híradástechnika

VOLUME LVIII.

2003/11

November

Az információs technológia és hatásai

ITU World Telecom 2003

Összeköttetések minősége és megbízhatósága

A Hírközlési és Informatikai Tudományos Egyesület folyóirata

Tartalom

HOL VAN A SZAKADÉK? (NOVEMBER) 1

AZ INFORMÁCIÓS TECHNOLÓGIA ÉS HATÁSAI

Benczúr András
Számítógépek és híradástechnika: az emberiség új kommunikációs korszaka (II. rész) 2

Kovács Balázs, Vida Rolland
A Zigbee technológia 9

Mészáros Etelka
A „Fuzzyról" általában 15

Dr. Tarnai Géza, Dr. Izabela Krbilová, Dr. Jiří Zahradník
Egységes mobil távközlési szolgáltatás az európai vasutak számára 18

ITU WORLD TELECOM 2003

Dr. Lajtha György
Nincs királyi út 23

Kontor Kornélia
Távközlési Ifjúsági Világfórum 28

Könyvet ajánlunk 30

Eisler Péter
Xyscom 31

ÖSSZEKÖTTETÉSEK MINŐSÉGE ÉS MEGBÍZHATÓSÁGA

Stikkel Gábor, Szederkényi Gábor
Meddig teszteljünk? 36

Limbek Réka, Sziklai Péter
Rejtjelező homomorfizmusok 42

Imre Sándor, Szalay Máté
LTRACK – Új mobilitás-menedzsment 49

A RÁDIÓZÁS JÖVŐJE ÉS MÚLTJA

Dr. Sárkány Tamás
Digitális rádiózás a hosszú/közép/rövid hullámú tartományokban 53

Könyvet ajánlunk 57

Dósa György
A hazai antenna vizsgáló telephely története 59

Címlap: Az ITU toronyból rálátni a világra

Hol van a szakadék?

(November)

Az egész világon sokat lehet hallani a digitális szakadékról, mely a számítástechnikai tudással és Internettel rendelkezők, valamint azok között van, akik mindehhez nem férnek hozzá. A World Telecom Kiállítás és Fórum ismét előtérbe helyezte ezeket a kérdéseket. Számos előadás foglalkozott ezzel a témával, ahol a költségekről, a terjesztésről és az oktatásról egyaránt szó esett. Sokat hirdették a december elején megrendezendő WSIS konferenciát, amely az információs társadalom elterjesztésének problémáival foglalkozik. Tehát mindaz, amit az előadótermekben hallottunk, azt a benyomást kelthette a résztvevőkben, hogy propagandával, kormányzati intézkedésekkel, vagy segélyekkel gyorsítani lehet az informatika terjedését.

A kiállítás már nem egészen ezt mutatta. Sok, eddig elfelejtett ország jelentkezett olyan műszaki újdonságokkal, melyek azt mutatták, hogy kutatóik, mérnökeik és kereskedőik már nagy lépéseket tettek az információs technológiák elsajátítása és alkalmazása felé. Meglepő élmény volt, hogy az eddig elmaradottnak hitt Kína az új technológiák terén milyen eredményeket ért el. Egy eddig soha nem hallott kínai vállalat, a Huawei, talán az egész kiállítás legnagyobb pavilonját létesítette, és itt találkozhattunk a távközlés és informatika legújabb eredményeivel. A pavilonon belül egy külön kis helyiség tájékoztatta a közönséget arról, hogy kaphatók Kínában az Ubiquitous megvalósításához szükséges elemek. Ez azt jelenti, hogy mára egyértelműen uralják az összes mobiltechnológiát és elegendő mesterséges intelligenciát tartalmaznak kapcsolórendszereik ahhoz, hogy bárkit, bármikor, bárhol megtaláljanak.

A kínai pavilon látogatása során megtudhattuk, hogy a telefonsűrűség az elmúlt 4-5 évben meg tízszereződött. Bizonyos korlátok között terjed az Internet hozzáférés is. A további terjedést éppen a politikai korlátok nehezítik. Kínát ezen kívül több másik cég is képviselte, melyek közül kiemelkedett a ZTE, ahova belépve azt hihette az ember, hogy a Bell laboratórium kiállítását látogatja meg. Megjelent a kiállítók között még Hong Kong, külön pavilonban Azerbajdzsán és Ukrajna is. Tehát ahol valódi érdeklődés mutatkozik a távközlési szolgáltatások iránt és a felhasználók észreveszik, hogy számukra előnyös a fix telefon, vagy a mobil hozzáférés, sőt esetleg az Internet hozzáférés is, ott saját erőből sikerült betemetniük a szakadékot.

Magyarországot sajnos csak egy vállalkozás képviselte, igaz hogy ez újszerű, egészen speciális távközlési eszközt mutatott be, melyhez hasonlót máshol nem láttunk. Erről a kis térségeket többféle technológiával elérő, telefon és Internet célokra egyaránt használható rendszert mutattak be. Erről ebben a számban Eisler Péter cikke számol be.

8 évvel ezelőtt azonban ezen a kisvállalkozáson kívül még megjelent Genfben a MATÁV, az Antenna Hungária és számos más világcég magyarországi fejlesztő helyeinek eredménye is. Az érdektelenségen azonban nem lehet sem pénzzel, sem kormányhatározatokkal segíteni.

A fenti gondolatokhoz kapcsolódik Benczur András bevezető cikke, amely a matematika oldaláról mutatja be az informatika hatásait. A cikk első része szeptemberi számunkban jelent meg. Az információs társadalom problémáival a World Telecomról készült beszámolóban találkozunk. A műsorszórás jövőjéről és múltjáról olvashatunk, ahol a jövő érdekességeit és a múlt eredményeit lehet majd összehasonlítani.

Az információs társadalom egyik kritikus pontjával, az adatok védelméről, biztonságáról számol be egy cikkünk. Ez azért különösen érdekes, mert tökéletes biztonság nem érhető el, de mindenképpen törekednünk kell ennek javítására. Bár a kiállításon a külföldieket meglátogatva és a hazai partnerekkel beszélgetve ismét kialakult az, hogy elsősorban az etikát kellene az iskolában tanítani, és akkor automatikusan terjedne az információs technológia is. Legalább annyira kellene tisztességesnek lennünk, mint az autókkal kapcsolatban. Ha százalékosan csak annyi hamis rendelés történne, mint amennyi autót ellopnak, akkor biztos, hogy rövid időn belül meghaladná az Internet penetráció az autók számát.

Lajtha György

Számítógépek és híradástechnika: az emberiség új kommunikációs korszaka

II. rész: Matematikai háttér

DR. BENCZÚR ANDRÁS

abenczur@ludens.elte.hu

Kulcsszavak: informatika, matematika, távközlési alkalmazások

Írásomban az emberi kommunikáció jellemző formális modelljeire, az elemi kommunikáció, valamint az információs rendszer modelljére építve jellemzem a kommunikáció fejlődési folyamatát, és ebben helyezem el a jelenkor új kommunikációs világát. Rámutatok benne a korlátokra és a lehetőségekre, ugyanakkor hangsúlyozom, hogy a megoldásokra nincs általános recept, kimeríthetetlen feladatrendszer előtt állunk. A kiszámítható világ nem helyettesítheti a valóságot, csak korlátozott méretékben modellezheti, segíthet megismerésében, a jövő előrejelzésében. Dolgozatom második részében ennek matematikai hátterébe is betekintést nyújtok.

3. Matematikai feladatok

Első matematikai feladatként nézzük a lehetséges üzenetek és a lehetséges csatornajel-sorozatok közötti megfeleltetés problémáját a Shannon-modellben. Az alapfeladat egyszerűen megfogalmazható: különböző üzenetnek különböző jelsorozatot kell megfeleltetni. A skatulyaelv azt mondja ki, hogy ha kevesebb skatulya van, mint golyó, akkor van olyan skatulya, amelyben egynél több golyó van. Ezért tehát legalább annyi csatornajel-sorozat szükséges, mint amennyi üzenet lehetséges.

Kezdjük a csatorna mennyiségi jellemzésével.

A csatorna *C* kapacitását a *T* időhosszúságú (megkülönböztethető) jelsorozatok számának, *N(T)*-nek segítségével definiáljuk:

$$C = \lim_{T\to\infty} \frac{\log_2 N(T)}{T}$$

Ha két csatornára *N(T)* megegyezik, akkor a két csatorna helyettesíthető egymással, ekvivalensek. A legegyszerűbb csatorna a szimmetrikus bináris csatorna. Két jel vihető át, mondjuk 0 és 1, és minden jel ugyanolyan hosszú (időben). A csatorna kapacitás, C, erre a csatornára pontosan azt jelenti, hogy egységnyi idő alatt C jel, vagyis C bit vihető át. Ez magyarázza, hogy a kapacitás mérőszámának dimenziója bit/sec.

Nehezebb kérdés matematikailag a forrás választási lehetőségeinek számát meghatározni.

A Shannon-entrópia nem is ezt méri közvetlenül, hanem a választás bizonytalanságát, vagyis, hogy a lehetséges üzenetekből milyen bizonytalansággal történik a választás. A választás véletlenségét valószínűség-eloszlással jellemezzük, ami matematikai modellel való közelítés. A bizonytalanság mérőszámát megadó függvény természetes elvárásokat kielégítően került meghatározásra.

A folytonosságra, az egyenletes eloszlásokon való monotonitásra és a megfigyelés lépcsőzésére tett feltevések alapján felírt függvényegyenlet megoldásaként adódik a Shannon-entrópiaformula:

A $\{p_1, p_2, ..., p_n\}$ valószínűségeloszlás entrópiája

$$H(p_1, p_2, ..., p_n) = -\sum_{i=1}^{n} p_i \log_2 p_i .$$

A forrás entrópiáját úgy határozzuk meg, hogy igen hosszú üzeneteket tekintünk. A hosszú üzenet választásának eloszlására meghatározzuk az entrópiát, és osztjuk az üzenet hosszával. Általános estben az üzenet hosszával végtelenhez tartva határértékként kapjuk az üzenet elemi részeire, szimbólumaira az átlagos entrópiát, *H*-t. Az *L* hosszú, *L* szimbólumból álló üzenet entrópiája ekkor *L(H±γ)* lesz. Amennyiben a forrás működésének sebessége *V* szimbólum/sec, akkor *T* idő alatt a forráshoz *TV(H±γ)* entrópia rendelhető.

Az előkészítés után nézzük a skatulyák és golyók számát. A formulákban a görög betűk az idő igen nagynak választásával tetszőlegesen kicsivé tehető mennyiségek. A *C* kapacitású csatorna *T* idő alatt

$$2^{T(C-\delta)} \le N(T) \le 2^{T(C+\delta)}$$

számú különböző jelsorozatot képes átvinni, ennyi a dobozok száma.

Hogyan lehet az entrópiából a választható üzenetek számára következtetni? Az igen hosszú véletlen jelenségekre igen általános feltevés (ergodikusság) mellett az jellemző, hogy közel 1 valószínűséggel egy tipikus halmazba esik a jelenség előfordulása. A tipikus halmaz elemeinek valószínűségére valószínűség-számítási törvények alapján alsó és felső becslés adható, és az bizonyítható, hogy közel egyenletesen oszlanak el a választási lehetőségek a tipikus halmazon. A tipikus halmaz, vagyis a meghatározó többség *M(VT)* számosságára *V* sebesség és *T* idő esetén a valószínűségekre kapott becslés reciprokjaként a

$$2^{TV(H-\lambda)} \le M(VT) \le 2^{TV(H+\lambda)}$$

egyenlőtlenség teljesül. Így kaptuk meg tehát a golyók számát.

A skatulyaelvből kapjuk a csatorna alaptételét, mely szerint tetszőleges $\varepsilon > 0$ választáshoz $V < C/H - \varepsilon$

sebesség esetében lehetséges miden különböző T idejű tipikus üzenetet különböző T hosszú jelsorozattal kódolni, azaz lehetséges az adást veszteségmentesen működtetni. Nem lehet azonban *V>C/H* sebesség esetén veszteségmentesen továbbítani minden üzenetet.

A kommunikáció fenti alapvető matematikai törvényszerűsége megadja adott csatorna esetében a kommunikáció lehetőségeit és korlátjait, de nem ad közvetlen segítséget a megoldáshoz. Az entrópia-formula független az eloszlás permutációjától, és nem függ az üzenet szimbólumkészletétől sem. Konkrét forrás kódolása esetében mindkét információnak rendelkezésre kell állnia mind a forrás kódoló-adó oldalán, mind a rendeltetési hely vevő-dekódoló oldalán. Adattárolási és számítási kapacitás nélkül (kivéve az analóg esetet) az új típusú csatornák nem lennének használhatók.

A vázolt blokkséma csatornadoboza a jel tér- és időbeli terjedését jelentő közeget ábrázolja, és magában foglalja a terjedés közben bekövetkező torzulásokat, a zajt is.

A matematikai elmélet egyik fontos összetevője a forrás bizonytalanságának mérőszámaként bevezetett entrópia, ami egyben az optimális kód hosszának várható értékére ad alsó korlátot. Ugyanez a mérőszám alkalmas a zaj, és a titkosítás kérdéseinek vizsgálatára is.

Shannon [1] alapművében nem különbözteti meg élesen a kódoló-adó és a vevő-dekódoló kettős funkcióját. A digitális adatátvitelben ezek már élesebben szétválnak, a kódolás és dekódolás algoritmikus feladata önállósulhat. Az információelmélet központi feladata pedig a véletlen jellegű zaj kezelésére, az adás és a vétel együttesen hatékony megoldására, a nagy csatornakapacitás, vagy más jellemzővel, a nagy sávszélesség elérésére irányul. A forrás jó kódolása nem a csatorna kapacitásának biztosítása, hanem jó kihasználása szempontjából fontos. Elméletben függetlenné tehető a két feladat. A forrást kódolhatjuk a lehető legtömörebben bináris jelsorozattá, és a csatornajeleket elegendő ez után csak a független, azonos eloszlású, két egyforma valószínűségű lehetőségből álló forráshoz (szimmetrikus Bernoulli-eloszlás) illeszteni.

A vázolt gondolatmenet alapján látható, hogy a csatorna jó kihasználásához a forrás üzenetét hosszú időszakaszonként blokkolva kellene továbbítani, ami jelentős késleltetést okozhat. A nagy teljesítményű csatornák messze meghaladják az emberi üzenet-kibocsátás által igényelt teljesítményt. Az időbeli összegyűjtés és blokk-kódolás helyett a hasonló hatást biztosító térbeli összegyűjtést, azaz több forrás üzenetének párhuzamos továbbítását lehet alkalmazni.

A közeli jövő lehetőségeinek érzékeltetésére próbáljuk elképzelni, mit jelent a 2008-ra jósolt 1Tera-bit/sec, azaz 10^{12} bit/sec kapacitású Ethernet csatorna. A Föld akkori lakosságát 10 milliárd, azaz 10^{10} embernek véve, 128 billentyűs klaviatúrát használva másodpercenként mindenki írhatna folyamatosan 14 leütésből álló szöveget, és ez egyszerre átvihető lenne ezen a csatornán.

