feltételezi a számítógép, internet-kapcsolat és információs tudás meglétét. Az e-kereskedelemnek két nagy csoportját különböztetjük meg, a B2B (vállalatok közötti) és B2C (vállalat és fogyasztó közötti) típust.

Elsőként a **B2B piac** jött létre, létrehozásának célja az eladások és vásárlások költségeinek csökkentése, a tranzakciós ciklusok rövidítése és az információk hatékonyabb megosztása. 1998-ban a B2B tranzakciók értéke elérte a 145 Mrd USD-t a világban. 2000-ben ez az érték 2,9 billió USD volt, jellemzően észak-amerikai, európai és ázsiai-csendesóceáni forrásokból. Hazánkban ilyen B2B piac a Marketline elektronikus piactér, egyelőre a hosszú megtérülési idő miatt csak a nagyobb vállalatok engedhetik meg a kereskedelem eme formáját. Híreink szerint a magánhálózatokon és a virtuális magánhálózatokon viszont a vállalatok belső kereskedelme és a beszállítói kapcsolatok már széles körben elterjedtek.

A **B2C piac** forgalma egyelőre nagyságrendileg kisebb. Hazánkban az elektronikus kereskedelem, azon belül a fogyasztói kiskereskedelem 1999-ben indult, ekkor 160 millió forint volt a forgalom (ugyanezen időszakban az USA-ban 20,5 Mrd USD, Európában 5,4 Mrd USD volt a forgalom). A rendelhető áruk választéka egyre nő. Bár a fogyasztók bizalmatlanok még a vásárlás eme formájával szemben, aki mégis ezt a vásárlási formát választja, leginkább műszaki cikkeket, könyveket, zenehordozókat vesz. A magyar lakosság kb. 10%-a használja rendszeresen az internetet, jellemzően a fiatalabb korosztály, amely még nem fizetőképessé a piac szempontjából. Az internet gyorsabb ütemű terjedését leginkább a magas telefontarifák gátolják. A hazai e-kereskedelem fejlődését nehezítő magas távközlési díjak mellett a postai vagy más vállalkozások szállítási költségei is fékezően hatnak. A vásárlói bizalom erősítéséhez kedvező szabályozási, jogi, infrastrukturális és pénzügyi környezetet kell teremteni.

Az **elektronikus kormányzás**, egészségügy gyerekcipőben jár, tulajdonképpen kimerül az önkormányzatok és egészségügyi intézmények honlapjában, ahol az alapvető információkon kívül más ritkán található, nincs lehetőség ügyintézésre.

## Lehetséges megoldások a szélesebb körű és hatékonyabb kommunikációra

A televízión keresztül igen széles rétegekhez lehet eljuttatni üzeneteket, azonban vigyázni kell, mert a sze-

lektív figyelem miatt az üzenetek nem biztos, hogy elérik a megcélzott szegmenst.

Vidéken az égető számítógép- és internethiányt a *teleházak* működtetésével próbálja a kormány enyhíteni. A Nemzeti Teleház Stratégia egyik fontos célkitűzése az országot lefedő KÖZHÁLÓ megvalósítása (ingyenes közcélú internetelés és vonalhasználat) a teleházak bázisán. Jelenleg 221 működő, 159 fejlesztés alatt álló teleház, továbbá 38 működő, 52 fejlesztés alatti telekunyó van Magyarországon. A működő teleházak több mint 50-féle szolgáltatást nyújtanak egyebek közt a térségfejlesztés, oktatás, szociális gondoskodás, foglalkoztatás, civil szervezetek és a kisvállalkozások ki-  
szolgálása területén. Példák a szolgáltatásokra: internetelési lehetőség, elektronikus levelezés a polgárok számára, közhasznú tájékoztatás, ügyviteli szolgáltatások, számítógépes munkák elvégzése stb.

Szükséges a szállítási, postai költségek csökkentése (pl. tömeges szállítás), a távközlési díjak mérséklése és az információs tudásbázis szélesítése.

A *helyi önkormányzatok* segítségével sokban javítani lehetne a lehetőségek bemutatását. Vidéken, még a nagyobb városokban is az emberek nagyfokú bizalmatlansága tapasztalható minden újjal szemben. A népesség alacsonyabb iskolázottsága, az idegen nyelvek ismeretének hiánya óriási akadály az új eszközök alkalmazásának megtanulásában és használatában. A problémát nem lehet csupán számítógépek ajándékozásával megoldani, az igényt is kívülről kell feléleszteni, mivel jellemzően nincs meg a vidéken élő emberekben az igény az információs társadalom által nyújtott termékekre/szolgáltatásokra, az életvitelük a környezetben elfogadott és évtizedek óta gyakorolt szokásokon alapul.

A falvakban a polgármester és a lakók között családi-as a kapcsolat; amennyiben a vezetők bizalmát sikerül megnyerni, már jó úton haladunk a helyi lakosság elérésében. A számítógép és az internet a vidéken élők életét is megkönnyítené a mindennapokban, a gazdálkodásban, a közösségi kapcsolattartásban, a jóléti szolgáltatásokban. Az alacsony jövedelemmel rendelkezők csak akkor tudják igénybe venni az informatikai szolgáltatásokat, ha a kormány anyagilag támogatja az infrastruktúra megteremtését és az üzemeltetést. Az önkormányzatok működése általában alulfinanszírozott, kerülnek a bevételt nem hozó tevékenységeket, így a kormányzatnak kell tudatosítania ennek a területnek a kiemelt fontosságát és finanszíroznia a rendszer elterjesztését.

### Irodalom:

1. [www.ittk.hu/infini](http://www.ittk.hu/infini)
2. Dataquest
3. Arbitron
4. [www.hif.hu](http://www.hif.hu)
5. [www.telehaz.hu](http://www.telehaz.hu)



# A rejtjelző rácsok születése

## Girolamo Cardano

DÉNES TAMÁS

matematikus

Sok szempontból aktuális Girolamo Cardanora (1501. szept. 24.–1576. szept. 21.) emlékezni napjainkban, amikor éppen 500 éves születésnapját ünnepeljük.

Cardano korának, a reneszánsznak kiváló képviselője, igazi sokoldalú gondolkodó. Nem csupán reneszánsz polihisztor volt, de életében megjelent 131 könyvével és 111 kéziratban hátramaradt művével valószínűleg bekerülhetne a rekordok könyvébe is. Teljesítményét növeli és egyben a reneszánsz gondolkodás sokrétűségét jól tükrözi, hogy eme tekintélyes mennyiségű írásmű hány tudományterületet ölel fel.

Behatóan tanulmányozta a csillagászatot, a fizikát, a sakk és a szerencsejátékok elméletét (a valószínűségszámítás úttörője volt), egész életében orvosi praxist folytatott és természetesen előadásokat tartott az orvostanhallgatóknak. A test gyógyítása mellett foglalkozott a lélek „gyógyításával” és a halál problémájával, melyek keverékeként tanulmányozta a „lélek halhatatlanságát”. Behatóan elemezte Néro és Szókratész munkáit, valamint az erkölcs, a bölcsesség, a zene és más művészetek törvényszerűségeit. Tanulmányozta a kimeríthetetlen fizikai világot, valamint minden, emberrel kapcsolatos jelenséget, mint például a belső szervek, a fogak, az idegrendszer vagy az álmok.



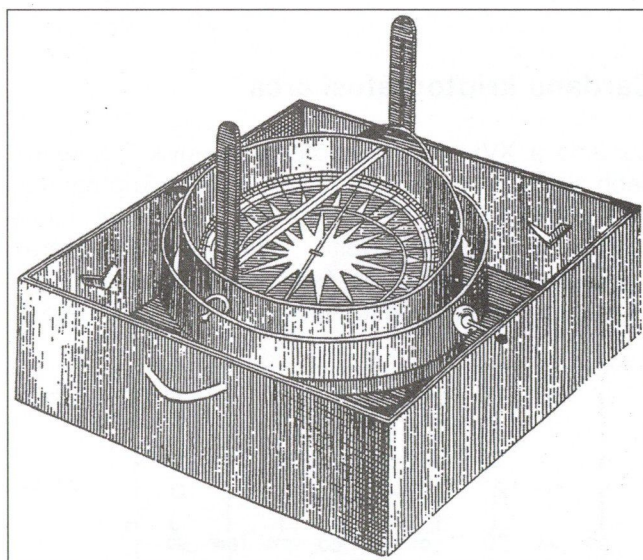
Éppen ezért érdekes (és egyben szomorú), hogy az utókor számára Cardano nevéhez többnyire csak a harmadfokú egyenlet róla elnevezett megoldóképlete társul, amely ráadásul a tudománytörténet egy máig vitatott kérdése. 1545-ben megjelent könyve, az *Ars magna sive de regulis algebraici* (Nagy művészet, avagy

az algebrai szabályokról) ugyanis képleteket tartalmaz az általános alakú harmadfokú egyenlet gyökeire, mégis a mai napig kétséges, hogy ezeket a képleteket valóban ő fedezte-e fel.<sup>1</sup>

Kevés olyan, majd fél évezredes műszaki találmány van, amely korunk hétköznapijaiba szinte változatlan formában beépült, Cardano előtt ezért mindenképpen meg kell hajolnunk. A „cardan” (méginkább „kardán”) ismerős minden autósnek. A kardán a vizekről „jött” a szárazföldre: 1530 körül, a hajózás fénykorában, a hullámokon dobálódzó hajók tájoló műszereit stabilizálni kellett. Ezt a feladatot oldotta meg Cardano új felfüggesztési rendszerével, melyről saját műveinek egyiké-

ben sem található részletes leírás. Az 1. ábra egy korabeli hajózási kézikönyvből származik.

Napjaink autóiba millió és millió példányban építik be az egész világon a „cardan”-nak (kardáncsukló, kardántengely) nevezett alkatrészt, amely életünk nélkülözhetetlen részévé is vált. Talán érdemes ezt a fél évezre-



1. ábra Cardano-felfüggesztés egy tájolóban (hajóiránytű)

<sup>1</sup> A matematikátörténészek szerint egy bizonyos Scipione del Ferro (1465–1526) megtalálta az általános alakú harmadfokú egyenlet megoldását, melyet közzétett kollégáival. Ez 1515 körül történhetett, amikor Itáliában gyakran tartottak matematikai versenyeket. Ferro egyik kollégája azt javasolta Niccolò Tartagliának (1500–1557) akkori nagy képzettségű matematikusnak, hogy oldjanak meg harmadfokú egyenleteket. Tartaglia a kijelölt határidő előtt megoldotta az egyenleteket, módszerét azonban titokban tartotta. Cardano kitaró érdeklődésére elmondta neki a megoldást, de megeskette, hogy hallgat róla. Cardano azonban nem tartotta meg esküjét, és 1545-ben az *Ars magna*-ban ismertette a harmadfokú egyenlet megoldásának módszerét. Így kezdődött a heves, ádáz vita Tartaglia és Cardano között, amelynek végére a matematikátörténet a mai napig nem tudott pontot tenni.



denként egyszer előforduló pillanatot kihasználni arra, hogy Cardano eme rejtett, mégis mindennapi aktualitását nevével és képével összekapcsoljuk.

Sajnos nem csupán munkássága, de szélsőségesen viharos élete is kivívhatná helyét a rekordok könyvében. Cardano megismerte a nyomort és a pompát, bejárta a világot, volt egyetemi tanár, megfordult palotákban és börtönökben is. Kilábolt a pestisből és látta fia kivégzését, míg másik fiának büntetésből saját kezűleg vágta le a fülét. Önéletírásában így ír életének négy legfájóbb csapásáról:

„Az első a házasságom volt, a második fiam keserű halála, a harmadik a bebörtönöztetésem, míg a negyedik és talán legfájdalmasabb, legkisebb fiam természetete.”

Megjósolta, hogy hetvenöt évesen fog meghalni, és a hátramaradt szóbeszéderek szerint, hogy jóslata beteljesedjék, éhhalállal emésztette el magát. Pontosan tudta, hogy korának egyik legszívesebb egyénisége, amint ez kiderül önmagáról írt jellemzéséből:

„Természetemnél fogva filozófusi és a tudományokra hajlamos elmével rendelkezem. Szellemes vagyok, elegáns, illedelmes, kéjsóvár, vidám, ájtatos, hű, a bölcsesség barátja, megfontolt, vállalkozó szellemű, kíváncsi, szolgálatkész, versengő, találékony. Sajátmagam szereztem műveltségemet, ravasz vagyok és kegyetlen, járatos a tudomány titkaiban, józan, dolgos, mélabús, álnok, áruló, varázsló, mágus, boldogtalan, nem szeretem felebarátaimat, a magányosságot kedvelem, ellenszenves, szigorú, féltékeny, tréfacsináló, rágalmozó, talpnyaló, szeszélyes vagyok. Lám, milyen ellentmondások vannak jellememben és magatartásomban!”

## Cardano kriptográfusi arca

Cardano a XVI. századi kriptográfia egyik legjelentősebb alakja. Erről keveset tudunk, mert a kriptográfiát (a titkosírást vagy rejtjelzést) természeténél fogva „zárt ajtók mögött” művelték. Uralkodók, hadvezérek szigorúan bizalmas levelezését bonyolították különböző módszerekkel titkosított levelekkel. Cardano nem írt

|      |      |      |      |      |      |      |      |      |       |
|------|------|------|------|------|------|------|------|------|-------|
|      |      |      |      |      |      |      |      |      |       |
| 1    | 2    | 3    | 4    | 5    | 6    | 7    | 8    | 9    | 10    |
|      |      |      |      |      |      |      |      |      |       |
| 10   | 20   | 30   | 40   | 50   | 60   | 70   | 80   | 90   | 100   |
|      |      |      |      |      |      |      |      |      |       |
| 100  | 200  | 300  | 400  | 500  | 600  | 700  | 800  | 900  | 1000  |
|      |      |      |      |      |      |      |      |      |       |
| 1000 | 2000 | 3000 | 4000 | 5000 | 6000 | 7000 | 8000 | 9000 | 10000 |

3572.

7240.

12509.

2. ábra Cardano javasolt tömörített számírási rendszere a *De Subtilitate*-ből

önálló könyvet a kriptográfiáról, de e tárgyban született gondolatait, módszereit két igen népszerű könyvébe beépítette.

Az első könyv 1550-ben jelent meg, címe „*De Subtilitate*” (A ravaszság), amelyben gazdagon illusztrált tudományos ismeretek mellett részletesen tárgyalta, hogyan lehet a vakokat olvasni és írni megtanítani a tapintásra támaszkodva. Ugyanebben a könyvében tette közzé meghökkentő javaslatát „sűrített számírási rendszeréről”, melynek az eredeti könyvből származó illusztrációját a 2. ábán láthatjuk.

Az olvasók nagyon kedvelték Cardano anekdotikus stílusát és sokszor bizarr illusztrációit, így hat évvel később megírta a második kötetet, melynek címe „*De Rerum Varietate*” (A változatosság gyönyörűségéről).

Mindkét könyvet több nyelvre lefordították és egész Európában terjesztették. E két kötetben Cardano összefoglalását adja a megelőző 3000 év és kora kriptográfiájának. Mindezek után leírja saját, az addigiakhoz képest új rejtjelzési eljárásait.

A fátylatávíró, az ókort messze megelőző hírközlési módszer adhatta Cardanónak az ötletet, hogy megalakítsa a táblázaton alapuló titkosítás két nagy családját. Az egyik az „intervallum-rejtjelzés”, amelyben a titkos üzenet a betűk közötti távolságokon alapult, ami a modern sztegonográfia kezdeti lépése [3]. A „szöveg a szövegben” sztegonográfiai eljárás, amely rejtjelzés nélkül, úgynevezett fedőszövegbe csomagolva rejtje el a titkos üzenetet, napjainkban ismét előtérbe került. A digitális technika soha nem látott perspektívákat nyit eme módszereknek, hisz lehetővé teszi, hogy nem csupán fedőszövegbe, hanem digitalizált álló vagy mozgóképbe, vagy akár digitalizált hanganyagba rejtve továbbítsunk titkos üzeneteket.