A forrás (jövőbeli) véletlenségét matematikai idealizált modellel közelítjük. A valós szituációt egy bizonytalanabb, nagyobb entrópiájú matematikai jelenséggel, sztochasztikus folyamattal helyettesítjük. A valós forrás tipikus kimenetei ezért részhalmazát képezik a matematikai modelljében kapott tipikus véletlen halmaznak, amennyiben jól modelleztük a forrást.

A Shannon-modell leegyszerűsített, elemi bemutatása után térjünk át múlt megértésével, jellemzésével összefüggő kérdéskörre, ami a felhalmozott adat- és ismeretkészlet elemzéséhez ad matematikai hátteret.

A nagyon hosszú vagy kiterjedt, konkrétan előforduló folyamatot (realizációt) önmagában is nézhetjük, eloszlás nélkül, tömöríthetőség szempontjából. Ez átvezet az algoritmikus jellemzés világába, a nagy adatállományok tömörítésének kérdéseihez, ami a második matematikai feladatköre a dolgozatnak.

A Kolmogorov-bonyolultság elméletköre a 60-as évek elején fejlődött ki elsősorban Kolmogorov iskolájában, de attól függetlenül és szinte egyidőben R. Solomonoff és Chaitin munkássága alapján. A kiindulási kérdések sorában a véletlenszám-generátorok jóságának ellenőrzése, a véletlen jelenségek algoritmikus jellemzése, az univerzális számítógépi tanulási algoritmus a leglényegesebbek.

Kolmogorov az elmélet indulását jelentő [2] dolgozatában a következő kérdést tette fel: milyen rövid kód lenne elegendő ahhoz, hogy a „Háború és béke" teljes szövegét abból egy számítógép előállítsa? Mondhatná valaki, hogy tud definiálni olyan függvényt, amely a 0 kódhoz a „Háború és béke" teljes szövegét rendeli. Ekkor azonban a vevő oldalra ennek a függvénynek egy programkódját át kell küldenie, s a program kódja valószínűleg adatként tartalmazná a regény valamennyire tömörített szövegét. Az is igaz, hogy ha már egyszer ott van a rendeltetési hely vevőjében ez a programkód, akkor elég a 0 üzenet és a program azonosítójának küldése a regény helyett. *(Gondoljunk viszsza az I. részből a 7. ábra adattároló elemeire.)*

Alapvető feltétele egy kód használatának, hogy ismerjük és ki tudjuk számítani azt a függvényt, amivel a dekódolást elvégezhetjük. Azt is mondhatjuk, hogy a kód és a dekódoló program kódjának ismerete kell együttesen a dekódoláshoz.

A két kód együttes hoszszának minimuma jelenti a tömöríthetőség alsó határát. Ez az intuitív alapja a Kolmogorov-bonyolultságnak, amit a következőkben vázlatosan ismertetünk.

Először egy tetszőleges kiszámítható (parciális rekurzív, Turing-kiszámítható) függvény szerint definiáljuk egy nem negatív egész szám, vagy egy véges bináris szó bonyolultságát. (A nem negatív egész számok és a véges bináris szavak közötti kölcsönösen egyértelmű megfeleltetést használva egy egész számot és a neki megfeleltetett véges bináris szót azonosnak tekintjük. A kiszámítható függvények többsége parciális függvény, ami azt jelenti, hogy bizonyos helyeken nincsenek meghatározva, mert ott a kiszámításuk végtelen ciklusba esik.)

Definíció: Az *x* nem negatív egész számnak az *f(p)* kiszámítható függvény szerinti bonyolultságán a

$$C_f(x)=\min\langle l(p)|\, f(p)=x\rangle,$$

értéket értjük, amennyiben létezik *x*-nek ilyen *f* szerinti *p* kódja, és végtelen a bonyolultság, ha ilyen kód nem létezik. Az *l(p)* függvény a *p* kód hosszát adja.

Az elmélet alaptétele, amelyet a három említett matematikus egymástól függetlenül, szinte egy időben talált meg, optimális kódoló létezését mondja ki:

Tétel: Létezik olyan optimális kiszámítható függvény, $f_0(p)$, hogy bármely *f(p)* kiszámítható függvényre és *x* egész számra

$$C_{f_0}(x)\le C_f(x)+k_f\ ,$$

ahol k_f csak *f*-től függő konstans. ■

(A bizonyítás az univerzális kétváltozós függvény létezésére alapul. Létezik olyan *U(n,p)* kiszámítható függvény, amelyre minden *f(p)* kiszámítható függvényhez létezik n_f, hogy $U(n_f,p)=f(p)$.

Az (n_f,p) rendezett pár alkalmas kódjából és az univerzális függvényből tudjuk az optimális kódoló függvényt megkonstruálni. Az optimális kódoló a dekódoló program és a hozzátartozó kód együttes hosszára adja a minimumot.)

Definíció: Látható, hogy az optimális függvények szerinti bonyolultság csak konstanssal tér el egymástól, ezért tetszőlegesen rögzíthetjük, mondjuk az f_0, optimális függvényt, és segítségével definiáljuk az

$$I(x)=C_{f_0}(x)$$

Kolmogorov-bonyolultságot. ■

Az *I(x)* függvény azonban csak elméleti objektív felső határ a tömöríthetőségre, mert nem kiszámítható függvény. Ennek ellenére két alapvető tulajdonsága alapján lehet vele számolni:

1. Felülről becsülhető a tétel alapján bármilyen konkrét függvény szerinti bonyolultsággal.
2. Az $I(x)=k$ érték mögött egy konkrét *k* hosszú *p* kód áll, amire $f_0(p)=x$.

A Kolmogorov-bonyolultság sok szempontból jobban használható változata, az úgynevezett prefix Kolmogorov bonyolultság, csak olyan kódoló függvényeket enged meg, ahol a lehetséges kódok halmaza prefixmentes, azaz egyik kód sem folytatása egy másiknak. Ebben az esetben is létezik optimális g_0 prefixmentes kódoló, és definiálható segítségével a

$$K(x)=C_{g_0}(x)$$

prefix Kolmogorov-bonyolultság.

Hasonló úton jutunk a feltételes Kolmogorov-bonyolultsághoz, ami azt fejezi ki, mennyit segít egy *x* szám kiszámításában egy másik *y* szám ismerete.

Definíció: Az *x* szám *y* szerinti feltételes közönséges, illetve prefix Kolmogorov-bonyolultságán, *I(x|y)*-en, illetve *K(x|y)*-en a

$$I(x\,|\,y)=C_{f_0}(x\,|\,y)=\min(l(p)|\, f_0(p,y)=x)$$

illetve

$$K(x\,|\,y)=C_{g_0}(x\,|\,y)=\min(l(p)|\, g_0(p,y)=x)$$

értékeket értjük, ahol $f_0(p,y)$ és $g_0(p,y)$ kétváltozós optimális kódoló függvények. ■

Mindkét függvény tulajdonságai megegyeznek a feltétel nélküli esetre mutatott tulajdonságokkal.

A feltételes bonyolultság alkalmas arra, hogy egy véges halmaz elemeinek a halmaz szerinti feltételes bonyolultságát elemezhessük. Ehhez még arra van szükség, hogy magát a halmazt kóddal jellemezhessük, azaz a halmaz kódjából elő tudjuk állítani program segítségével a halmaz elemeit.

Legyen A véges elemű halmaz, kódja legyen *a*, és elemeinek száma legyen *m*. Nézhetjük x∈A esetén az *I(x|* A)= *I(x|a)* és *K(x|* A)=*K(x|a)* feltételes Kolmogorov bonyolultságokat. A Kolmogorov-bonyolultság 2. tulajdonsága alapján megint a skatulya elv szerint látható, hogy A elemeinek többségére az A szerinti feltételes bonyolultság nem lehet érdemben kisebb, mint $\log_2 m$. Ugyanis a $\log_2 m$-nél Δ-val rövidebb kódok száma, amit f_0, illetve g_0 használhat, legfeljebb $m2^{-\Delta}$.

Amennyiben az *a* kód úgy viselkedik, mint egy felsorolható halmazsereg paramétere, és *a* alapján az m_a elemű A_a halmaz elemeit algoritmikusan fel tudjuk sorolni, akkor a

$$K(x|a) \le \log_2 m_a + c$$

is teljesül valamilyen *c* konstanssal, amely a halmazsereg felsoroló függvényétől függ csupán.

Speciálisan, ha A az *a* hosszú szavak halmaza, azt kapjuk, hogy a szavak döntő többsége még a hosszának ismeretében is legalább olyan bonyolult, mint amilyen (hosszú), de nem is bonyolultabb a hosszánál. (Ebben az esetben ugyanis $m=2^a$.)

Az algoritmusokkal kezelt jelek világának egy másik fontos törvényére mutat rá a feltételes Kolmogorov-bonyolultság, amit az **információ-nemnövekedés törvényének** nevezhetünk. Szemléletesen úgy vethető fel a kérdés, hogy mennyi információt nyerhetünk ki az adatbázisokból? Mit jelent az például, hogy az apa–fiú kapcsolatokat tároló adatbázisból a nagyapa–unoka kapcsolatokat ki tudjuk nyerni? A kérdés az, hogy valóban nyerünk-e információt? A válasz: a kinyert információ nem lehet több annál, mint amennyit bevittünk.

A pontos matematikai megfogalmazáshoz jelölje *x* az adatbázis tartalmát, *q* a kérdésadatot, *v* pedig a *q* kérdésre adott választ. Minthogy a válasz *x*-ből és *q*-ból kiszámítható, valamilyen kétváltozós *f* kiszámítható függvényre *f(q,x)=v*. A feltételes Kolmogorov-bonyolultságot definiáló optimális függvény 1. tulajdonsága szerint

$$K(v\,|\,x)=C_{g_0}(v\,|\,x)\le C_f(v\,|\,x)+n_f\le l(q)+n_f\ .$$

A fenti egyenlőtlenség azt fejezi ki, hogy az adatbázis tartalmának ismeretében a válasz feltételes Kolmogorov-bonyolultsága, azaz információmennyisége nem lehet nagyobb a kérdés hosszánál. (Finomabb becsléssel az is megmutatható, hogy a kérdés prefix Kolmogorov-bonyolultságánál nem nagyobb a válasz feltételes információmennyisége. Ezen felül még az is teljesül

az adatbázis tartalmára, *x*-re, hogy a válaszfüggvény valamilyen végrehajtható programkódját is tartalmazza.)

Ennek a törvénynek finomabb elemzésekor azt is figyelembe kell venni, hogy a választ megkapó személy – aki lehet a kérdező is – általában kevesebb információval rendelkezik, mint amit a teljes adatbázis tartalmaz. Ehhez az információhoz viszonyítva a válasz feltételes információmennyisége lehet nagyobb is, mint a kérdés információmennyisége. Ez azt jelenti, hogy a választ megkapó saját tudása és a kérdés ismeretében nem tudná a választ előállítani további kívülről kapott információ nélkül, illetve a kérdés, a válasz és a saját ismerete nem lenne elég ahhoz, hogy megértse a választ. Az adatbázis nem az egyén, hanem az információs rendszer kollektívájának együttes ismeretét tükrözi. Az egyén így tud többet kapni a közösből annál, mint amit ő adott hozzá.

Természetszerűen vetődik fel a kérdés, hogy a két információmennyiség, a Shannon-entrópia és a Kolmogorov-bonyolultság, vagy másik nevén Kolmogorov-entrópia között van-e kapcsolat. Általánosságban azt lehet mondani, hogy minél nagyobb jelenségről van szó, annál szorosabb a két mennyiség kapcsolata.

Az igen hosszú véletlen jelenségekről, mint amilyen egy igen hosszú üzenet, már említettük, hogy úgy viselkednek, mint egy lényeges halmazra koncentrálódó egyenletes eloszlású jelenség. Egy *L* hosszú tipikus $X=x_1x_2 \ldots x_L$ üzenet *p(X)* valószínűsége a

$$2^{-L(H+\varepsilon)} \le p(X) \le 2^{-L(H-\varepsilon)}$$

egyenlőtlenségnek tesz eleget. Jelöljük ezt a tipikus halmazt **A**-val, és elemeinek számát *m*-mel. Tekintettel arra, hogy a *p(X)* valószínűségek összege az **A** halmazon legfeljebb 1, és tetszőlegesen közel lesz 1-hez, ha *L*-et elég nagynak választjuk, ezért *m*-re az alábbi becslést kapjuk:

$$(1-\delta)2^{L(H-\varepsilon)} \le m \le 2^{L(H+\varepsilon)}.$$

Amennyiben az **A** halmazt algoritmikusan jól tudjuk jellemezni, ami a gyakorlatban tipikusan statisztikai jellemzőkre tett egyenlőtlenségekkel történik, akkor használhatjuk a *K(x| A)* feltételes Kolmogorov-bonyolultságot, és *m* becsléséből az

$$L(H-\varepsilon') \le K(X \mid A) \le L(H+\varepsilon')$$

becslés adódik, ahol ε' tetszőlegesen kicsi választásához valamilyen alkalmasan nagy L_0-nál nagyobb *L*-re teljesül az egyenlőtlenség.

Azt kaptuk tehát, hogy a Shannon-entrópia szerint az egy szimbólumra jutó entrópia a tipikus halmaz elemein megegyezik a feltételes Kolmogorov-entrópia – azaz az elméletileg legrövidebb kód hosszának – egy szimbólumra jutó részével.

Összegezve, mindkét esetben arra jutottunk, hogy meg kell találni a jelenség szempontjából lehető legkisebb, és minden lényeges lehetőséget tartalmazó halmazt, amit hatékonyan jellemezni tudunk, és ezen a halmazon az egyenletes kódhossz választásánál nem érdemes jobb kódolási módszert keresni. Ezzel kaptuk meg mindkét úton a kódolás univerzális lehetőségeit és korlátjait.

(Pontosan ezt fejezi ki a Kolmogorov-féle struktúrafüggvény: adott *x*-hez keressük azt az *x*-et tartalmazó véges $A(x,\alpha)$ halmazt, amelynek prefix Kolmogorov-bonyolultsága legfeljebb α, és elemszáma, m_α minimális. Az *x* struktúrafüggvénye $str_x(\alpha)=\alpha+\log_2 m_\alpha$. Az $A(x,\alpha)$ halmaz az *x*-hez hasonló elemek halmazának tekinthető.)

A fentiekből érezhető, hogy a véletlenség és az algoritmusok között valamilyen kapcsolat van. Paradox módon végtelen sorozatok véletlenségét algoritmikusan lehet jellemezni. Kolmogorov utolsó [3] dolgozata, amelyet Uszpenszkij-jel közösen írt, igen részletes áttekintést ad a véletlenség és az algoritmusok összefüggéséről. Adott eloszlás szerinti végtelen véletlen sorozatok halmazának komplementere algoritmikusan jellemezhető, és úgy nevezett effektíven null-mértékű halmazt jelent az adott eloszlás szerint.

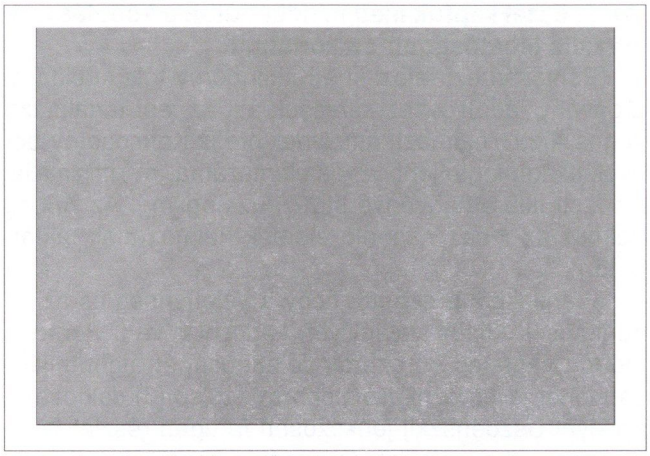
Véges esetben minden más. Képzeljünk el 1000 pénzfeldobással létrehozott nulla-egy sorozatot, és egy csupa nullából álló 1000 hosszú sorozatot. Nyilván az elsőt véletlennek tekintjük, a másodikat nem. Kezdjük el a második sorozatot bitenként összevissza sorrendben átírni az első sorozattá. Meg tudjuk-e mondani, hol történt a váltás a nem véletlen és a véletlen eset között?

(A múlt megvalósult véletlensége is egészen más, mint a jövő lehetséges véletlensége. Vegyük például a 10 pénzérme feldobási kísérletet. Ennek eloszlása egyszerű, mind az $1024=2^{10}$ eset azonos valószínűségű. Végeztessük el a kísérletet 10240 személlyel. Igen nagy a valószínűsége, $1-e^{-10}$, hogy lesz közöttük olyan, aki csupa fejet dobott. Véletlennek fogjuk-e tekinteni ezt az eredményt? Nem jó a kérdés, az eredmény már nem véletlen, csak véletlenül ez adódott.)

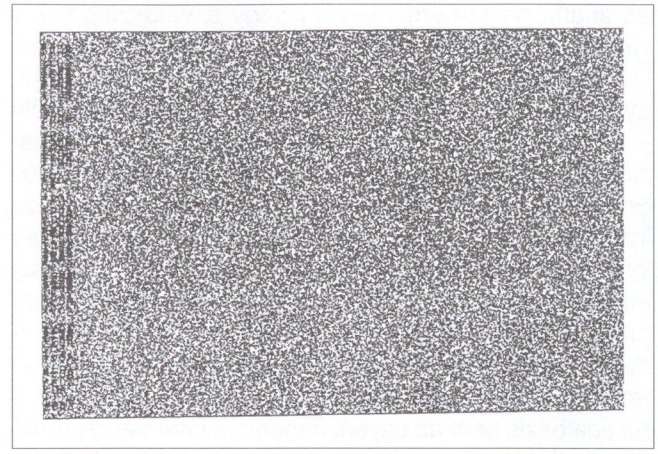
Véges sorozatokra a véletlen nem definiálható, csak az, hogy mennyire tekinthető véletlennek. Egy véges halmaz elemét akkor tekintjük a halmazban véletlenszerűnek, ha a halmaz szerinti feltételes Kolmogorov entrópiája nem sokkal kisebb a halmaz elemszámának logaritmusánál. Egy elem annál véletlenszerűbb, minél közelebb van feltételes Kolmogorov-entrópiája a halmaz elemszámának logaritmusához.

Egy véletlen jelenségből származó nagyon hosszú előfordulások egyre nagyobb hányada viselkedik a fenti értelemben erősen véletlenszerűen. Az algoritmikus tanulás lényege: kiszűrjük a jellemző szabályosságokat, s a megmaradó egyedi tulajdonságokat tömörítetlen adatként adjuk meg. A jellemző sajátosságokkal megadott halmazon a vehetjük lehető legvéletlenebb egyenletes eloszlást, és így kapjuk meg a jelenséghez hasonló lehetőségek halmazát.

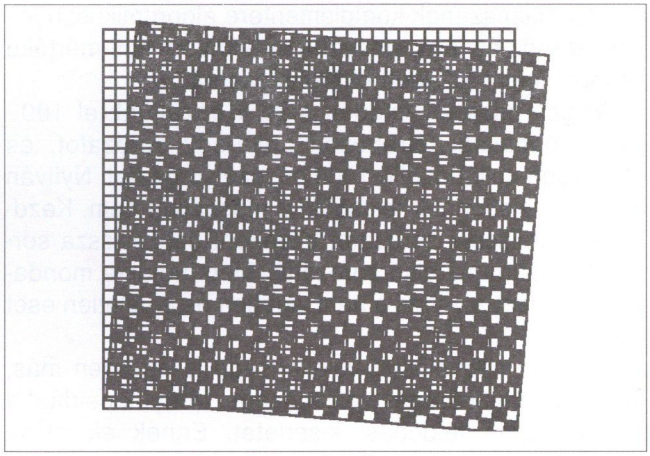
Nézzünk erre egy érdekes vizuális példát. Vegyük az 1/2 szürkeségű színezéseket, vagyis ahol a képpontok (képcellák) fele fekete, fele fehér. Az I. rész [Híradástechnika 2003/9] ábráinak sorszámozását folytatva, a *10. és 11. ábrák* két eltérő színezést mutatnak. A *10. ábra* sakktábla-színezés, elég annyi adat róla, hogy



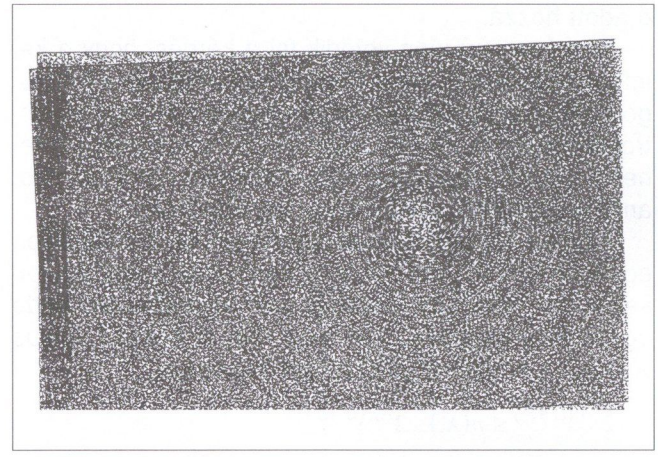
10. ábra



11. ábra



12. ábra



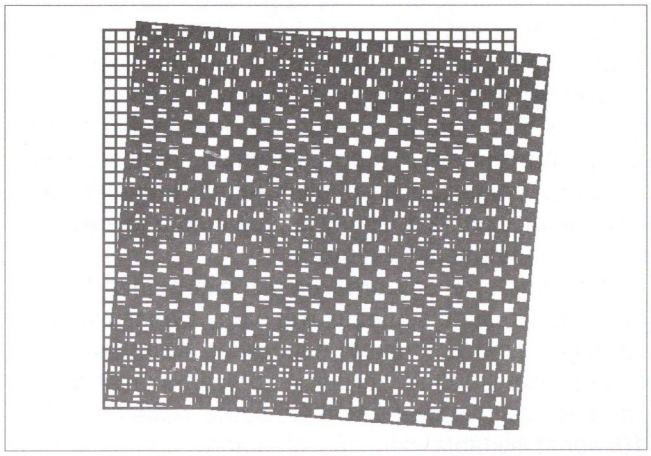
13. ábra

bal felső cella színe milyen, és a teljes színezést elő tudjuk állítani. A *11. ábra* véletlenszám-generátorral készült, megfelel egy tipikus színezésnek. (Az ábra 1990-ben készült, s e baloldalon látható sötét sáv a lézernyomtató hibaüzenete volt.) Aki nem ismeri a generátort, gyakorlatilag nem tudja tömöríteni a kép kódját.

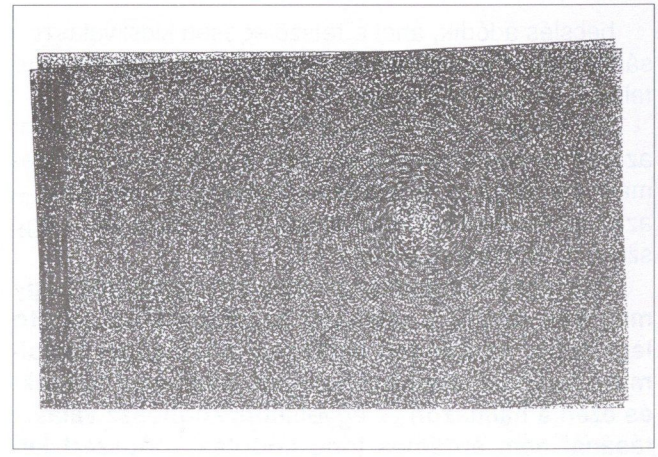
Véletlennek köszönhetően a két ábra igen érdekes vizuális tulajdonságát észleltem egy előadásom [4] előkészítése során. Írásvetítő fóliát készítettem az ábrákról, és a fólia az eredeti ábrára helyezve interferencia képeket mutatott. A 10. ábra sakktábla színezése négyzetrácsos szimmetriájú sötétedéseket mutat. Ez egyszerűen következik a sakktáblaszínezésből, nagyítva látható egy részlet a *12. ábrán*. (Ilyen elven viselkednek a Moiré-alakzatok is.)

Meglepő a 11. ábra színezésének viselkedése volt. Koncentrikus körök jelentek meg rajta. A fólia mozgatásával a körök középpontja fehér foltként vándorolt, a forgatás hatására a körök összehúzódtak, vagy tágultak. A *13. ábra* a két színezés elforgatásos öninterferenciájáról egy álló képet mutat, mozgásban a jelenség még érdekesebb.

14. ábra



15. ábra



Kicsinyítve kis mértékben a fóliát, más típusú interferencia jelenik meg: egy pontba futó sugárnyaláb, vagy egy pontba futó spirálkarok *(14. és 15. ábra)*. Mozgatás közben a középpont fehér foltként vándorol, további forgatás hatására a spirálok erősebben csavarodnak, közben beszűkülnek. (Komplementer színezéssel is megnéztem a jelenséget, minden hasonlóan viselkedik, csak a középpont lesz sötét folt.)

A jelenség mögött a véletlen tömegjelenségek alapvető tulajdonsága húzódik: egy véletlen fekete-fehér színezésben miden kis alakzat valószínűségének megfelelő gyakorisággal fordul elő.

Amikor az eredeti képre ráhelyezzük a róla készült fóliát, egy sík-transzformációt végzünk. A transzformáció sajátgörbéire illeszkedő hosszabb fekete alakzatok rajta maradnak a görbén, és egymást fedve megnyúlnak. Ezek a megnyúló alakzatok rajzolják ki az egybevágóság forgatásos esetében a köröket, centrális kicsinyítés esetében a sugárnyalábot, forgatásos kicsinyítés esetében a spirálokat.

A vizuális magyarázat mellett más magyarázata is van a jelenségnek: a sajátgörbék mentén az egymásra helyezett ábrák fekete pontjainak száma adott hosszúságú kis szakaszon nagyobb szórású, mint más görbék mentén. Ez a nagyobb szórás válik láthatóvá. A jelenséget Julesz Béla: „Dialógusok az észlelésről" c. könyvében a randompont-kinematogramok monokuláris mozgásészlelése tárgyalásánál Glass-hatás és Glass-mintázatok néven említi (Glass, 1969).

Visszatérve az algoritmikus tanulás kérdéskörére, a Kolmogorov-bonyolultság ezen a téren szintén fontos elvi szerepet játszik, segítségével univerzális tanuló algoritmusok adhatók, amelyek azonban nem kiszámíthatóak.

A Shannon-entrópiaformula a p valószínűséghez a $-\log_2 p$ információmennyiséget rendeli. Ennek megfordításaként a prefix Kolmogorov-entrópiával a

$$\pi(x) = 2^{-K(x)} \text{ eloszlást, amelyre } \sum_{x=1}^{\infty} \pi(x) < 1 \ ,$$

kapjuk a nem negatív egészek felett a Kraft-egyenlőtlenséget is felhasználva. A kiszámítható eloszlások között ez a legnagyobb bizonytalanságnak megfelelő eloszlás, amelyet a Levin-féle apriori eloszlásként emlegetnek.

Erre épül az univerzális tanuló eljárás a statisztika klasszikus Bayes-módszere szerint. A Bayes-módszer, mint a statisztikai tanulás alapmegoldása, a megfigyelt jelenség eloszlásának paraméterét adó paramétertéren a megfigyelés előtti apriori eloszlásból és a megfigyelésből a Bayes-tétel szerint számítja ki a paramétertéren a megfigyelés utáni eloszlást. A Bayes-elv szerint, amennyiben az apriori eloszlás ismeretlen, véges paramétertér esetén a legbizonytalanabbat, az egyenletes eloszlást kell választani. Végtelen paramétertérre ez nem használható, s ha a kiszámítható eloszlások világában vagyunk, akkor a nem negatív számok halmazát véve paramétertérnek, a Levin-féle apriori eloszlás választása a legjobb megoldás. Ez az alapja az univerzális tanuló algoritmusnak. Minthogy $\pi(x)$ nem kiszámítható, kiszámítható közelítései adják a megvalósítható tanuló algoritmusokat. (Lásd M. Li és P. M. B. Vitányi [5], és a The Computer Journal [6] speciális kiadását Kolmogorov Complexity címmel. Az információelmélet témakör legfrissebb hazai szakirodalma Györfi László, Győri Sándor és Vajda István [7] tankönyve.)

A véges világban – tehát a digitalizált világban is – a matematika végtelen ideális konstrukciói (végtelen kicsi és nagy, a folytonosság, univerzális algoritmusok, véletlen) csak segítenek, végtelennel közelítik a véges modellt, amit utána vissza kell véges közelítésbe hozni.

Ezzel a gondolatsorral lépjünk át a számítógépes információs rendszerek új világába.

4. Összefoglalás

Attól kezdve, hogy egy üzenet, vagy instrumentális felvétel következtében egy jel bejutott a hálóba, minden a processzorok működése szerint történik vele. A processzorokon programok futnak, amelyek megint csak valamilyen üzenetek eredményeként jöttek létre, és jel alakban is léteznek.

Az adattároló, a processzor, az adó, a vevő, a csatorna, az interakciós berendezések mind műszaki alkotások, sokszor igen finom fizikai jelenségekre épülve. Ettől még a processzorokon futó programok készítéséhez nem csak műszaki, hanem a felhasználási területre vonatkozó ismeretek is szükségesek. Láthatóan a jelek világában mindent áthat a programozás, a szoftverkészítés feladata.

Legmeghatározóbb komponensként a programozható számítógépek – domináló módon a Neumann-elvű számítógépek – biztosítják a teljes világháló működtetését. Az 1945-ben lefektetett architektúra még nincs 60 éves, a köré épülő újabb és újabb technológiák pedig még mindig megjósolhatatlan lehetőségeket hoznak felszínre. A legutóbbi 10 év dominálóvá váló legfontosabb technológiái időrendben: személyi számítógépek, Internet, World Wide Web, mobil kommunikációs eszközök, Gbit Ethernet, HTML és XML, multimédia berendezések, e-kereskedelem, GPS és térinformatika, hálózati számítás, Web Service, mobil érzékelők (beépített rendszerek+mobil kapcsolat), átható számítás (pervaisive computing).