Igen sajnálatos, hogy Cardano ötlete éppen a terrorizmus kezében éli reneszánszát, ezzel kijátszva a rejtjelzésre kihegyezett „nagy füleket”, azokat a földi és műholdas lehallgató rendszereket, amelyek több milliárd dolláros befektetésekkel épültek ki. A módszerek a hamisítás elleni védekezésben, digitális aláírások biztonságának növelésében és az információbiztonság egyéb területein is használhatók a köz javára (lásd [4],[7],[8],[10],[12]).

## A Cardano-rács

A másik, táblázaton alapuló módszer az úgynevezett Cardano-rács, melynek megismeréséhez idézzük fel magának Cardanónak a szavait:

„Végy két azonos méretű pergamenlapot, és azonos vonalak mentén készíts kivágásokat különböző helyeken. Ezek a kivágások legyenek kicsik, de mégis legalább akkorák, mint az ABC nagybetűi. Az összes kivágásokba összesen 120 betűt lehessen elhelyezni. Az egyik pergamenlapot majd a levelező társadnak adod. Amikor alkalom adódik, először írd az üzenetedet olyan tömören, ahogy csak lehetséges, így az üzenet kevesebb betűt is tartalmazhat, mint amennyi a kivágott ab-



lakokban elhelyezhető. Amikor beírtad az üzeneted az egyik pergamenlapra, tedd ugyanezt a másikkal is. Ezután töltsd ki az első lapon az üresen maradt helyet úgy, hogy teljes mondatokra egészítsék ki a már ráírt szöveget. Ez a kitöltés úgy történjen, hogy a teljes szöveg stílusa és tartalma összefüggő és egységes legyen. Amikor a levelezőtársad megkapja a te üzenetedet, ráhelyezi a megfelelő kivágásokkal ellátott pergament, és így elolvashatja az üzenetet."

A Cardano-rács sikerét talán annak köszönheti, hogy egyszerű, de mégis fantasztikus változatosságot biztosít. Ekkora siker nagyon ritkán tapasztalható a kriptográfia történetében, hiszen az ismeretek állandó bővülésével a titkok megfejtésének technikája általában utoléri a titkosítók technikáját. Demonstrációként bemutatjuk a Cardano-rács egy modern alkalmazását, amikor az úgynevezett fedőszöveg egy mindenki által hozzáférhető napilap cikke lehet, így a fedőszöveg eljuttatása a címzetthez nem okoz problémát. A rácsrejtés további érdekessége, hogy az ablakokban nem csak egyedi betűk, hanem egy vagy több szó is szerepelhet, amint azt a 3. ábra mutatja.

Népszabadság, 2001. október 13.  
(Budapest melléklet)

Csepel

Egész napos rendezvényt szervez a kerületi diákönkormányzat október 13-án, szombaton. Az eseményen – melyet a Csepel Plaza színpadán rendeznek – sport- és táncbemutatókkal, vetélkedőkkel, kézműves- és kozmetikai gyakorlatokkal, bűvészprodukciókkal, lufishow-val és villámkérdésekkel várják az érdeklődőket. Valamennyi program ingyenes.

napos

lufishow-val

ingyenes.

fedő-  
szöveg

Cardano-  
rács

3. ábra Cardano-ráccsal kiolvasható rejtett üzenet

Bár Cardano neve e téren nem vonult be a köztudatba, rejtjelző rácsa 450 éve fennmaradt, sőt még a szépirodalomban is találkozhatunk vele. Jules Verne *Sándor Mátyás* című regényében ilyen rejtjelző rács segítségével próbálják a titkos összeesküvést megszervezni.

A 4.a. ábrába Karinthy Frigyes saját, úgynevezett intarziáját írtuk be (az intarzia tulajdonképpen a „szöveg a szövegben” rejtés egy speciális formája). Így még érde-

kesebb, hogy a 4.b.–4.d. ábrák rácsait a 4.a. ábra szövegmatrixára helyezve egészen más rejtett szövegek olvashatók ki ugyanabból a fedőszövegből, azaz ugyanabban a szövegben mennyi különböző rejtett szöveg lehet elhelyezve (az ablakokban levő betűket balról jobbra és fentről lefelé összeolvasva, megkapjuk a rejtett szöveget).

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| M | A | G | Á | T | E |
| G | Y | É | G | I | K |
| A | R | I | N | T | I |
| F | R | I | G | Y | E |
| S | I | K | E | R | Ü |
| L | N | I | F | O | G |

4.a. ábra

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| M | A | G | Á | T | E |
| G | Y | É | G | I | K |
| A | R | I | N | T | I |
| F | R | I | G | Y | E |
| S | I | K | E | R | Ü |
| L | N | I | F | O | G |

4.b. ábra

A 4.a. ábrába beírt szöveg: „MAGÁT EGY ÉGI  
KAR INTI FRIGYE SIKERÜLNI FOG”

A 4.b. ábra rácsával kiolvasható rejtett szöveg:  
„MÁTÉ KINT INOG”

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| M | A | G | Á | T | E |
| G | Y | É | G | I | K |
| A | R | I | N | T | I |
| F | R | I | G | Y | E |
| S | I | K | E | R | Ü |
| L | N | I | F | O | G |

4.c. ábra

|   |   |   |   |   |   |
|---|---|---|---|---|---|
| M | A | G | Á | T | E |
| G | Y | É | G | I | K |
| A | R | I | N | T | I |
| F | R | I | G | Y | E |
| S | I | K | E | R | Ü |
| L | N | I | F | O | G |

4.d. ábra

A 4.c. ábra rácsával kiolvasható rejtett szöveg:  
„EGYÉK INGYEN”

A 4.d. ábra rácsával kiolvasható rejtett szöveg:  
„AGG KINT FIGYEL”

## A forgatórács

Cardano az előzőekben leírt egyszerű rácsképzési eljárás mellett (ablakok tetszőleges kivágása) megkonstruált egy másik rács-előállítási és -kitöltési módszert, a forgatórácsot. A forgatórács olyan eszköz, amely 90 fokként elforgatva ablakaival pontosan egyszer lefedi a hozzá tartozó betűmatrix összes mezőjét.

A rács ablakait úgy kell kijelölni, hogy elforgatáskor valamennyi ablak mindig más és más helyre kerüljön. Könnyen belátható, hogy a forgatórács előállításának alapvető kritériuma, hogy a rács mérete ( $n$ ) csak páros szám lehet, valamint a kivágható ablakok száma egyértelműen meghatározott, hiszen ahhoz, hogy az  $n^2$  betűmatrix-mező mindegyike a rács négy forgatása



során pontosan egyszer kerüljön lefedésre, pontosan  $\frac{n^2}{4}$  ablakra van szükség.

Ha a forgatórács mérete 6x6-os, akkor az előzők alapján 9 ablakot kell képeznünk úgy, hogy azok a forgatás fenti feltételeinek megfeleljenek. A forgatórács alkalmazását a fenti Karinthy-intarzián mutatjuk be, az 5. ábra rácsát felhasználva.

|   | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 |   |   |   |   |   |   |
| 2 |   |   |   |   |   |   |
| 3 |   |   |   |   |   |   |
| 4 |   |   |   |   |   |   |
| 5 |   |   |   |   |   |   |
| 6 |   |   |   |   |   |   |

5. ábra

|   | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 |   |   |   |   |   | M |
| 2 | A |   | G |   | Á |   |
| 3 |   |   |   |   |   | T |
| 4 |   |   |   | E |   |   |
| 5 |   |   | G |   |   |   |
| 6 |   |   | Y |   |   |   |

5.a. ábra Az 1.–9. betűk elhelyezése a rács alaphelyzetében.

|   | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 |   |   |   |   | G |   |
| 2 |   |   |   |   |   |   |
| 3 | I | K |   |   | A |   |
| 4 |   |   | R |   |   |   |
| 5 | I |   |   |   | N |   |
| 6 |   |   |   | T |   | I |

5.b. ábra A 10.–18. betűk elhelyezése a rács 90°-os elforgatásánál.

|   | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 |   | F |   | R |   |   |
| 2 |   |   |   | I |   |   |
| 3 |   |   | G |   |   |   |
| 4 | Y |   |   |   |   |   |
| 5 |   | E |   | S |   | I |
| 6 | K |   |   |   |   |   |

5.c. ábra A 19.–27. betűk elhelyezése a rács 180°-os elforgatásánál.

|   | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | E | F | R | R | G | M |
| 2 | A | Ü | G | I | Á | L |
| 3 | I | K | G | N | A | T |
| 4 | Y | I | R | E | F | O |
| 5 | I | E | G | S | N | I |
| 6 | K | G | Y | T | É | I |

5.d. ábra A 28.–36. betűk elhelyezése a rács 270°-os elforgatásánál.

Ezzel a betűmátrix mind a 36 mezője kitöltésre került, ezt a betűmátrixot küldjük a címzettnek.

Az 5.d. ábra betűmátrixát kapjuk eredményül, amelyet elküldünk a címzettnek, aki az 5. ábra rácsának birtokában el tudja azt olvasni. Példánkban külön érdekesség, hogy az így megfejtett szövegből a 4.a.-4.c. ábrák egyszerű rácsaival újabb rejtett szövegek olvashatók ki. Ezzel egyúttal arra is fény derült, hogy a Cardano-rácsok a sztegonográfia mellett rejtjelzésre is felhasználhatók.

## Cardano-rácsok Cardano után

A Cardano-rácsok történetének elmúlt 450 évében több újjászületésnek lehettünk tanúi. Pontosán Cardano „*Ars magna*”-jának megjelenése után 250 évvel, 1795-ben jelent meg Carl Friedrich Hindenburg német matematikus tanulmánya, melyet teljesen a rejtjelzésnek, ezen belül a rejtjelző rácsoknak szentelt. Azért nem úgy fogalmaztam, hogy a Cardano-rácsnak, mert (a tudománytörténetben nem szokatlan módon) Cardano nevét meg sem említi. Feltehető tehát a kérdés, hogy vajon Hindenburg tudott Cardano kriptográfiai munkásságáról? És ha ő nem ismerte Cardano rács-rejtjelző módszerét, akkor még indokoltabb e kérdés megfogalmazása Vernével kapcsolatban, aki egy évszázaddal Hindenburg után írta le fent említett regényében pontosan a forgató rácsot.

Tompítja a fenti kérdés élét, hogy Hindenburg nem csupán pontos leírását adta a Cardano-rácsnak, hanem bizonyos továbbfejlesztését is bemutatja. Ennek lényege, hogy ha a rács oldalait megjelöljük az *a, b, c, d* betűkkel, akkor a rácsforgatásokat úgy adhatjuk meg, mint e négy betű valamely sorrendjét (például: *abcd*, vagy *bdca*, vagy *cadb* stb.). Mivel a négy betű összes különböző sorrendjeinek száma 24, ez azt jelenti, hogy a különböző rácslefedések számát e módosított módszerrel 24-szeresére növelhetjük.

Ennél jóval nagyobb jelentőségű Hindenburg igen előremutató megállapítása, hogy a nyílt szöveget át lehet írni a betűkhöz rendelt sorszámmok bináris alakjára, s így a bináris számjegyek (0,1) lesznek a rácskeverés tárgyai. Ezáltal egy igen biztonságos keverést lehet elérni, továbbá ennek kivitelezése a bináris alapon működő számítógépek segítségével nagyon egyszerű. Érde-



kesség, hogy a rejtjelző rácsok megkonstruálásának problémája összefügg az úgynevezett bátyaproblémával, nevezetesen hogyan lehet egy sakktáblán nyolc bástyát úgy elhelyezni, hogy egyik se üsse a másikat. Ezzel eljutunk a matematika olyan modern területeihez, mint a latin négyzetek és a permutációs mátrixok elmélete és ezek alkalmazása a rejtjelző rácsokra. A kriptográfia szempontjából fontos, hogy a forgatórács biztonsága növelhető, ha a keverést esetleg ugyanazzal, esetleg másik ráccsal kétszer vagy többször elvégezzük.

Bármilyen mostohán bánt is Cardanóval a tudomány- és technikatörténet, gondolatai és általa a reneszánsz szelleme ma is mindennapjaink részét képezik.

### Irodalom

1. Dénes Tamás: Cardano és a kriptográfia. Középiskolai Matematikai és Fizikai Lapok, LI. évf. 2001/6.
2. Dénes Tamás: Biztonságos információ(s) társadalom? INFO-Társadalomtudomány, 53. szám 2001. augusztus
3. Dénes Tamás: Sztegonográfia. Rejtett információk rejtjelzés nélkül. Híradástechnika, 2001/8.
4. Dénes Tamás: Digitális ujjlenyomat. A dokumentumvédelem új korszaka. Magyar Távközlés, XI. évf. 5. szám, 2000. május
5. Dénes Tamás: Titok Tan avagy Kódtörő ABZ. Kriptográfia mindenkinek. Bagolyvár Könyvkiadó, megjelenés alatt
6. Carl Friedrich Hindenburg: Urchid der Reinen und Angewandten Mathematic herausgeben von Carl Friedrich Hindenburg. Leipzig, 1795.
7. S. Katzenbeisser–F. A. P. Petitcolas (Ed.): Information Hiding Techniques for Steganography and Digital Watermarking. Artech House Books, 2000.
8. Löfvenberg: Random Codes for Digital Fingerprinting. Linköping Studies in Science and Technology. Thesis No 749. Linköping, 1999.
9. Charles J. Mendelsohn: Cardan on cryptography. Scripta Math., 1938. 10. A. Pfitzmann (Ed.): Information Hiding. Proceedings of Third International workshop, IH'99 Dresden, Germany, Sept. 29. – Oct. 1., 1999.
10. A. Pfitzmann (Ed.): Information Hiding Proceedings of Third International Workshop, IH'99 Dresden, Germany Sept. 29. – Oct. 1., 1999.
11. Révay Zoltán: Titkosírások. Budapest, 1978, Zrínyi Katonai Kiadó.
12. G. J. Simmons: Identification of data, devices, documents and individuals. Proc 25th Annual IEEE Carnahan Conf. On Security Technology 1991, IEEE, New York, pp. 197–218.
13. Svékus Olivér: Titkosírások. 1989, Móra Ferenc Könyvkiadó.

## Hír

A Corning kibővített átszervezési tervet hirdetett meg, ami munkaerő-leépítésekkel és a termelés felfüggesztésével jár világszerte a fényvezetőszál-gyártó üzemek java részében.

E lépések eredményeképpen a Corning kb. 1 milliárd dollárnyi díjat remél elkönyvelni 2001 második felében, amelyből kb. 350 millió dollár a harmadik negyedévben kerül könyvelésre. A társaság becslése szerint a költségek kétharmada nem készpénz lesz.

Míg a társaság nem adott útmutatást a harmadik negyedévre vonatkozóan, a Corning várakozása szerint pro forma veszteséget fog elkönyvelni, a konszenzushány elemzői becslés szerint a részvényenkénti pro forma nyereség kettő és hat cent közé tehető.

A társaság azt is kijelentette, hogy a munkaerő csökkentés év végére elérheti a 12 000 főt – ez 50%-kal meghaladja a már bejelentett 8000 főt. A társaság alkalmazotti létszámának maximuma 2001-ben 43 000 fő volt.

A munkahelyek közül több mint négyszáz leépítésére a Corning Deeside-i (Észak-Wales) fényvezetőszál-gyárában kerül sor. A Corning az üzem év végi bezárását javasolja, mivel gyengül a fényvezetőszál iránti kereslet Észak-Amerikában és Európában.

Ez azonban nem az egyetlen, a Corning terveiben szereplő üvegszálüzem. A társaság további négy egysége közül háromban kívánja leállítani a fényvezetőszál-gyártást október végén. A termelés 2002-ben újraindul, amint javulnak az üzleti feltételek.