Mindez a sok pozitív lehetőség mellett negatív jelenségeket előidéz. A számítógépes bűnözés, az információ-szennyezés és a „Nagy Testvér" mindenre kiterjedő megfigyelési lehetősége talán a legfontosabb negatív hatások.

A 3. szakaszban felvázolt matematikai modellek lehetőségeket és korlátokat mutatnak az új, digitalizált, mesterséges világot létrehozó kommunikációs technológiák számára. Ezek a törvényszerűségek tipikusan csak határértékben érvényesek, és mint sok más eszmei fogalma a matematikának, mint a végtelen nagy és kicsi, a folytonosság, valószínűség, univerzális algorit-

musok, a véges rendszereket felülről közelítik a végtelenből. Az információs technológiák a felhasználható egyre kisebb téridő-granulátumú jelek segítségével egyre nagyobb méretű véges feladatok megoldását teszik lehetővé. Egyre nagyobb mennyiségben, finomsággal, felbontással képesek a múlt üzeneteit, észleléseit feldolgozható módon megőrizni. Az információ mérőszámaira épülő matematikai törvények egyre erősebben érvényesülnek, de nem adnak megoldást feladatainkra, keresnünk kell a jó közelítő, kompromisszumos, véges megoldásokat.

Fontos felhívni a figyelmet arra, hogy miután egy üzenet, vagy észlelés jelekké kódolódott, többé már egyáltalán nem véletlen; a múltban, a kiválasztás, megfigyelés előtt volt véletlen. A múltra vonatkozó rögzült észleléseink, feljegyzéseink, ítéleteink lehetnek hiányosak, pontatlanok, homályosak, de már nem véletlenek abban az értelemben, hogy valami eloszlás jellemezné őket. Amennyiben tudnánk, hogy a múlt milyen valószínűség-eloszlásból származik, a hiányzó, homályos részeket ki tudnánk egészíteni az eloszlásra jellemző tipikus jelenségekkel, szimulálhatnánk a hiányzó részeket. Amennyiben a jövő jelenségei is ebből az eloszlásból fognak bekövetkezni, a múlthoz ebben az értelemben hasonló jelenségekre számíthatunk a jövőben.

Ami továbbra is véletlen a világhálón lévő jelek gyűjteményében, az a rárakódó zaj. Paradox módon a programok jelentik a legnehezebben kezelhető, és elkerülhetetlen zajforrást, ami téves üzenetek vételét eredményezi. Az informatikus szakemberek képzésében ez a meghatározó feladat: olyan szakemberek legyenek, akik képesek ennek a zajnak csökkentésére.

Dolgozatomban – egyáltalán nem véletlenül –, központi szerepet játszik a véletlen. A kommunikációnak kizárólag véletlen szituációk között van szerepe. Bízhatunk benne, hogy a természet és az élet lényege a véletlen, a kiszámíthatatlanság, ezért az emberi kommunikáció mégis csak az emberek között fog fennmaradni.

Kolmogorov a véletlen problémáját így foglalta össze:

„A mindennapi beszédben véletlennek hívjuk azokat a jelenségeket, amelyekben nem tudunk olyan szabályosságokat találni, amelyek lehetővé tennék, hogy pontosan előre jelezzük jövőbeli bekövetkezésüket. Általában véve, nincs alapunk abban hinni, hogy egy véletlen jelenségnek bármilyen meghatározott valószínűséggel kellene rendelkeznie. Különbséget kell tenni ezért a valódi véletlen (mint a szabályosság teljes hiánya) és a sztochasztikus véletlen (ami a valószínűségelmélet tárgya) között. Ez felveti annak kérdését, hogy magyarázatot keressünk arra, hogyan alkalmazható a véletlen matematikai elmélete a valós világra."

A válasz valahol a múlt és a jövő viszonyában kereshető. A két entrópia-fogalom közötti átjárás is erre a kapcsolatra mutat lehetőségeket. A tudományok fejlődésében ennek kihasználásában az információs technológiák fejlődése új korszakot nyitott. A múlt megfigyeléséből a jövő lehetőségeinek eloszlására következtethetünk, s beavatkozási lehetőségeinkkel a kedvezőbb irányba alakíthatjuk az eloszlást. Az emberiség kommunikációjának ez lehet a legbelső célja.

Irodalom

[1] Claude E. Shannon – Warren Waever, A kommunikáció matematikai elmélete (az információelmélet születése és távlatai), OMIKK, Budapest, 1986.

[2] Kolmogorov A.N., Three approaches to the quantitative definition of information. Problems of Information Transmission (1) 1965. 1–7.

[3] Kolmogorov A.N.–Uspenskii V.A., Algorithms and randomness. SIAM J. Theory of Probability and Applications, 32 (1987) 389–412.

[4] Benczúr András, An attempt to the algorithmic definition of fuzziness. Annales Univ. Sci. Budapest., Sect. Comp. (1991) 19–33.

[5] Ming Li,–Paul Vitanyi, An Introduction to Kolmogorov Complexity and its Applications. Second Edition, Springer Verlag 1997.

[6] Kolmogorov Complexity, Special Issue, eds. Alexander Gammerman and Vladimir Vovk, The Computer Journal, Vol. 42, No. 4, 1999.

[7] Györfi László–Győri Sándor–Vajda István, Információ- és kódelmélet, Budapest, Typotex Kiadó, 2000.

A Zigbee technológia

KOVÁCS BALÁZS, VIDA ROLLAND

Budapesti Műszaki és Gazdaságtudományi Egyetem, Távközlési és Médiainformatikai Tanszék

kovacsb@tmit.bme.hu, vida@tmit.bme.hu

Kulcsszavak: mobil távközlés, Bluetooth, személyi távközlés

Napjainkban egyre jobban terjednek a vezeték nélküli hálózatok, melyek lehetővé teszik a mobil eszközök hálózati kapcsolatát. A jelenlegi vezeték nélküli technológiák a minél nagyobb sávszélesség elérésére, és az ad hoc hálózati együttműködés támogatására koncentrálnak. Az energiafelhasználás minimalizálása csak másodlagos szerepet kapott. A hálózati trendek szerint azonban a jövő hálózatai az olyan eszközök hálózati kommunikációját is megkívánják, melyek szempontjából kritikus az energiaellátás. Eme cikkben bemutatjuk a Zigbee technológiát, melyet ezen eszközök rádiótávközlésének biztosítására fejlesztettek ki.

1. Bevezetés

A számítástechnikai és kommunikációs technológiáknak napjainkban tapasztalható összefonódása forradalmi hatása van az emberek mindennapi életére. A legszembetűnőbb jelenség a mobiltelefonok, laptopok és személyi digitális asszisztensek *(Personal Digital Assistant,* PDA) elterjedése. Eme technológiai fejlődés egy olyan szemlélet kialakulását eredményezte, mely szerint minden személy és eszköz között egy időtől és helytől független távközlési csatornát kellene fenntartani. A vezeték nélküli technológiák immáron lehetővé teszik az eszközök közötti megkívánt minőségű folyamatos fizikai kapcsolatot.

A leginkább ismert, és elterjedőben lévő vezeték nélküli átviteli technológia, az IEEE 802.11 szabványcsalád [1]. Nagyjából 50 méteres hatótávolságig 54 Mb/s átviteli sebesség elérését teszi lehetővé, mely alkalmazás szinten akár jó minőségű videó többesadást *(multicast)* is megvalósíthat. A 802.11 legelterjedtebb alkalmazási területét azon helyi hálózatok alkotják, ahol a vezetékek jelenléte nem megengedhető, vagy felesleges, ahol szükség van a hálózat egyszerű, mobil elérésére és a minél nagyobb átviteli sebességre. Ennélfogva a 802.11 technológiát használó eszközök általában PDA-k, laptopok.

Egy másik jól ismert vezeték nélküli technológia a Bluetooth [2]. Célja a relatív kis adatátviteli sebességű eszközök kábeleinek helyettesítése. Mivel hatótávolsága 10 méter körülire tehető, a Bluetooth leginkább személyi hálózatokban *(Personal Area Network,* PAN) alkalmazható. Adatátviteli sebessége 1 Mb/s, mely alkalmazási szinten 720 kb/s-re csökken. Ez a sebesség jó minőségű audio átvitelre, illetve közepes minőségű videó átvitelre képes. Leginkább telefonokba, fejhallgatókba, egerekbe, billentyűzetbe és egyéb hasonló kategóriájú adatátvitelt igénylő eszközbe telepíthető.

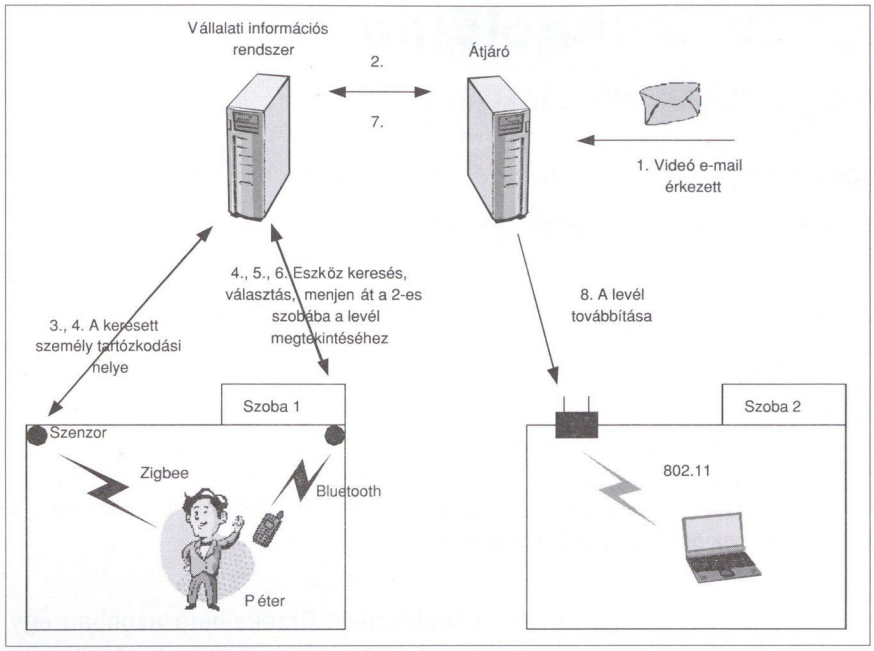
Mind a helyi, mind pedig a személyi vezetéknélküli hálózati technológiák olyan eszközöket használnak, melyek feltölthető akkumulátorral, esetleg folyamatos tápellátással rendelkeznek. Érzékelhető azonban egy olyan technológia hiánya, mely primitívebb, egyszerűbb eszközökkel is üzemeltethető. Olyan eszközökre gondolunk, melyeket nincs lehetőség naponta, vagy akár hetente energiával újratölteni. Eme probléma megoldására dolgozták ki a Zigbee technológiát.

2. A jövő hálózatai

A 802.11 és a Bluetooth technológia lehetővé teszi azt, hogy vezeték nélküli csatorna épüljön fel két, egymás hatótávolságán belüli eszköz között. Egy megfelelő hálózati infrastruktúra, a technológiák megfelelő alkalmazása és a helyes hálózati rétegbeli protokollok segítségével (címzés, útválasztó algoritmusok) elérhetjük, hogy az adott infrastruktúrán belül található minden eszköz között kapcsolatot lehessen létesíteni. Napjainkban már elkezdődött egy ilyen hálózat kiépülése, az azonban még nagyon messze van, hogy bármely két eszköz között bárhol és bármikor összeköttetést lehessen kialakítani és fenntartani.

Az elmúlt évtizedben előtérbe került egy új hálózati elképzelés, mely a fenti cél megvalósítására törekszik. A *ubiquitous* avagy *pervasive* (mindenhol jelenlévő, körülölelő) hálózati kommunikáció filozófiája arra épül, hogy mindennapjaink során ne a feladataink megvalósításához szükséges eszközökre, hanem konkrétan a feladatokra tudjunk koncentrálni. Ennek a hálózatnak a lényege egy összetett, háttérben maradó intelligens rendszer, mely úgy segíti a felhasználókat, hogy az valójában nem is tudatosul bennük. Ennek megvalósulásához összehangoltan működő, érzékelő és reagáló globális infrastruktúrára lenne szükség.

Példának említhető egy irodaházban egy olyan videó levelező-rendszer, mely mindig az aktuális tartózkodási helyünkhöz közel található kijelzőre vetíti ki az üzenetünket. Tegyük fel, hogy egy videó e-mail érkezett Péter számára, a munkahelyére *(1. ábra).* Mikor a vállalati átjáró megkapja az elektronikus küldeményt,



1. ábra A három technológia alkalmazási lehetősége egy jövőbeli hálózati környezetben

3. A Zigbee technológia

A Zigbee technológiát a Zigbee Alliance [5] nevű szervezet fejleszti, melynek számos neves ipari partner is tagja. 35 vállalat vesz részt aktívan a Zigbee szabvány kidolgozásán, közülük talán az öt legjelentősebb a Honeywell, az Ivensys, a Mitsubishi, a Philips és a Motorola. A harminc további projektrésztvevő között találhatunk félvezetőgyártással, mobil IP-vel foglalkozó cégeket és számítástechnikai eszköz *(Original Equipment Manufacturers,* OEM) gyártókat.

megkérdezi a vállalati információs rendszertől, hogy hova küldje az épületen belül a levelet. Az információs rendszer elindít egy keresést Péter személyi azonosítójára. A Zigbee segítségével az egyik szenzor érzékeli Péter azonosító kártyáját, és visszaküldi annak pozícióját az információs rendszernek. Ezek után a rendszer keres Péter közelében egy, az üzenet megjelenítésére alkalmas eszközt. Tételezzük fel, hogy talál egy Bluetooth kompatibilis mobiltelefont, vagy egy 802.11-es kapcsolattal rendelkező laptopot a szomszédos szobában. Ezek után választhat, hogy a telefonján, vagy a laptopon akarja megnézni az üzenetet. Mivel a telefon képességei nem biztos, hogy lehetővé teszik a videólevél megjelenítését, a levél interfészének adaptálásával az eszköz képességeihez igazíthatja a rendszer a megjelenítendő üzenetet. Ellenben ha Péter a laptopot választja, akkor tökéletes minőségben követheti végig a videó-levél tartalmát. Péter végül úgy dönt, hogy átmegy a szomszédos szobába. Válaszát visszaküldi az információs rendszernek, mely az átjáróval közli a levél továbbításának célcímét.

Egy másik példa keretében gondolhatunk egy olyan rendszerre is, melyben a hazafelé vezető utunk során az utcai mobil hálózat érzékeli pozíciónkat, és kiszámolva a hazaérkezésünk várható időpontját, előre beállítja az otthoni hőszabályozót az általunk kívánt hőmérsékletre.

Ahhoz, hogy ez az automatizmus működjön, szükség van többek között elektronikus személyi azonosítókra, érzékelő berendezésekre, szabályozórendszerekre stb. Olyan apró és folyamatosan működésben lévő eszközökről van szó, melyek szempontjából kritikus az energiaellátás. Nyilván senki sem szeretne a szobájában lévő tucatnyi szenzorhoz hetente elemet vásárolni, majd azokat cserélni. Mindamellett, hogy ez folyamatos kiadást róna költségvetésünkre, kényelmetlenné tenné a rendszer használatát. Eme problémák megoldására készült a Zigbee.

Ezek a résztvevők technikai hozzájárulással segítik a szervezetet, és az elkészült specifikációk hozzáférésében előnyt élveznek. Feladatuk a Zigbee technológia formálása ipari alkalmazási lehetőségekhez (Millenial Net, Atmel, Microchip, Chipcon stb.)

A Zigbee Alliance feladata egy olyan rendszer kidolgozása, mely rádiós áviteli technológiát biztosít olyan eszközök számára, melyek kis adatforgalmat bonyolítanak, de helyes működésükhöz, illetve elterjedésükhöz rendkívül fontos a minél hosszabb élettartam és a minél alacsonyabb előállítási költség. A Zigbee Alliance a halózati rétegtől az alkalmazási rétegig terjedő feladatokra fókuszál, megvizsgálva a különböző alkalmazási lehetőségeket.

A Zigbee fizikai és közegelérési vezérlő *(Medium Access Control,* MAC) rétegét az IEEE dolgozta ki, a technológia perspektíváinak követésével. Az elkészült terveket a 802.15.4 szabványban rögzítették [3].

A Zigbee olyan piacokat céloz meg, mint az ipari és kereskedelmi alkalmazások (pl. monitorozás, érzékelés, automatizálás, vezérlés), egészségügyi alkalmazások (érzékelés, diagnosztika), szórakoztató elektronika (televíziók, videók, távirányítók, játékok), számítógép-perifériák, vagy a házi automatizálás (biztonság, világítás, hőszabályozás).

3.1 A rádiós interfész

Az IEEE 802.15.4 három különböző frekvenciatartományban működik: a 2.4 GHz-es ISM sávban, a 915 MHz-es Amerikában engedélyezett ISM sávban, és Európában 868 MHz-en.

A fizikai szintű adatátviteli sebesség 20 kb/s-tól 250 kb/s-ig terjed, mely valójában maximum 128 kb/s információs sebességet eredményez. Az interferenciák ellen a rendszer direkt szekvenciális spektrumkiterjesztést *(Direct Sequenced Spread Spectrum,* DSSS) alkalmaz. A 250 kb/s-os sebesség eléréséhez másodpercenként

	Sáv	Lefedettség	Adat sebesség (kbps)	Csatornák száma	Modulációs eljárás	Chip sebesség (kchip/s)	Szimbólum sebesség (ksymbols/s)
2.4 GHz	ISM	Világ	250	16	O-QPSK	2000	62.5
868 MHz		Európa	20	1	BPSK	300	20
915 MHz	ISM	Amerika	40	10	BPSK	600	40

1. táblázat az IEEE 802.15.4 frekvenciatartományai

62,5 k szimbólumváltás szükséges, 1 szimbólum pedig 4 bitet reprezentál. A DSSS 1 bitet 4 chip segítségével igyekszik meghatározni.

A Zigbee eszközök minden adás előtt vivő érzékeléses, többszörös hozzáférést kezelő, ütközést elkerülő *(Carrier Sense Multiple Access with Collision Avoidance,* CSMA/CA) algoritmus alkalmazásával győződnek meg arról, hogy adásaik ütközés nélkül fognak lezajlani.

A rendszer maximális hatótávolsága 10 és 75 méter közé esik, de leggyakrabban 30 méter körüli. A protokoll lefoglalt időrésekkel tudja garantálni az időkritikus alkalmazások számára a kis késleltetésű adatátvitelt, az adatcsomagok célba érkezését pedig kézfogásos algoritmussal biztosítja.

3.2 Energia menedzsment

A Zigbee tervezése során a legfontosabb szempont a csekély energiafogyasztás és az olcsóság elérése volt, ezért mind a protokollvermet, mind pedig a protokoll működését ennek megfelelően optimalizálták. Egy Zigbee eszköz működése során két állapotban lehet: aktívban és alvóban. Az alvó állapot percekig, vagy akár órákig is tarthat. Aktív állapotba egy eszköz csak akkor kerül, ha a rajta futó alkalmazás(ok) úgy kívánják. Ezáltal egy átlagos Zigbee eszköz működési időtartamának mindössze 0,1%-át tölti aktív állapotban, mindez pedig jelentős mértékű energiamegtakarítást eredményez.

Példaképpen, egy 802.11 típusú rádiós interfésszel működő eszköznek folyamatos üzem esetén 667 mW-os teljesítményleadást jelent az interfész működtetése. Mindez egy folyamatosan működő 802.15.4 eszköz esetében 30 mW körül alakul. Ha ehhez hozzávesszük a 0.1%-os üzemelési szorzót, akkor jelentős mennyiségű energiát tudunk megtakarítani, mely nagyon fontos a korábban említett szenzorok és egyéb kis adatátviteli sebességgel és hosszú élettartamot igénnylő eszközöknél.

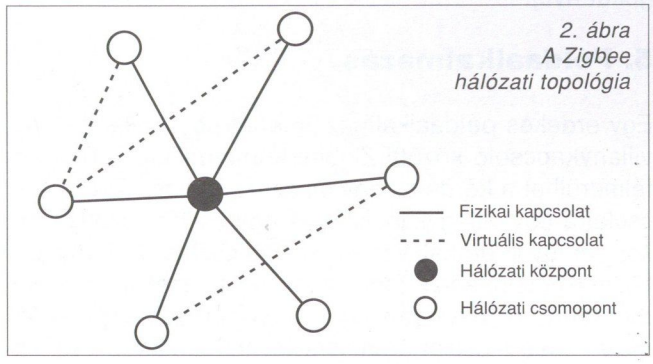
3.3 A hálózat szervezése

A technológia alapjában véve csillag topológiába szervezi a hálózatban résztvevő eszközöket, de virtuális kapcsolatok létrehozásával peer-to-peer összeköttetéseket is lehetővé tesz. Mivel a csillag topológia egy központi entitást igényel, ezért két eltérő hálózatszervezési szerepet lát el: a központba helyezi a hálózati irányítót, a csillag ágaiba az egyszerű hálózati csomópontokat *(2. ábra).*

Egy hálózatba maximum 255 csomópont szerveződhet. A központi egységnek mindenképpen olyan eszköznek kell lennie, mely folyamatos tápellátással és elegendő számítási kapacitással rendelkezik egy hálózat felügyeletéhez. Feladata a hálózat beacon üzeneteinek küldése, a hálózat felállítása, az egyszerű csomópontok szervezése, a csomópontok paramétereinek tárolása, a párosított csomópontok üzeneteinek továbbítása, és az adatok folyamatos fogadása. Az egyszerű csomópontok csak a központi egységgel tudnak közvetlenül kommunikálni. Ezen eszközök akkor küldenek adatot, ha a rajtuk futó alkalmazás igényli azt, lekérdezik a hálózati irányítót, hogy van-e a számukra tárolt adat, és igyekeznek minél több időt alvással tölteni.

A hálózati forgalom szempontjából három fajta eszközt különböztetünk meg. Egyrészről léteznek periodikus adatforgalmat bonyolító eszközök, melyek egy adott alkalmazás által definiált rendszerességgel küldenek adatot (pl. szenzorok). Ebben az esetben az eszközök a központi egység beacon jeleire ébrednek fel, és kérdezik le a központot. Másfajta forgalomtípus jellemzi a rendszertelen adatforgalmú eszközöket, melyek valamilyen külső hatás alapján dolgoznak (pl. villanykapcsoló). Az ehhez hasonló eszközök csak akkor kapcsolódnak a hálózathoz, ha szükséges, és így jelentős mértékű energiát tudnak megtakarítani. A harmadik típusba az ismétlődő, kis késleltetésű eszközök sorolhatóak, melyek kihasználhatják a rendszer *garantált időrés* opcióját (pl. egerek).

A Zigbee protokollverem megvalósítása a hálózati szerepeknek megfelelően két változatban is elkészült. A több funkcióval rendelkező verzió mindössze 32 kilobyte memóriát igényel, míg az egyszerű csomópontok számára készült változatnak körülbelül 8 kilobyte-ra van szüksége. A hálózati irányítóknak természetesen kiegészítő memóriára is szükségük van, hiszen csomópont adatbázist, tranzakciós adatbázist és párosítási táblát is fenn kell tartaniuk.



2. ábra
A Zigbee hálózati topológia

Az egyszerű hálózati topológiának köszönhetően egy entitás átlagosan 30 ms alatt épül be egy hálózatba, alvó állapotból 15 ms alatt kerül aktív állapotba, míg egy aktív egységnek átlagosan 15 ms-ra van szüksége ahhoz, hogy kommunikációs csatornához jusson.

3.4 Biztonsági kérdések

A parancsok, beacon üzenetek és visszaigazolások titkosítására a Zigbee MAC szintű titkosítást használ, egy ugrásnyi (hop) távolságnál nagyobb esetben azonban a felsőbb rétegek biztonságára támaszkodik. A MAC szint a továbbfejlesztett titkosítási szabvány *(Advanced Encryption Standard,* AES) [4] nevű kriptográfiai algoritmust használja, és sok különböző biztonsági csomagot definiál, melyek az AES algoritmusra épülnek. Ezek a biztonsági csomagok támogatják a MAC keretek bizalmasságát, integritását és hitelességét. Habár a biztonsági feldolgozást a MAC szint végzi, a felsőbb rétegek állítják elő a biztonsági kulcsokat és határozzák meg az adott esetben használandó biztonsági szinteket. Amikor a MAC szint továbbít (fogad) egy titkosított csomagot, megnézi a keret célcímét (forráscímét), ellenőrzi a címhez hozzárendelt kulcsot, majd eme kulcsot használja a keret feldolgozásához, a kulcshoz rendelt biztonsági csomag alapján. A keretekben egy bit jelzi a titkosítás használatát.

4. Zigbee vagy Bluetooth?

A Zigbee és a Bluetooth alapjában véve eltérő alkalmazásokhoz készült. Míg a Zigbee a szenzorhálózatokat, házi automatizálást és egyéb korábban említett alacsony intelligenciájú csomópontokból álló hálózatok kialakítását támogatja, addig a Bluetooth a PDA-k, mobil telefonok stb. hálózatba szervezéséhez készült.

A két technológia céleszközeinek természetesen van metszete, mely esetekben az adott alkalmazási környezet dönt arról, hogy a technológiák közül melyik az életképesebb. A Zigbee és a Bluetooth között azonban nagyon fontos különbség az, hogy a Zigbeet kis adatcsomagok ávitelére tervezték nagy méretű, statikus felépítésű, rendszertelenül működő eszközökkel teli hálózatban (255 csomópont), Ezzel szemben a Bluetooth kis hálózatban (8 csomópont) viszonylag nagy adatcsomagokat továbbít, ad hoc hálózati támogatást, valamint nagyobb adatforgalmat bonyolító alkalmazási lehetőségeket nyújt.

5. Példaalkalmazás

Egy érdekes példaalkalmazás lehet egy csillár és egy villanykapcsoló közötti Zigbee kommunikáció. Rögtön felmerülhet a kérdés, hogy mi szükség van rádiós kapcsolatra egy villanykapcsoló és egy csillár között, amikor amúgy is be kell vezetékezni a csillárt a villanykörték működtetéséhez. Természetesen a vezetékezés nem maradhat el, azonban egy hagyományos kapcsolót, mely képes a csillár áramkörét nyitni és zárni, magába a csillárba is beépíthetünk. Ezt a kapcsolót mi fizikailag nem használnánk, csak elektromos impulzusok hatására működne. Egy általunk használt másik kapcsoló viszont a Zigbee technológia segítségével egy rádiós interfészen keresztül kommunikálna a csillárral a hálózat központi egységének közreműködésével. Ezáltal a kapcsolónk semmilyen fizikai helyhez nem lenne kötve. Akár napról-napra átrendezhetnénk villanykapcsolóinkat fúrás-faragás nélkül, vagy tetszőlegesen rendelhetnénk össze lakásunk csillárait és kapcsolóit.

	Bluetooth	Zigbee
Rádiós interfész	FHSS	DSSS
Protokollverem	250 kbyte	32 kbyte
Tápellátás	Újratölthető	Nem újratölthető
Eszköz/hálózat	8	255
Link/információs sebesség	1 Mbps/720 kbps	250 kbps/128 kbps
Hatótávolság	~10 m	~ 30 m

2. táblázat Bluetooth és Zigbee összehasonlítás

Természetesen ez csak egy, a házi automatizálás témakörébe tartozó példa leírása volt. A Zigbee technológia ennél sokkal szélesebb körű felhasználási lehetőségeket kínál. Amennyiben a Zigbee az általa kitűzött célokat az elvárásoknak megfelelően képes lesz teljesíteni, mindenképpen fontos szerepet játszik majd a jövő hálózataiban.

Irodalom

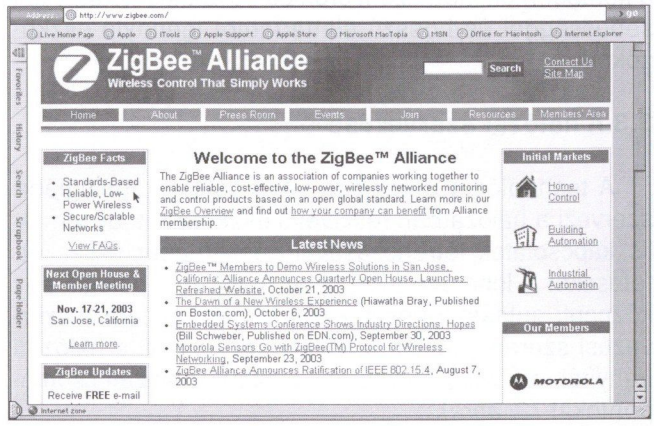
[1] IEEE Std. 802.11, 1999 Edition, http://standards.ieee.org/catalog/olis/lanman.html

[2] Jaap Harsten: "BLUETOOTH – The universal radio interface for ad hoc, wireless connectivity", Ericsson Review No. 3, 1998

[3] IEEE Std. 802.15.4, 2003 Edition, http://standards.ieee.org/catalog/olis/lanman.html

[4] National Institue of Standards and Technology – Computer Security Resource Center http://csrc.nist.gov

[5] Zigbee Alliance, http://www.zigbee.org



Hírek

A Budapesti Fasori Evangélikus Gimnázium legendás hírű tanára, Rátz László születésének 140. évfordulója alkalmából az Ericsson Magyarország Kft., a Graphisoft Rt. és a Richter Gedeon Rt. alapítványa a Magyar Természettudományos Oktatásért, az Oktatási Minisztérium képviselőjével, az iskola tanáraival együtt emlékezett meg október közepén a „Rátz László Életműdíj" névadójáról. A legendás tanár úr diákjai közé tartozott többek között Neumann János, az első számítógép megalkotója és Wigner Jenő Nobel-díjas fizikus is. Az eseményen felszólalt Kroó Norbert, az Alapítvány kuratóriumának elnöke, az MTA főtitkára. Beszédében hangsúlyozta, hogy a társadalmi szerepvállalás az oktatás területén kiemel.kedő fontosságú feladat.