# Hírek

Egy hónappal azután, hogy a Sun Microsystems kezdeményezésére a világ 33 neves cége bejelentette a „Liberty Alliance” szövetség megalapítását, hogy nyílt megoldást fejlesszen ki és alkalmazzon a hálózati azonosítás kezeléséhez, több mint 2 ezer cég kért információt a szövetségben való részvétel feltételeiről. A Liberty Alliance” kulcsfontosságú pontra tapintott, amelyet igen sok, különféle területeken és iparágakban tevékenykedő szervezet lát kritikus tényezőnek. Ez a megoldás azt jelentené, hogy megvalósítható az egy pontos bejelentkezés, a decentralizált hitelesítés és a nyílt autentikáció bármely, az internetre csatlakozó eszközről, a hagyományos asztali számítógépektől és mobiltelefonoktól kezdve egészen a TV-kig, autókig, hitelkártyákig és pénztárgépekig. Bármely szervezet, amely érdeklődik a Liberty Alliance Project iránt, a részleteket a [www.projectliberty.org](http://www.projectliberty.org) címen találhatja meg. A Liberty Alliance Project a tervek szerint megkezdte egy, az üzleti és a személyes adatok kezelésére, a fogyasztói elterjedésre, továbbá a technológiai fejlődésre vonatkozó terv elkészítését.



A Sun™ ONE (Sun Open Net Environment) szotverplatform az „on-demand” típusú szolgáltatások kiépítésére szolgál. Az „on-demand”, azaz az igényeken alapuló szolgáltatások azt jelentik, hogy az információ, az adatok és az alkalmazások bármikor, bárkinek, bárhol és bármilyen eszközön keresztül biztosíthatók. A ONE a meglévő rendszerek egyszerűsítésével építi a szolgáltatási infrastruktúrát. A Sun Forte for Java Tools, az iPlanet Application, Web és Integration szerverei mind-mind támogatják az XML-t és a SOAP-ot, vagyis a meglévő rendszerek összekapcsolhatók a webes szolgáltatások világával. A Java Web Service Designer az Enterprise JavaBeans-metódusokat XML-műveletekbe „csomagolja”, és lehetővé teszi, hogy webes szolgáltatásokká szervezzük őket. Az iPlanet Portal Server szolgál a vizuális megjelenítés és az integráció eszközeül.



Az Infineon Technologies megkezdte a 0,14 mikron technológiájú 256 megabites DRAM szériagyártását, valamint elindítja az 512 megabites DRAM-áramkör mérését. A 0,14 mikronos gyártási technológia – amely 18 százalékkal kisebb struktúrát használ, mint a cég eddigi legkisebb, 0,17 mikronos technológiája – 30 százalékos költségcsökkenést eredményez chipenként. A 0,14 mikronos technológia átvitele 200 mm-ről 300 mm átmérőjű szilíciumszeletekre további 30 százalékkal csökkentheti a költségeket. A drezdai gyárban jövő év tavaszán kezdik meg a 0,14 mikronos, 300 mm-es gyártást.



Az Ericsson Magyarország által a PanTel Rt. részére üzembe helyezett AXE központ kapcsolatát biztosítja a PanTel IP-hálózata és a hagyományos távbeszélőrendszerek között.

Az AXE rendszer alkalmassá tehető arra, hogy a hagyományos, áramkörkapcsolt fogalom vezérlését adatkommunikációs (csomagkapcsolt) hálózaton végezze. Ezzel elkerülhető a szolgáltatásorientált dedikált hálózatok kiépítése. Másik nagy előnye, hogy a távközlési szabványok maximális támogatása révén biztosított a más rendszerekkel való együttműködés, ami a biztonság és a jövőállóság záloga az operátorok számára.

Az AXE segítségével a fejlődés két útja nyílik meg. Az egyik, Ericsson kínálja lehetőség az, hogy az Engine koncepció részeként az AXE egy speciális szoftver segítségével telefon-szerver funkciót lát el.

A másik irány az ún. Open Network Gateway (ONG) koncepció irányába való elmozdulás, ami a PSTN/IP konvergencia lehetőségét teremti meg.

Jelenleg a világ 136 országában 11 ezer AXE központ működik, ezek 120 millió vezetékes és 170 millió mobilvonalat kezelnek.



# Arckép a közelmúltból: Kozma László

FEKETE SZILVESZTERNÉ

*Jövőre lenne 100 éves Kozma László (1902–1983) akadémikus, a Villamosmérnöki Kar volt dékánja, a Vezetékes híradástechnikai Tanszék egykori vezetője. A jövő évi megemlékezések előfutáraként cikkünk egyszerre szól fiatalabb és idősebb olvasóinkhoz. A fiatalabbak megismerhetik Kozma professzor munkásságát, az idősebbek pedig, akik ismerték, bizonyára szívesen idézik fel e cikk alapján tanáruk, példaképük emlékét. A jövő őszi emlékünnepeig érdekes részleteket gyűjtünk össze azzal kapcsolatban, hogyan hatott napjaink távközlési kutatásaira, a korszerű távközlési szolgáltatások fejlesztésére munkássága, amelynek sok eredményét ma is tapasztaljuk vagy használjuk. Reméljük, cikkünk sokakban ébreszt érdeklődést Kozma professzor pályafutása és életműve iránt.*

Kozma László az Osztrák-Magyar Monarchia állampolgáraként született, és hosszú élete során mintegy kilenc rendszerváltást ért meg. Élete nem egyéni sors volt csupán. Amit egy ember átél, az sok esetben közösségi sors is. Hazája tragikus történelmi korszakai beárnyékolták életét, megszakították szakmai munkásságát. Az ellenséges társadalmi erőkkal a tudós ember fölényével nézett szembe. Mindig nagyobb közösségekben gondolkodott, amelynek műszaki előrehaladásáért saját szakterületén oly sokat fáradozott.

Miskolci középiskolai éveitől kezdve fel az érdeklődése a műszaki tudományok iránt, ezért elhatározta, hogy érettségi után jelentkezik a Budapesti Műszaki Egyetemre (1921). Ám keserű leckét kapott a 20-as évek magyar társadalmi valóságától: az 1920-ban bevezetett „*numerus clausus*”-ra hivatkozva elutasították felvételét. Más megoldást keresett ekkor, villanyszerelőként helyezkedett el az Egyesült Izzóban. A gyár a magyar ipar egyik fellegvára volt, kutatólaboratóriumában nagyszerű mérnökök és fizikusok dolgoztak; köztük Bródy Imre is, aki a kriptontöltésű lámpák alapelvét ismertte fel, s munkatársaival a kripton olcsó ipari előállításának módszerét is kidolgozta. Szellemi teljesítményük ragyogó példaként állt a fiatal villanyszerelő előtt, aki munkája mellett angolul tanult, hogy a külföldi szakirodalmat eredetiben olvashassa. Tehetséges és szorgalmas, így jellemezték őt a gyár vezető szakemberei, akik ösztöndíjat adtak össze részére, hogy továbbtanulhasson. Kozma László 1925-ben kezdte el tanulmányait a brünni német nyelvű Műszaki Egyetemen, ahol 1930-ban villamosmérnöki oklevelet szerzett.