Az Alapítvány díjazottjai azok a középiskolai és általános iskolai tanárok, akik az alapítók tevékenységi köréhez szorosan kapcsolódó magyarországi matematika-, fizika-, kémiaoktatás területén kimagasló szerepet töltenek be a tantárgyak népszerűsítésében és tehetséggondozásban. Az egyenként 1 millió forint összegű Rátz Tanár Úr Életműdíjat az Alapítvání kuratóriuma 2001-től kezdve évente ítéli oda 2 matematika-, 2 fizika és 2 kémiatanárnak.

Az InfoPark Alapítványt azzal a céllal alapította az InfoPark Rt., hogy a társadalom és a gazdaság fejlődését elősegítő kutatás-fejlesztési tevékenységet és annak hasznosítását támogassa. Az Alapítványhoz 1 millió forinttal járult hozzá az IVG Immobilien AG, aki az InfoPark épületeit készítette és a STRABAG Rt-vel megállapodott egy újabb, C jelű épület létrehozásáról 12.500 m^2 bérbe adható területtel. Az InfoParkban jött létre a Matáv Innovációs Központja 2000 tavaszán 18.300 m^2 területtel. Itt működik ezen kívül az IBM, a Hewlett Packard, az AXELERO és a Panasonic is. Az ipari fejlesztők szoros kapcsolatban vannak az InfoPark két alapító létesítményével, a Budapesti Műszaki és Gazdaságtudományi Egyetemmel, valamint az Eötvös Lóránd Tudomány Egyetemmel. A közös munka meghozta az eredményt és amikor az InfoPark meghirdette pályázatát, melynek jelszava az „Ötlettől a megvalósításig", 28 pályázat érkezett. Ezek közül az Alapítvány Kuratóriuma nyolcat választott ki, melyet az IVG Immobilien AG 1 millió márkás adományának kamataiból, 38,8 millió forinttal támogatott.
Az Alapítvány támogatását és az eredmények hasznosítását négy pontban hirdette meg:

- Az Alapítvány hozzájárul a kutatást-fejlesztést végző egyetemi kutatói csoportok, egyéni kutatók kutatási költségeihez, kutatási infrastruktúrájának megteremtéséhez.
- A kutatók számára ösztöndíjakat és egyéb pénzügyi támogatásokat biztosít.
- Hozzájárul a kis- és középvállalkozások kutatási-fejlesztési költségeihez.
- Pótlólagos tőkeforrásokat, befektetőket keres a vállalkozások számára.

A kuratórium az alábbi nyolc pályázatot díjazta:

1. *Szirmay-Kalos László, BME:*
   Az e-aláírás alkalmazásba vételét megalapozó módszertan kidolgozása
2. *Szencz Balázs, AITIA:*
   Hangportál fejlesztőeszközök megvalósítása
3. *Fehér Gábor, BME:*
   Biztonságos vezetéknélküli szuperhálózat elosztott környezetben
4. *Köves Gergely, Search-lab Kft.:*
   Informatikai biztonság alapjait oktató, tudatosítását elősegítő és ismeretterjesztő Internetes portál
5. *Lőrincz András, ELTE:*
   Távoktatás, távmunka, kommunikáció mozgássérültek számára:
   didaktikus készségfejlesztő eszközök és programcsomag
6. *Kiss Sándor, SenseNet Kft:*
   Vakok és gyengénlátók által is használható portálfejlesztő és publikáló platform kifejlesztése a Sense/Net Portal Engine 5.0 alapján
7. *Dr. Kovács Attila, ELTE:*
   Minőségbiztosítás a szoftveriparban: kutatóbázis létrehozása és működtetése
8. *Dr. Élő Gábor, Széchenyi Egyetem:*
   Új elvű térbeli helyzet-független mutatóeszköz kéziszámítógépekhez, mobiltelefonokhoz

November 6-án az InfoParkban dr. Bakonyi Péter helyettes államtitkár megnyitó szavai után dr. Detrekői Ákos a BME rektora adta át a díjakat. Az ülés elnöke dr. Klinghammer István az ELTE rektora volt. Az ülésen röviden ismertették a kutatások lényegét és azok megvalósítási lehetőségeit.
Nagyra értékeljük, hogy az InfoPark építője, üzemeltetője és tulajdonosai visszaforgatják a magyar szellemi erők támogatására nyereségük egy részét.

Hírek

A **Mindentudás Egyetemének** első két szemesztere során a 39 előadást a helyszínen 20 ezren hallgatták meg. Televízión, rádión és az újságokon keresztül pedig átlagosan heti 2 millió néző és olvasó követte a két szemeszter programját. Az előadássorozat internetes portálja, amely az első „tanév" alatt több mint 10 millió oldalletöltést ért el – a szeptemberben indult harmadik szemeszterben megújulva várja az érdeklődőket.

Az eseményhez kapcsolódó on-line felmérés szerint a közönség igen nagyra tartja az előadássorozatot: a válaszadók 98%-a tartja hasznosnak, 80%-a pedig nagyon hasznosnak a ME programját. Az Egyetem állandó „hallgatóságának" kialakulására utal, hogy a felmérés szerint a második szemeszterben a megkérdezettek 30%-a mind a huszonöt előadást nyomon követte, és közel hetven százalékuk az előző szemeszternek is szinte minden előadását figyelemmel kísérte. A második szemeszter oldalletöltési rekordját az Axelero Internet május 21-én regisztrálta Mihály György „Mire jó a kvantumfizika?" című előadását követően: 19.000 látogatás során 78.000 oldalt töltöttek le az internetezők.

Az online felmérés szerint az ME eseményeiben való személyes, illetve on-line részvétel a magas végzettségűek, a tudományoktól és az internettől már megérintettek elfoglaltsága. Az adatok is azt bizonyítják, hogy az ME inkább a képzésből már kikerültek, mintsem a tanulók programja: az on-line megkérdezettek több mint fele dolgozik, közel 20%-a pedig dolgozik és tanul egyszerre. Ez azt mutatja, hogy az ME honlap hatékonyan juttatja el a friss tudományos eredményeket a graduális képzésből már kikerült érdeklődőknek. Az on-line felmérésből az is kiderül, hogy a honlap látogatói rendkívül gyakori internetezők: az első szemeszter válaszadóinak több mint 60, a második szemeszter válaszadóinak 71%-a naponta internetezik, sokuknak – majdnem 70%-uknak – van otthoni hozzáférése. A munkahelyen, iskolában (is) internetezők a válaszadók 73%-át teszik ki.

Szeptemberben jelent meg az Axelero Internet támogatásával, a Print-X kiadó gondozásában Pohly Ferenc **Kattintókönyv** című kötete, amely elsősorban azoknak szól, akik eddig óvakodtak szorosabb ismeretséget kötni a Világhálóval. A szerző szerint az internetezők többsége csak a net legszűkebb szeletét használja. A Kattintókönyv őket is igyekszik új területekre, vagy akár egy új életstratégia felé kalauzolni. A könyv nem arról szól, hogyan kell kattintani, hanem hogy mire és főként miért? Pohly Ferencet munkája a legnagyobb hazai internetszolgáltatóhoz köti. Az Axeleróval közös szándék vezérelte: az Internet megismertetésén, új szempontú bemutatásán keresztül a hazai piac, azaz a felhasználók számának bővítése, a Háló használatának elterjesztése.

A 2003/2004-es tanév kezdetével a **Debreceni Egyetem** sugárúti, valamint a Vámospércsi úti kollégium épületeinek felújítását követően az épületek számítógépes és telefonhálózatának kialakítására is sor kerül. Az Egyetem döntése értelmében konvergált adat-hang infrastruktúrát építenek, így a telefonforgalmat is az adathálózaton keresztül viszik át. Az egységes adat-hang infrastruktúra részeként a két épületben új számítógépes (LAN) hálózatot alakítanak ki a Cisco Catalyst típusú eszközeivel. A kollégiumi szobákba összesen 151 darab Cisco IP telefont telepítenek. A rendszer kapcsolódni fog az NIIFI (Nemzeti Információs Infrastruktúra Fejlesztési Iroda) 26 akadémiai intézményt összekapcsoló IP hálózatához is.

Kovács Kálmán informatikai és hírközlési miniszter és Füzes Péter az **Oracle Hungary** ügyvezető igazgatója közös sajtótájékoztatón jelentették be, hogy az Oracle EMEA (Európa, Közel-Kelet és Afrika) központja Magyarországon hozza létre Oracle Data Warehouse Nearshore Center nevű új szervezetét. Az Adattárház és Üzleti Intelligencia rendszerek építésére szakosodott szervezet az Oracle Hungary részeként fog működni, magasan képzett, elsősorban a szabad munkaerőpiacról felvett informatikai szakemberek alkalmazásával. A dolgozók létszáma két év alatt el fogja érni az 50 főt. Az Oracle a központ létrehozásával a Magyarországon felhalmozódott szaktudást és szakmai tapasztalatokat kívánja hasznosítani más európai leányvállalatainál úgy, hogy a magyarországi foglalkoztatásnak köszönhetően a szürkeállomány hazánkban marad. A központ szeptemberben kezdte meg működését.

Sikerrel ért véget az **Ericsson Magyarország „Constructive Thinking"** című nemzetközi interaktív szemináriuma, melynek ebben az évben Budapest adott otthont, elismerve ezzel az Ericsson Magyarország régióban betöltött szerepét. A rendezvény keretében a meghívottak a cég legújabb, következő generációs szélessávú vezetékes- és mobil megoldásaival és alkalmazásaival ismerkedhettek meg. A szemináriumra ellátogatott Kovács Kálmán informatikai és hírközlési miniszter is. Az egyhetes szemináriumnak közel 150 vendége volt, a távközlési iparág jelentős vállalatainak képviselői személyében, mind itthonról, mind pedig a régióból, Macedóniából és Szlovákiából.

A megnövekedett felhasználói igények következtében a vezetékes telefónia kulcsszava a közeljövőben a sávszélesség lesz: a különböző felhasználói igényeknek, alkalmazásoknak a hálózat nem szab majd határt. A vendégek élő demonstráció keretében olyan alkalmazásokkal ismerkedtek meg, mint az Ethernet DSL Access (EDA), a többcélú szélessávú hálózat, on-line stratégiai játékok, videofilmek igény szerinti letöltése, illetve video- és hangátvitel.

A „Fuzzyról" általában

Igen! Nem! Vagy talán mégis?

MÉSZÁROS ETELKA

meetelka@freemail.hu

Kulcsszavak: véletlen események, sztochasztikus folyamatok

A fuzzy életünk több területén jelen van, magyarul bizonytalant, zavarost jelent. A hétköznapi életben fuzzyról beszélünk amikor nem tudjuk konkrétan meghatározni egy eszközről, hogy jó-e vagy rossz, vagy személyeknél, amikor valamilyen tulajdonságuk meghatározásánál bizonytalanok vagyunk. Bár a fuzzy módszert már sok területen alkalmazzák, de a mérnökök többsége számára nem ez az a számítási mód, mely a napi problémák megoldásánál eszükbe jutna. Messze vagyunk attól, hogy ez a munkák segítésére egyáltalán felmerülne. Ez indokolja ennek az ismertető jellegű cikknek a megjelenését.

A fuzzy története

A fuzzy aránylag fiatal tudományág. Először 1965-ben *Lotfi A. Zadeh professzor* fogalmazta meg a fuzzy halmazok matematikáját. 1974-ben megjelent a működőképes fuzzy szabály alapfogalma. Londonban, ekkor készült az első olyan rendszer amely sikeresen alkalmazta a fuzzyt – egy gőzgépet szabályozott. Nem sokkal később egy dán cementmű szabályozási feladataira is használták.

Az áttörés 1987-ben történt, ekkor készültek el a *Sendai-i metróval,* amelyet fuzzy módszerek segítségével teljesen automatizáltak. Itt egyetlen ember közreműködésére sincs szükség, mivel a szerelvények vezetőitől az állomásfőnökig mindent ellát az automatikus szabályozó rendszer. Ebben a metróban nem kell kapaszkodni, mert a rendszer alkalmazkodó képességénél fogva soha nem fékez vagy gyorsít hirtelen.

Ezt követően megjelentek a gazdasági döntéstámogató, diagnosztizáló fuzzy alkalmazások is, ma pedig a robotikán keresztül az ipari folyamatokon át, a háztartási gépekig minden területen hódit a fuzzy. 1991-ben új fordulópont következett be, ekkor mutatták be a pilóta nélküli helikopter irányítást. Jó példa a fuzzyra az iraki háborúban is bevetett követő rakéta, mely az előtte kiszámíthatatlan mozgást végző célpontokat is eltalálta.

Ezen felbuzdulva azzal foglalkoznak a fuzzy-logikusok, hogy igen nagy bonyolultságú rendszereket is sikerüljön egy fuzzy szabályrendszeren alapuló modellel kezelni. Elképzelhető, hogy néhány év múlva egész üzemeket, gyárakat fognak automatikusan vezérelni ilyen szabályozó rendszerekkel.

A fuzzy logika már az ókori filozófusok tanaiban is fellelhető. Például *Arisztotelész* (i.e. 384-322) filozófiájára jellemző volt az idealista és materialista elképzelések közötti ingadozás. Világképe egyértelműen materialista talajon állt, új kategóriákat (szubsztancia, anyag-forma, lehetőség-valóság) fogalmazott meg, és rendszerezte a valóság mozgásformáit. Gondolatait a lét egységességének, az egyes, a konkrét dolog és az általános , objektiv összefüggésének hangsúlyozásában fejezte ki. Hangsúlyozta az érzéki megismerés fontosságát, mint az emberi megismerés kiinduló pontját. Ehhez csatlakozik a tapasztalat, a világot csak érzékeinken keresztül ismerhetjük meg.

Herakleitosz (i.e. 535-475) felismerte az ellentétek egységét, egymásba való átcsapását és harcát, vagyis megfogalmazta a dialektika alaptételeit. *Parmenidész* (i.e. kb. 544) pedig idealista lételmélete alapján bírálatnak vetette alá a tapasztalati megismerést, kimutatta a természetfilozófia alapfogalmainak – mozgás, változás, lét és nemlét ellentmondásos voltát.

A filozófusok elméleteiből nyilvánvalóvá válik, hogy az élet több területére vonatkoztatva, az élet semmilyen folyamatát nem lehet csak kategorikus igen-nemmel, vagy jó-rosszal kifejezni.

A dolgokról általában egymáshoz viszonyítva állapítjuk meg azok jellemzőit. Például egy emberről mi dönti el, hogy valaki öreg, szép vagy csúnya, magas vagy alacsony. Csakis az, hogy mit tekintünk alapértéknek, mihez viszonyítjuk az illetőt. Például egy 150 cm magas ember egy pigmeus szemszögéből óriás, viszont egy kosárlabda csapat legtöbb tagjához viszonyítva igen alacsony.

Mi dönti el, hogy valaki okos, öreg, esetleg kövér? Megadhatjuk konkrétan az életkort években vagy a tömeget kilogrammban, de még ez sem visz közelebb a megoldáshoz. Hány éves kortól mondhatjuk valakire, hogy öreg? Ez esetenként változó lehet, de még ekkor sem egy ponton átlépve válik azzá. Tehát összehasonlításokkal állapítjuk meg a dolgokról, hogy azok milyen viszonyban állnak egymással, azonban, hogy teljes legyen a „zavarodottságunk" észrevehetjük, hogy ez a viszony a precíz értékek ismerete nélkül is meghatározható. Egyszerűen látjuk, hogy két ember közül melyik a magasabb.

Az ilyenfajta kételyek leküzdésére vezették be a fuzzy logikai módszereket. A fuzzy logikát minősítő vagy laza logikának fordíthatjuk.

A hétköznapi megfogalmazások után megpróbáljuk a halmazalgebra, a szabályozás minősítés, valamint a gyakorlati élet területén behatárolni a fuzzyt, ezzel talán megfoghatóvá, érthetővé válik korunk egyik évszázados alapokon nyugvó, mégis új tudományága.

A fuzzy logika halmazalgebrai megközelítésben

Amennyiben az 1-100 évesig tartó életkort a 0 és 1 tartomány közé helyezzük és tudjuk, hogy valaki 75 éves, akkor az illető öregségi százaléka 0,75.

A hagyományos logikai műveleteknél az eseményekhez hozzárendeltük a (0,1) halmaz valamelyik elemét, ezek jelentik az állítások hamis vagy igaz értékét. A fuzzy rendszerekben ehelyett az állításoknak a teljes (0,1) zárt tartományt feleltetjük meg, tehát a két érték között még tetszőleges számú köztes állapot is elképzelhető. Így elmondhatjuk valakiről, hogy eléggé magas, vagyis magasságának logikai értéke 0,75. A teljes tartományt így különböző osztályokra bonthatjuk, úgymint egyáltalán nem, egy kicsit stb.

A hagyományos logika alapját képező halmazelméletnél legyen $\mathbf{A} = (a_1, a_2, a_3, \ldots a_n)$ egy halmaz. A klasszikus logikánál egy elem halmazba tartozása egyértelműen megállapítható, egy tetszőleges, a_k elemről eldönthető, hogy az **A** halmaz eleme vagy sem. Ha beletartozik, úgy ezt egy logikai igaz, ha pedig nem egy logikai hamis értékkel jellemezzük. A logikai igaz értéket 1-el a hamis értéket 0-val jelöljük. Ebben az esetben az, hogy egy elem beletartozik-e **A**-ba, jellemezhető vagy egy 0-val vagy pedig 1-el. A fuzzy logika abban új, hogy a halmazba tartozás 0, illetve 1 értékei nem ennyire szélsőségesek, hanem köztes értékek is léteznek, amelyek megmutatják, hogy egy adott a_k elem mennyire tartozik bele a halmazba: kissé, kevésbé, nagyon vagy egyáltalán nem.

Az **A** halmazbeli a_k elemhez hozzárendelünk egy számot, általában 0-t és 1-et, ami az elem halmazba tartozásának a mértékét mutatja. Az **A** halmaz a fuzzy gondolkodással az alábbi módon néz ki:

$$\mathbf{A} = a_1\, a^{(k1)},\ a_2^{(k2)},\ a_n^{(kn)}.$$

A felső indexbe írt értékek a halmazelemekhez rendelt, halmazba tartozást jellemző számokat jelölik.

Erre jó például ha az **A** halmazunk az emberek centiméterben kifejezett testmagassága és csak az egész értékeket vesszük.

$$\mathbf{A} = (120,\ 121, \ldots . 175,\ 250)$$

A halmazelmélet szerint, ha meg akarunk határozni két részhalmazt, *M* jelölje a magas emberek halmazát, *L* az alacsony emberekét, akkor kell találjunk egy elemet, például a 175 cm, amelytől magasabb emberek az *M*=(175, 176,....200) halmazba tartoznak, míg az alacsonyabbak az *L*=(120, 121, 173, 174) halmazba.

A gyakorlatban azonban ilyen éles határokat nem szabhatunk, mert ha valaki kb. 172 cm magas azt mondjuk, hogy nagyjából alacsony. Tehát az állításunkban van egyfajta bizonytalansági tényező, körülbelül, vagy nagyjából. A fent említett, egyes elemhez rendelt értékek éppen ezt a bizonytalanságot kezelik.

Az egyes részhalmazok elemeihez hozzárendelünk egy-egy számot. Például:

$$\mathbf{L} = (120^{(1)},\ 130^{(1)},\ 170^{(0,5)}\ 180^{(0,1)})$$

$$\mathbf{M} = (120^{(0)},\ 140^{(0)},\ 170^{(0,4)},\ 180^{(0,9)})$$

A két halmazban lehetnek teljesen különböző elemek is és az elemekhez rendelt számok között sem a halmazon belül sem két halmaz között semmilyen összefüggés nincs előírva, kivéve azt, hogy „értelmes" legyen.

A legáltalánosabban definiált fuzzynak része a valószínűségi logika. Csakhogy míg a valószínűségi logikában egy kockával 1/6-os eséllyel 3-ast dobva és 1/6-os eséllyel 4-est, így a 3-as vagy 4-es dobásnak együttesen 2/6-od, azaz 1/3-ad az esélye. A fuzzy látszólag ehhez hasonló. Az irodalom szerint a fuzzynak egy része a valószínűségszámítás, vagy annak egy altenatívája.

Fuzzy alkalmazása a szabályozástechnikában

Hagyományosan a következőképpen alakul egy folyamat kétértékű logikai eszközökkel: A szabályozott folyamat különböző értékeit figyelve észrevesszük, ha azok átlépnek egy bizonyos küszöbértéket. Ekkor bekapcsol a folyamatot kiegyenlítő szabályozó rendszer és mindaddig aktív állapotban is marad , amíg a tulajdonságok újra a kritikus érték alá vagy fölé nem érnek. A fuzzy rendszernél ennél összetettebben kell eljárnunk. Először a vizsgált tulajdonságokban lévő eltéréseket fuzzy logikai értékekké kell átalakítani. Ekkor el kell döntenünk, hogy be kell-e avatkozni, és ha igen milyen mértékben. Végül a kapott logikai értéket vissza kell alakítanunk konkrét műveletté, ezt a folyamatot pedig defuzzyfikálásnak nevezzük.

Nézzük meg a fennt leírtakat egy példán: egy légkondicionáló berendezés egyik része a hideg levegőt befúvó ventilátor. Egy egyszerű programozható logikai vezérlő eszközzel a hőmérséklet bizonyos pont fölé érésekor a ventilátor bekapcsolódik. A fuzzy vezérlővel a hőmérsékletet részekre bontjuk. Így az optimális, még elviselhetően meleg és a rettentő meleg tulajdonságoknak való tartományt feleltetünk meg.

A fuzzy rendszerek előnyei a hagyományos szabályozással szemben:

Vannak olyan problémák, amelyek bonyolultak, nehezen modellezhetők és nagyon nagy számolási igényük van. Ezeknek a problémáknak a megoldásában segíthet a fuzzy, amely hasonlít egy kicsit az emberi agy természetes modellalkotására, úgy is nevezhetnénk, hogy a józan gondolkodás modelljét lehet ennek a segítségével alakítani. A problémák megoldása így könnyebb és a rendszer ügyes modellalkotásra képes.

Az emberi agynál ez a modellalkotási képesség csökkenhet (például alkoholos befolyásoltság alatt), de talán erre az állapotra is megfogalmazható egy fuzzy képlet.

A fuzzy említésekor nem feledkezhetünk meg a számítógépekről sem, melyek bizonyos értelemben már léteznek, csak még nem elterjedtek, azonban vannak olyan alkalmazásai is amelyek már mindennaposak. Mint sok minden másban a japán szakemberek a fuzzy módszerrel előállított termékekben is az élen járnak. Ilyen a fuzzy videokamera, amely egy belső fuzzy algoritmus segítségével kiszűri a remegő kéz, hajó vagy repülő okozta képrezgést. Olyan lesz a felvétel mintha álló helyzetből készítették volna. A fókuszálása is sokkal jobb, nem csak egy objektumra fókuszál, hanem tulajdonképpen az egész képmezőt figyelembe veszi bizonyos mértékig.

1998-ban Magyar Fuzzy Társaság alakult, csaknem 60 kutató részvételével abból az alkalomból, hogy az *International Fuzzy System Association* (Nemzetközi Fuzzy Társaság) új rendeletet vezetett be. Az egyéni tagságot beszüntette és kimondta, hogy csak nemzeti szervezeteken keresztül lehet a társaság munkájába bekapcsolódni. A társaságnak az a célja, hogy az érdeklődési körébe tartozó területeket fejlessze. A társaság működése nem korlátozódik pusztán a fuzzy logikára és a fuzzy halmazok elméletére, hanem magában foglalja a fuzzy technológiák, neurális hálózatok, genetikus algoritmusok, a bizonytalanság elemzése témaköröket is.

Ezzel a cikkel igyekeztünk felhívni a figyelmet egy eddig, a Híradástechnikában még egyáltalán be nem mutatott és a hazai mérnöki gyakorlatban is kevéssé használt módszerre. Reméljük, hogy hamarosan gyakorlati eredményekről is beszámolhatunk.

Irodalom

[1] James F. Brule:
Fuzzy systems - A tutorial
[2] Beszámoló a Magyar Fuzzy Társaság
1998-99. évi munkájáról
[3] Magyar Larousse,
Akadémiai Kiadó, Budapest, 1991
[4] L.A. Zadeh:
„Fuzzy sets" Info. and Ctl.,
Vol. 8, 1965

Hírek

A **nanocsövek** (Híradástechnika, 2001/10) és alkalmazásuk kutatása terén elért eredményeiért Nobel-díjjal kitüntetett Rick Smalley professzor által alapított gyár napi 1-2 font szén-nanocsövet készít. Bővítésének fő akadálya az, hogy a nanocső grammonként 500 dollárba kerül. Mivel nanocsövekben az elektronok jóval gyorsabban haladnak, vezetőképességük különlegesen jó, ami a távközlésben, mikroelektronikában, automatikában és általában az integrált áramkörökben jósol nagy jövőt számukra. Ezzel párhuzamosan az intelligens anyagokban és más ipari alkalmazásokban is egyre szélesebb körben kezdik alkalmazni.

A nanocsövek a valaha is felfedezett legjobb hővezetőnek bizonyultak, ami például zártterek hűtését forradalmian könnyítheti. Kis méreteik miatt hatszor könnyebbek és 500-szor erősebbek, mint az acél. Polimerekbe ágyazott nanocsővel megoldható villamos áram átvezetése szigetelő anyagon, vagy rendkívül erős, ugyanakkor hajlékony műanyag-tárgyak készítése, mivel a nanocsövek 120 fokban elhajlíthatók, majd eredeti alakjukra ugranak vissza. Feltételezik, hogy a nem túl távoli jövőben radarhullámokat visszaverő festékeket lehet felhasználásukkal készíteni. Másik ígéretes újdonság a pászmákból összefont szilícium-nanohuzal, amit a mai integrált áramkör-technikához könnyebben lehet adaptálni. Több vállalat keresi a módját annak, hogy 2005-ben nanocsöveket használjon lapos képcsövekben, plazmaképernyőkben és folyékony kristályos monitorokban. A nanocsövet alkotó hatszögnek egyik elrendezésében a nanocső mint fém, a másikban félvezetőként viselkedik. Utóbbiakkal remény van tranzisztorok kialakítására is.

A **Bell Laboratóriumok** új rekordot állítottak föl a fényvezetős távközlésben. 4000 km távolságra 2,5 Tb/s sebességet értek el, megdöntve az eddigi rekordot, ami 2000 km-en 1,6 Tb/s volt. A hibátlannak bizonyult átvitelre 64 DWDM útján előállított, egyenként 40 Gb/s sebességű csatornát használtak. A DPSK (differential phase shift keying) módszert alkalmazták, amit a Bell Labs nagykapacitású rendszerek számára fejlesztett ki. A kísérlet során a kutatóintézet más újdonságait is felhasználták.

Az Egyesült Államok szenátusa egyhangúan megszavazta a kéretlen elektronikus **reklámlevelek (spam)** küldésének tilalmát. A korábban közzétett elképzeléseknek megfelelően fel fogják állítani azoknak a magánszemélyeknek listáját, akikhez nem szabad spam-ot küldeni. Ha valakit emiatt feljelentenek, a bíró millió dolláros pénzbüntetést, vagy hosszabb elzárást szabhat ki. Jelenleg a spam-ok az egész elektronikus levélforgalom felét foglalják le, megzavarják az előfizetőket, a vállalkozóknak pedig több milliárd dollárjába kerülnek elpocsékolt sávszélesség és csökkentett termelékenység formájában.

(H.Gy.)

Egységes mobil távközlés szolgáltatás az európai vasutak számára*

TARNAI GÉZA, *BME Közlekedésautomatikai Tanszék*
IZABELA KRBILOVA, JIŘI ZAHRADNIK
Zsolnai Egyetem Vezérlési és Informatikai Rendszerek Tanszék

Kulcsszavak: vasútbiztonság, sínáramkörök, váltóvezérlés, vonatellenőrzés

A Nemzetközi Vasútegylet 1993-ban döntött a közcélú GSM rendszeren alapuló, egységes, nemzetközi együttműködésre képes vasúti rádiós szabvány kidolgozásáról. A szabványosítás alapján kialakított GSM-R rendszer bevezetése óta 32 európai nemzeti vasúttársaság vállalt kötelezettséget. Az új technológia közös, integrált platformot képez a különböző vasúti alkalmazások magasabb szolgáltatási színvonalú megvalósítása, többek között az egységes európai vonatbefolyásoló rendszer számára.

1. A Morse-távírótól a GSM-R-ig

A vasúti közlekedés az egyes állomások és a vonalhálózat egészének kiterjedtségéből, valamint a sokszereplős, bonyolult vasútüzemi technológiából adódóan a távközlési szolgáltatások hagyományos fogyasztója. A vezetékes összeköttetések (telefon, távíró) már a vasutak korai szakaszában is szolgálták az üzemi technológiát. Ilyen kapcsolatrendszer épült ki például

- az egyes állomásokon a forgalomirányítók (forgalmi szolgálattevők) és a váltóőrök, váltó- és sorompókezelők,
- az egymással szomszédos állomások forgalmi szolgálattevői,
- a két állomás forgalmi szolgálattevői és az állomások közötti vonalszakaszon szolgálatot teljesítő térköz- és sorompóőrök,
- a forgalmi szolgálattevők és a vonal forgalma fölött diszponáló menetirányító között.