A fiatal mérnököt az antwerpeni Bell Telephone amerikai cég szerződtette, amely a 30-as években Európa legnagyobb, telefonközpontokat előállító vállalata volt. A kezdeti évekre így emlékezik vissza Kozma László: „...pár évig rutin jellegű áramköri tervezési

munkákkal bíztak meg. Fokozatosan bekapcsolódtam az új jellegű fejlesztési munkákba, részt vettem számos európai ország (Svájc, Belgium, Hollandia, Olaszország stb.) országos automatikus telefonhálózatának, az ún. távválasztásának kidolgozásában, közreműködtem továbbá új típusú telefonközpontok (7E és MA) ki-fejlesztésében. Mindezen munkáimmal kapcsolatban 1934 és 1938 között a vállalat több mint 25 szabadalmat jelentett be, amelyen feltalálóként én egyedül vagy társakkal együtt szerepeltem. Így elég jó „nevem volt”, és e körülmények alapján dönthetett a gyár műszaki igazgatója, hogy engem bízott meg a számológép fejlesztési munkákkal, ami akkor nagy megtiszteltetést jelentett számomra... Hogy miért, mi indokolta ezt az igényt, énnekem erről fogalmam sem volt! Ma persze tudom, hogy a háborús felkészülés már javában folyt, és a lövedékek (rakéták) irányításához, illetve elhárításához volt szükség elektromos számológépre. ...Én nagy ambícióval, de kis meggyőződéssel fogtam munkához” – írta Mérnöki tevékenységem az elektronikus számítógépek „őskorában” című cikkében [1]. A fejlesztéshez csak olyan alkatrészeket használhatott fel, amelyeket a „problémabeadó” és az „eredményt kiadó” készülék kivételével a telefonközpontokban is használtak.

1938 ősze és 1942 között három elektromos számológépet fejlesztett ki, amelyekre az antwerpeni gyár 10 szabadalmat jelentett be. A „tapogatózó kísérletnek” minősített első gépe (No1) decimális összeadó egységgel rendelkezett, kivonni és szorozni tudott, osztani nem. Sorrendkapcsoló gépeket és jelfogókat tartalmazott. Egyik hátránya lassúsága volt (az összeadás 1-1,5 mp-ig tartott), a másik az, hogy 16 vezeték kellett ahhoz, hogy a felhasználói készülékhez csatlakozzon, ami a sokfelhasználós kialakítást nehezítette. 1939 telén már működött, 2. elektromos kalkulátora, amely-nél sikerült kiküszöbölnie az első számológép hátránya-



it. „...Elhagytam a sorrendkapcsolókat, és csak egyfajta kis 11 pontos forgógépet használtam, amelyek a mindenkori részeredményt tárolták. Ez a számológép is decimális rendszerben dolgozott, és tudott osztani. A fő újítás a No1-gyel szemben az volt, hogy összeállítottam jelfogókból egy egyszeregy áramkört, amely megadta egyszerre a soron következő szorzónak és a szorzandó valamennyi számjegyének szorzatát 10-esekben és 1-esekben. Így a szorzás ideje lecsökkent két összeadás idejére.” [1] További újítása a vezetékek számának csökkentése volt, amivel többfelhasználós elrendezésűvé vált a készülék.

Tragikus történelmi körülmények között került sor a No3-as számú kalkulátor megépítésére, amelynél a 2-eshez képest csak kisebb áramkörti módosítást hajtott végre Kozma László. 1940 tavaszán a II. világháborút kirobbantó németek megtámadták Belgiumot, elfoglalták Antwerpent. A Bell Telephone élére német ellenőrző tiszt került. 12 csatornás vivőhullámú berendezések mellett különböző telefonközpontokat kellett nagy mennyiségben gyártaniuk a németek számára. A belgák ellenálltak, és szabotálták a termelést. A gyárban a németek háta mögött titokban még 1941 végéig folytak az elektromos számológéppel kapcsolatos fejlesztési munkák, de éppen ezek katonai jelentősége miatt a cég igazgatója azt leállította.

A szövetségesek győzelmei és várható partraszállásuk arra készítette a németeket, hogy hatalmas ember-tömeget mozgósítsanak az „atlanti fal” megépítésére az általuk megszállt országokból. Kozma László ekkor úgy döntött, hogy hazatér. 1942 végén itthon mérnöki állást nem kapott. Első munkahelye, az Egyesült Izzó alkalmazta műszerészként. Nem zúgolódott, pedig többször behívták munkaszolgálatra, átélte a deportálás összes szörnyűségét. 1945 augusztusában betegen tért vissza Budapestre. A fővárosban szétbombázott házak, lerombolt hidak látványa fogadta, de a szorgos embereké is, akik a háború ütötte sebeket igyekeztek eltüntetni.

Bár a Bell Telephone cég visszahívta egykori fejlesztőmérnökét Antwerpenbe, Kozma László úgy döntött, hogy szakmai tudását a hazai távbeszélő-hálózat helyreállítására és fejlesztésére fogja fordítani. 1945 és 1949 között a Standard Villamossági Rt. (későbbi BHG Híradástechnikai Vállalat) műszaki igazgatójaként hatalmas energiával látott neki a maga elé tűzött feladatok megvalósításának. Munkásságát rangos kitüntetéssel, a Kossuth-díj I. fokozatával jutalmazták. (1948). 1949-ben egyetemi tanárnak nevezték ki, és megbízták az újonnan alapított Vezetékes híradástechnikai Tanszék vezetésével. A Híradástechnika c. lapban a telefónia témakörében megjelent cikkei szakmai körökben is egyre ismertebbé tették nevét, joggal érezhette úgy, hogy végre itthon is beérkezett.

Tudományos pályája 1949-ben ismét megtört, sőt élete is veszélybe került. Koholt vádak alapján letartóztatták és 15 évi börtönbüntetésre ítélték a hírhedt Standard-perben. „Börtönévei alatt is dolgozhatott, tagja volt annak az elítéltekből álló szakmai elit csoport-

nak, amely a hivatalosan áltudománynak bélyegzett kibernetika lehetőségeit kutatta, és mint építőiroda fejlesztési terveket, előrejelzéseket is készített.” [5]

1954-ben szabadult, rehabilitálták, visszakapta tanári állását, és nekiláthatott a hazai mérnökképzéssel kapcsolatos pedagógiai tervei megvalósításához.

A villamosmérnöki oktatásba bevezetett kapcsolástechnika tantárgy gyakorlati szemléltetését kívánta biztosítani egy digitális programvezérlésű számítógép segítségével, amelynek terveit már börtönévei alatt elkészítette. A gép kifejlesztéséhez az Akadémia támogatását is sikerült megszereznie. A kivitelezés feltétele az volt, hogy hazai, a telefoniparban gyártott és használt jelfogókból kell megépítenie a készüléket, ami teljesen egyedi rendszertechnikai és áramkörti tervezésre ihlette. 1957 elejére készült el az áramkörti tervezéssel, majd a következő évben befejeződtek a kivitelezési munkák is, megkezdődhetett a konstrukció vizsgálata. Így jött létre az MESZ 1, az első hazai fejlesztésű digitális számítógép, amely „2000 db (10 féle) jelfogóból épült fel, az adatokat bebillentyűzték, az eredmény kiírására egy írógépet alakítottak át, a billentyűt elektromágnesek húzták meg. A fogyasztása 600-800 W volt. A programot kézzel lyukasztott lapon tárolták. A gép egycímű utasításokat használt, egy lapra 45 utasítást fért (5 bit a műveleti kód, 7 bit az adat címe), ezenkívül 9 konstans. A jelfogó adatbázisában 12 db 27 bináris számot lehetett tárolni. A gépben decimális/bináris és bináris/decimális átalakító volt.” [3]

A berendezés szerkezetileg 3 nagyobb egységből: vezérlőpultból, kalkulátorból és hálózati egyenirányítóból állt. Az MESZ 1 számítógép 10 évi működése alatt a hallgatók egész sora ismerte és kedvelte meg a számítástechnikát.

Kozma professzor számára a 60-as évek lázas munkával teltek el. Figyelmének középpontjában a mérnökképzés korszerűsítésének feladata állt, amit a Villamosmérnöki Kar dékánjaként (1961–1963) sikerrel valósított meg. Érdeme az elektronikai technológia szak létrehozása, amellyel megteremtette a hazai mikroelektronika egyik alapfeltételét. A híradástechnika szakos hallgatók egész sora tanult a Távbeszélőtechnika 1. és Frajka Bélával közösen írt Távbeszélőtechnika 2. című tankönyveiből.

Az MESZ 1-et a nyelvészek is használták, ami arra készítette, hogy a Nyelvtudományi Intézetnek egy nyelvt statisztikai automatát tervezzen (1964). Az intézet munkatársai évekig sikerrel alkalmazták a készüléket nyelvészeti kutatásaikban.

1961-ben a Magyar Tudományos Akadémia levelező, majd 1976-ban rendes tagjává választotta. Ismert tudósként minden lehetőséget felhasznált arra, hogy a hazai távbeszélő-technika elmaradottságára és hiányosságaira felhívja az ipari vezetés figyelmét. „Tény tehát, hogy mi telefonellátottság tekintetében le vagyunk maradva. Minthogy itt a termelés egyik alapfeltételéről van szó, félok, hogy ha a kérdést elhanyagoljuk, a hírközlés hiánya kerékkötője lesz a társadalmunk



fejlődésének” – írta 1967-ben a Magyar Tudomány hasábjain [4].

1963-ban készült el az a javaslata, amelyben a hazai crossbar telefonközpontok fejlesztését foglalmazta meg. Mély meggyőződéssel vallotta: „...Az általános jólét emelkedése hozzá fog járulni a telefon általános elterjedéséhez, és az országos automatikus telefonhálózat – egyéb híradástechnikai szórakoztató berendezések mellett – fogja lehetővé tenni, hogy a különbség a városi és falusi élet között végleg eltűnjék.” [4]

Idős emberként is fáradhatatlan volt. Tevékenyen részt vett a BME Híradástechnikai Elektronika Intézet munkájában, az MTA Távközlési Rendszerek Bizottságának elnökeként nagyon sokat tett a híradástechnikai ágazat fejlesztéséért. Alkotóerejét 1983-ban bekövetkezett haláláig megőrizte.

Elméleti felkészültség, konstruktív fantázia és nagy gyakorlati készség jellemezte Kozma akademikust, aki elévülhetetlen érdemeket szerzett azzal, hogy jó érzékkel látta meg a hazai híradástechnikai ágazat fejlődésének fő irányait, és ennek szolgálatába tudta állítani a mérnökképzést is. Ugyanakkor úttörője volt a

hazai számítástechnikának, amely ma már életünk szerves részévé vált. Szellemi örökségét ápolnunk kell. Munkássága, a nemzet iránti elkötelezettsége szolgáljon példaképül a most felnövekvő fiatal nemzedéknek.

#### Irodalom

1. Kozma László: Mérnöki tevékenységem az elektronikus számítógépek hőskorából. Magyar Tudomány, 1973. 1. sz. 28–38. p.
2. Frajka Béla: Dr. Kozma László és az MESZ 1. Neumann János Számítógéptudományi Társaság VI. kongresszusa, Siófok, 1995. május 28–31. Budapest, 1995, Neumann János Számítógéptudományi Társaság, 958–965 p.
3. Lajtha György: Kozma László. In Nagy Ferenc (szerk.): Magyar tudóslexikon A-tól Zs-ig. Budapest, 1997, BETTER, MTESZ, OMIKK, 496–497 p.
4. Géher Károly: Megemlékezés. Kozma László. Magyar Tudomány, 1984. 4. sz. 322–323. p.
5. <http://inlap.jate.u-szeged.hu/tortenet/ELETRAJZ/kozma/kozma.htm>

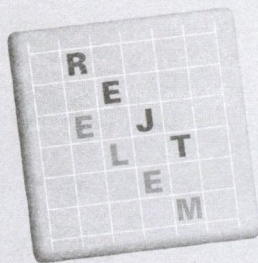
## Hír

A Siemens ICM (mobil információ és kommunikáció) ágazata a KST 2001 lengyel tudományos-telekommunikációs szimpózium keretében demonstrálta a harmadik generációs UMTS-mobiltechnológia hatékonyságát. A bemutató során hangot és adatokat továbbítottak az UMTS-hálózatban. A PTC-ERA 1996 óta ügyfele és stratégiai partnere az ICM-nek, amely NodeB bázisállomásokat és a központi hálózathoz szükséges alkotóelemeket szállít a PTC – ERA kísérleti hálózatához. A Siemens ICM már korábban is sikeresen vizsgálta a harmadik generációs technológiát. Ehhez szériagyártáshoz közel levő, harmadik generációs telefonkészülékeket használtak.

A Siemens ICN (információs és kommunikációs hálózatok) ágazatának átszervezése, az IC-területet érintő létszámcsökkentés egy átfogó csomag egyik eleme. A Siemens júliusban kiadott „Operation 2003” nevű intézkedési tervének elsődleges és egyben legkritikusabb feladata, hogy az ICN ágazat újra nyereségesen működjön. Ezt a célt úgy akarják elérni, hogy vevőikre, termékínálatukra és tradicionális erősségeikre összpontosítsanak. Az átszervezés a következő alapelveket foglalja magában:

- Nagyobb hangsúlyt fektetnek az eredményre, mint a forgalom növelésére.
- Az ICN saját termékeire koncentrálnak a hozzáadott érték maximalizálása érdekében.
- Olyan költségstruktúrát céloznak meg, amely „benchmark”-ként szolgálhat az infokommunikációs ipar számára. Ez további mintegy 5000 fős létszámcsökkentést tesz szükségessé 2002 végéig.
- Továbbra is működtetik a teljes egész értéktermelési láncot, azaz saját gyártóhelyeket üzemeltetnek, azonban számukat felére csökkentik, és elsősorban a magas integráltságú technológiával rendelkezőket tartják meg.
- Továbbra is irányvonal-meghatározók akarnak lenni az innováció területén, ezért a K+F kiadásokat a jelenlegi szinten kívánják tartani. Prioritást élvez az IP-konvergencia és a szélessávú elérési technológia.





## REJTelem

### JÁTÉKA FIATALOK SZÁMÁRA

Egyesületünk a magyarországi távközlési, informatikai szakemberek aktív fóruma. Évente több tucat rendezvény keretében hozzuk egymáshoz és a szakmához közelebb tagjainkat. Mint minden egyesületnek, így nekünk is fontos, hogy a fiatalság bekapcsolódjon munkánkban, tudjon rólunk, és használja ki az egyesületben rejlő előnyöket. Egyesületünk a 2001–2002-es tanévben egy internetes játékot hirdet meg, amely számos egyetem és főiskola weblapjáról is elérhető.

Az internetes játék 8 fordulóból áll, ebből egy személyes megjelenéssel, a többi az interneten keresztül, az Egyesület weboldalán. A játékra a regisztrációs oldalon lehet nevezni. Nevezési korhatár 30 év. A verseny jeligés, a feladatot kiértékelők csak a jeligét ismerik. A feladatkiírás tartalmazza az elérhető pontszámot, ami várhatóan minden hónapban egyenlő, 100 (50-50) pont. Ezzel összesen 800 pont érhető el. A verseny mindenkor aktuális állása a weboldalon folyamatosan nyomon követhető, az első 16 játékos sorrendje mellett mindenki láthatja a saját pontszámát is. A végén a legtöbb pontot gyűjtő nyer. Nem kell minden fordulón indulni. A versenyt egy versenybizottság vezeti, aki a versenyszabályzat szerint biztosítja a verseny tisztaságát. A versenybizottság nem azonos az értékelő bizottsággal. A kiértékelőknek a formailag nagyon hasonló pályázatokat joguk van az etikai bizottság elé tární, amely dönt. (Az etikai bizottság tagjainak nevét közzétesszük a weben.)

A feladatokat minden hó 16-ától teszi közzé a versenybizottság. A feladatbeadás határideje a következő hónap 15-e éjféli. A versenyhónapok: november, december, január, február, március, április, május, június. Eredményhirdetés júniusban. A díjakat a tagcégek, és az Egyesület ajánlja fel. A díjak megtekinthetők lesznek a játék weblapján.

### Feladatok

A feladatok főleg logikai jellegűek, egyre nehezedő megoldással. Minden fordulóban két feladat lesz a pontszámok differenciálódása érdekében. A célfeladatok mellett, amelyeknek egyértelmű az eredménye, gyűjtő és kreatív feladatblokkok is lesznek. Az utóbbi típusú feladatok nyelvi, kombinatorikai típusúak, amelyeknek számos megoldása lehet, ezért csekély a valószínűsége, az azonos megoldásoknak, így több néven nem küldhető be megoldás. A kreatív feladatok több részből összeálló, rejtett formában lesznek csak hozzáférhetőek. A rejtés a rácsrejtjelzés és a puzzle játék keveréke.

Minden hónapban megkonstruálunk egy R rejtjelző rácsot, amelyet meghatározott számú puzzledarabra darabolunk fel. Ugyanígy az R rács segítségével előállítjuk az M rejtjeles szövegmatrixot, amelyben tulajdonképpen a kreatív feladatot tartalmazó szöveget rejtjük el, és amelyet szintén puzzledarabokra darabolunk.

### A gyűjtés menete

Az R és M mátrixok puzzledarabjai a játék weblapján jelennek meg úgy, hogy egyszerre mindig csak egy R és egy M darab látható két-három-négy napig. Ez a gyűjtési szakasz. Akinek nem sikerül a gyűjtési szakasz alatt a teljes puzzle (azaz az R és M mátrixok) összegyűjtése, megtalálja a teljes feladatot a gyűjtési szakasz végén a Híradástechnika című folyóirat aktuális számában. Így a lemaradóknak újabb esélyük lehet a játékban maradásra. A feladat megoldásának feltétele, hogy az aktuális R és M mátrix rendelkezésre álljon, amelyeket az összes puzzledarab megfelelő összeillesztésével érhetnek el. Ezután az R rács segítségével olvashatóvá válik az M mátrixban elrejtett feladat szövege.

### Pontozás

A kreatív feladatblokk pontozása kétszintű:

Először az adott feladatban minden egyes jó megoldás 1 pontot ér, így az egy beküldő által adott összes jó megoldásokat összeszámoljuk, és első szinten annyi pontot kap, ahány jó megoldása volt. (Például az INFORMÁCIÓ szóra készített 20 anagramma 20 pontot, míg ha valaki 50 anagrammát készít, az 50 pontot ér.)

Ezután a végleges pontszám kiszámításához normáljuk a pontszámokat a legtöbb pontot elért beküldő pontszámával, és az így kapott arányszámok szerint osztjuk fel az 50 pontot.

Az utolsó (nyilvános) fordulón a legtöbb pontot elért 16 versenyző (jelige) vehet részt, ahol a feladatok megoldásához már időkorlátot is rendelünk, így a többi fordulóhoz hasonló típusú feladatok megoldása is jóval nehezebb lesz.

*Sok sikert kívánunk a játékhoz!  
A HTE vezetése*



# REJTelem

b T k z l  
T z í t  
y m a i o  
l e é e g  
ö t s b b  
ú j a s  
s ) ó n z  
m a r g y

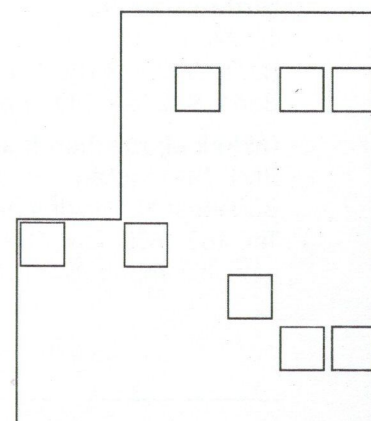
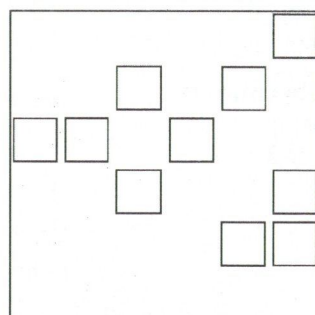
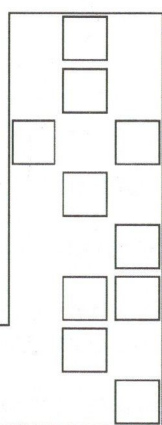
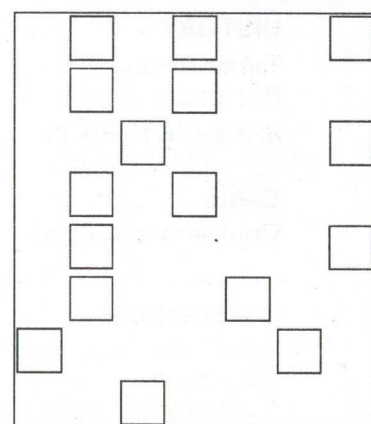
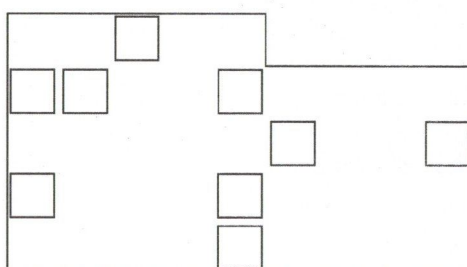
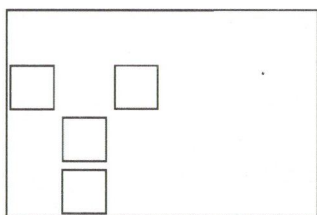
m é s s a s  
o á y s s é l  
í y e l r a  
i n e a l !  
s z o z m n  
f n s t e ó a  
z r e l k a

ű k b n e k  
z á z m s z !  
a g . r A t  
ö v i ó d

e ö m e A n s "  
a n T é O p á K e m  
A N e " z t t n s  
n a l k z c ö n b  
l b t ü t e j e é  
ö l  
ú a  
a v

k s é z ó ö ö z  
s e s h z g a b  
b z z e t ú é t  
á l é s j s t O  
a k h a A z

n e á a o l g h a  
a g k ( . e l e  
n m m á



Kérjük, ezt az oldalt másolja le és a másolaton vágja ki a játékban szereplő rácsokat!

**Beadási határidő: 2001. december 15.**



# Contents

**Dr. György Lajtha:**

Issue in this month.....1

## SELECTION OF ROUTE

**Csaba Végső, Dr. János Levendovszky, Gábor Rétvári**

QoS-route search in case of defective link information based on the theory of statistical inequalities .....3

**Attila Takács, Csaba Lukovszki, Róbert Szabó**

Simple traffic management method for transmission of voice traffic in IP-BSS networks .....13

## MOBILE

**Sándor Imre, Máté Szalay**

Ring hierarchy – reliable IP-micromobility network topology .....19

**András Földi, Sándor Cseh**

To what extent a tower can be loaded? Case study. The history of a television tower in Hungary.....25

## THEORETIC ACHIEVEMENTS

**Sándor Albrecht**

Processing of burst mode synthetic aperture radar (SAR) signals by application of momentary Fourier transformation .....31

**György Vesztergombi, Dr. János Levendovszky, Zsombor Elek**

New calculation procedures in the reliability analysis.....43

**Gyula Horváth**

From nano-tubes to nano-engineers .....49

## INFORMATION SOCIETY

**Brigitta Páti**

Little steps towards the information society.....53

## HISTORY

**Tamás Dénes**

Birth of the cypher grids Girolamo Cardano .....57

**Szilveszterné Fekete**

Portrait from the recent past: László Kozma .....63

**Game**.....66

**Contents in English**

### 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

Design by: Kocsis és Szabó Kft.

HU ISSN 0018-2028





## **Jelen a digitális jövő**

Az Antenna Hungária üzembe helyezte új digitális földfelszíni műsorszóró adóját, ezzel a jelenben képviselve a jövő technikáját. Megkezdődhetnek a kísérleti DVB-T adások, amelyek hamarosan forradalmasíthatják az eddigi televíziózást. A digitális földfelszíni műsorszórás hatékonyan járul hozzá az információs társadalom igényeinek kielégítéséhez. Az analóg műsorszórásnál lényegesen több szolgáltatást nyújt. Kifogástalan kép, tökéletes hang, mobil vételi lehetőség, interaktív szolgáltatások – ezt nyújtja a DVB-T, a jövő földi digitális televíziózása.



[www.dvb-t.hu](http://www.dvb-t.hu)

DigiTAG

**antenna**  **hungária**  
Teret adunk gondolatainak