A különböző szakszolgálatok (forgalom, kereskedelem, gépészet stb.) végrehajtó szolgálati helyeinek egymással és a felsőbb irányítási szintekkel való összeköttetésére kialakult a vasutak saját üzemi távbeszélő hálózata is, amely összeköthető a nyilvános hálózatokkal is. Nem egy szolgáltatás korábban, vagy nagyobb mértékben valósult meg a vasutak saját hálózatában, mint a nyilvános hálózatokon (például az automatikus távválasztás az akkori Csehszlovák Vasutak és a MÁV üzemi távbeszélő hálózatában).

Számos vasútüzemi technológiai előrelépést jellemző módon a mobil kommunikáció megjelenése és fejlődése tett lehetővé. Ilyen például a mozdonyrádiók több évtizeddel ezelőtti megjelenése vagy a kocsifelírók és a tolatócsapatok munkáját megkönnyítő hordozható készülékek elterjedése a vasutak üzemvitelében.

Tekintettel arra, hogy az egyes szolgáltatások az elmúlt több mint száz évben a legkülönbözőbb időszakokban, egymástól függetlenül, az akkori műszaki fejlettségnek megfelelő szinten valósultak meg, és korszerűsítésük is időben elhúzódó volt, az ezen szolgáltatásokat megvalósító távközlő hálózatok általában nem, vagy csak nehézkesen köthetők össze egymással.

Az összekapcsolást gátló kompatibilitási problémák még nagyobbak lehetnek, hogyha nem egyetlen, hanem több ország vagy vasúttársaság vonatkozásában vizsgáljuk őket. Ez például azt jelentheti, hogy a mozdonyokat a határállomáson vagy ki kell cserélni, vagy eleve számos, különböző rádióberendezéssel kell felszerelni. Még bonyolultabb a helyzet a pályamenti jeladó elemekről kapott információk alapján működő ún. vonatbefolyásoló berendezéseknél, hiszen ezekből Európa vasútjain közel 30 féle rendszer üzemel.

Az Európai Unió által a vasutak számára kitűzött cél, az egyes vasutak közötti akadálymentes átjárást jelentő interoperabilitás csak úgy valósítható meg, ha a vasutak egész Európában egységes kommunikációs platformot használnak.

Mivel a mobil kommunikációnak a vasútüzemen belül is egyre nagyobb a szerepe, és a GSM révén korszerű, tömeges felhasználása miatt kiforrott, kiterjedt szolgáltatásokkal rendelkező technológia áll rendelkezésre, amely a hagyományos hálózatokkal is összekapcsolható, célszerűnek látták a vasutak, hogy az egységes kommunikációs platform szerepét a GSM speciális vasúti igényeket is kielégítő változata töltse be. A Nemzetközi Vasútegylet (UIC) 1993-ban döntött a köz-

**** Nagyon vigyázunk arra, hogy a Híradástechnika hasábjain ne jelenjenek meg olyan cikkek, melyek más kiadványban már szerepeltek. Ezúttal azonban kivételt teszünk, és a PKI Tudományos Napok 2003 kiadványából kisebb módosításokkal átvesszük Tarnai Géza és szerzőtársainak munkáját. Az késztet bennünket erre a szokatlan lépésre, hogy elolvasva a cikkben szereplő specifikációt, az pontosan megegyezik azzal, amit a hazai biztonsági szolgálatok rádió-hálózatától megkövetelnek (Tetra, Tetrapol, EDR). Bízunk benne, hogy ezzel is segítünk a döntés meghozatalában, hiszen ez egy Európában elfogadott, bevált, Magyarországon is települt cégek gyártmánypalettáján szereplő rendszer, melynek üzemeltetésében már tapasztalatok is vannak.***

célú GSM rendszeren alapuló, egységes, a nemzetközi együttműködő képességet maximálisan támogató vasúti rádiós szabvány kidolgozásáról. A szabványosítás alapján kialakított GSM-R rendszer bevezetésére azóta 32 európai nemzeti vasúttársaság vállalt kötelezettséget, közöttük a Szlovák Vasutak (ŽSR) és a MÁV is.

A nemzetközi együttműködő-képesség biztosításán túlmenően a GSM-R rendszer bevezetése további előnyöket is nyújt az alkalmazó vasúttársaságoknak. Amellett, hogy lehetővé teszi az elavult, egyre nehézkesebben és költségesebben működtethető analóg technika kiváltását, közös, integrált platformot képez a különböző vasúti alkalmazások magasabb szolgáltatási színvonalú megvalósítása számára is. További előny, hogy egységes kommunikációs rendszerbe foglalja a jelenlegi, eltérő műszaki megoldású és frekvenciatartományú

- vonali rádiórendszereket,
- állomási technológiai rádiókörzeteket és
- munkairányító rádiórendszereket.

A GSM-R technológia nyújtja a kommunikációs infrastruktúrát az egységes európai vonatbefolyásoló rendszer (ERTMS/ETCS) 2. és 3. szintjének kialakítására, de egyes alkalmazásokban szerepe lehet már az 1. szintnél is. Az új technológia a közvetlen vasútüzemi alkalmazásokon túlmenően az utasok számára is számos új szolgáltatás bevezetését teszi lehetővé (például helyfoglaló rendszerek és jegykiadó automaták felügyelete, az utasok aktuális tájékoztatása a vonaton).

A GSM-R technológia az ETSI *(European Telecommunication Standards Institute)* GSM szabványain, valamint az UIC által megfogalmazott, vasútspecifikus feltételrendszeren (EIRENE) alapul. A rendszer lehetőséget nyújt arra is, hogy a konkrét implementációk során az előbbiekkel összhangban figyelembe vegyék az egyes vasúttársaságok speciális előírásait is.

2. A GSM-R rendszer szolgáltatásai

A GSM-R rendszer szolgáltatáskészlete a nyilvános GSM hálózatok számára szabványosított, a GSM 2+ fázisnak megfelelően specifikált és kipróbált alap- és kiegészítő szolgáltatásokra épül. A GSM-R-en belül vasútspecifikus elemeknek tekinthetők a szolgáltatásminőségi (QoS) paraméterekkel szemben támasztott szigorúbb követelmények és a speciális, vasúti alkalmazások.

Vasúti alkalmazás esetén az egyik legfontosabb specialitás a GSM-R-nek a vonatbefolyásolás rendszerében való alkalmazása, ami miatt nagy sebességű mobil felhasználókkal kell számolni (max. 500 km/h). Többek között ez az oka annak, hogy egyes paraméterekkel szemben szigorúbb követelményeket támasztanak.

Ilyenek például a következők:

- a hívásfelépítési idő,
- a sikeres hívások aránya,
- a hálózat rendelkezésre állása,
- az adatátviteli késleltetés,
- az adatátviteli hibaarány,
- az adatátviteli hibastatisztika eloszlása.

Ezeket a paramétereket természetesen több tényező is jelentősen befolyásolja, mint például

- a hívásátadások gyakorisága,
- hívásátadások sikerességi aránya (min. 99,5%),
- hívásátadási idők (max. 300 ms megszakadási idő),
- a rádiófrekvenciás lefedés a pálya mentén és
- számos egyéb tényező.

A következőkben néhány vasút-specifikus szolgáltatást mutatunk be. Ezek

- a gyors hívásfelépítés,
- körözvény- és csoporthívás,
- prioritási és megszakítási rendszer,
- funkcionális címzés és
- a helyfüggő címzés.

2.1. Gyors hívásfelépítés

A nyilvános GSM rendszerekben a hívásfelépítési idő akár 10 s, vagy nagyobb is lehet. A vasúti alkalmazások a hívások gyors és garantált felépítését igénylik. A hívásfelépítési időre vonatkozó, a hívás prioritásától függő követelmények a lenti *táblázatban* láthatók. Ezeknek az értékeknek az esetek 95%-ában teljesülniük kell, de a maradék 5% esetén sem szabad túllépniük a megadott értékek másfélszeresét.

2.2. Körözvény- és csoporthívás

A GSM-R körözvényhívás és csoporthívás a nyilvános hálózatokra vonatkozó GSM 2+ fázisban definiált szolgáltatásokon alapul. Mind a körözvény- mind a csoporthívás mindig egy adott területre és egy adott felhasználói csoportra vonatkozik. Körözvényhívás során egyirányú kapcsolat épül fel a hívást kezdeményező és egy hívási csoport tagjai között, azaz csak a hívást kezdeményező fél beszélhet, a hívottak passzív résztvevők. A csoporthívás viszont kétirányú kommunikáció, melynek során a hívott felhasználóknak bizonyos korlátozásokkal válaszadási lehetőségük van: egyidejűleg csak egy csoporttag tud beszélni, és a kezdeményező fél bármikor magához veheti a beszédet.

A hívásfelépítési időre vonatkozó, a hívás prioritásától függő követelmények

A hívás típusa	Hívás-felépítési idő
Vasúti vészhívás	<1s
Mobil készülékek közötti sürgős csoporthívások	<2s
Minden, a fenti osztályokba nem tartozó vasútüzemi hívás	<5s
Valamennyi, alacsonyabb prioritású hívás	<10s

A felhasználói csoportok összetétele mind a tagok, mind a terület vonatkozásában rugalmasan konfigurálható a rendszerben. Egy felhasználó több csoportnak is a tagja lehet. A csoport- és a körözvényhívás csak azokkal a csoporttagokkal épül fel, akik az előre meghatározott területen tartózkodnak. Ha egy résztvevő csoporttag felépült csoport- vagy körözvényhívás alatt elhagyja ezt a területet, akkor számára megszakadhat a hívás. Ugyanakkor, ha egy csoporttag akkor lép az előre definiált területre, amikor felépült csoport- vagy körözvényhívás van folyamatban, az ő készüléke is automatikusan belép a hívásba.

2.3. A prioritások kezelése

A vasúti távközlési rendszerekben a különböző fontosságú hívástípusokat célszerű megkülönböztetni annak érdekében, hogy a legfontosabb hívások akkor is létrejöjjenek, ha a hívott fél foglalt, vagy a rendszer olyan mértékben terhelt, hogy normál hívás felépítéséhez nem képes erőforrásokat biztosítani. Ennek érdekében a magasabb prioritású hívások megszakíthatják az alacsonyabb prioritásúakat.

A GSM-R rendszer a GSM 2+ fázis prioritási rendszere alapján öt felhasználói prioritási szintet különböztet meg 0-tól 4-ig. A legmagasabb prioritást a 0 jelenti. A vasúttársaságok közötti együttműködő-képességet a prioritási szinteknek a Nemzetközi Vasútegylet (UIC) általi egységes meghatározása garantálja. A hívási prioritásokat az alábbi *táblázat* tartalmazza.

A hívás típusa	Prioritás
Vasútüzemi vészhívás	0
Vasútbiztonsági vezérlőutasítás	1
Nyilvános vészhívás	2
Vasútüzemi hívás	3
Vasúti tájékoztatás és egyéb	4

2.4. Funkcionális címzés

Vasútüzemi szempontból ez a GSM-R egyik legfontosabb szolgáltatása. Alapja a GSM rendszerben definiált előfizető követési szolgáltatás. A lényege az, hogy egy adott szolgálati beosztást ellátó személyt mindig ugyanazon, a szolgálatot meghatározó számon lehessen felhívni, függetlenül attól, hogy éppen ki tölti be ezt a szolgálati beosztást.

Így például amikor a felhasználó a munkája során az 512. sz. vonat mozdonyvezetőjévé válik, akkor a telefonja menürendszerének segítségével bejelentkezik a beosztásának megfelelő funkcionális számra. Ettől kezdve ő ezen a számon is hívható a saját telefonszáma mellett. Amikor a vonat a végállomásra ér, és a felhasználó már nem tölti be ezt a beosztást, akkor kijelentkezik, majd a későbbiekben, amikor új szolgálati beosztást lát el, az ennek megfelelő funkcionális számra jelentkezik be.

A funkcionális hívószámok segítségével, a mozdonyt azonosító pályaszám ismeretében, bármely mozdony is felhívható, függetlenül attól, hogy éppen hol tartózkodik, és milyen feladatot lát el. Ugyanígy felhívható a vonatszám alapján bármely vonat mozdonya akkor is, ha nem ismert, hogy melyik mozdony továbbítja a vonatot.

A funkcionális hívószámok alapvetően három részből állnak:

- hívástípus –
  meghatározza, hogy pl. csoport-, körözvény-, vonat-, kocsi-, mozdony-, vagy egyéb hívásról van-e szó;
- felhasználó azonosító szám –
  a szolgálati hely, illetve a jármű azonosító kódja;
- funkció kód –
  a szolgálati helyen belül a konkrét beosztást, munkakört határozza meg.

A funkcionális számozási rendszer jelentős része nemzetközi előírások alapján van feltöltve, azonban nemzeti alapokon definiálható számmezők is vannak, hogy a rendszer az országonként, illetve vasúttársaságonként fellépő sajátságokat is ki tudja szolgálni. A vasutak közötti roaming szerződések megkötése után akkor is felhívható lesz a felhasználó ugyanazon a funkcionális számon, ha nem a saját vasútjának a területén tartózkodik.

2.5. Helyfüggő címzés

A helyfüggő címzés lehetővé teszi a mobil készülék által kezdeményezett hívásoknak az felhasználó földrajzi tartózkodási helyétől függő állomásra való automatikus irányítását. A vonali rádiórendszer esetében ez például azt jelenti, hogy ha a mozdonyvezető az e célra szolgáló rövid hívószámmal meghívja a menetirányítót, akkor a mozdony tartózkodási helyének megfelelő irányítói szakaszt felügyelő központ felé kell a hívást felépíteni, azaz a rövid hívószámot a helytől függő, fix hálózati hívószámmá konvertálja a rendszer. A rendszer annak alapján, hogy a hívó melyik cellában tartózkodik, egy adatbázisból kikeresi a területileg illetékes menetirányító fix hívószámát, és a hívást erre a számra irányítja át.

Helyfüggő címzéssel a diszpécser jellegű szolgálatokat célszerű ellátni. A területi illetékességi határok szabadon megválaszthatók, minden helyfüggő hívószámnál különböző lehet. A cellák közötti átfedésből adódóan az, hogy egy készülék mikor kerül át az egyik cellából a másikba, a pillanatnyi terjedéstől a cellák kihasználtságáig sok mindentől függ. Ha a felhasználó cellahatáron tartózkodik, és a cellahatár egyben illetékességi határ is, akkor bizonytalanná válhat a helyfüggő címzés. A funkcionális számozás megfelelő kialakítása azonban segíthet a bizonytalan címzés áthidalásában.

3. Rendszertechnikai sajátosságok

A GSM-R rendszertechnikailag alapvetően azonos felépítésű, mint az alapját képező GSM rendszer. Itt csak azokra a jellemzőkre térünk ki, amelyek a közcélú és a

vasúti alkalmazásoknál egymástól eltérnek, vagy a vasúti alkalmazások szempontjából különösen fontosak. Az eltérések, illetve specialitások részben a vonatbefolyásoló rendszerben történő alkalmazással függenek össze, melynél nagy megbízhatóságú adatátvitelt kell megvalósítani az igen nagy sebességű járművekkel (a szabvány 500 km/h értéket ír elő).

A vasúti alkalmazások céljára a 876...880 és a 921 ...925 MHz sávot jelölte ki az európai frekvencia-hatóság. Ez a 2x4 MHz-es sáv szomszédos a GSM kiterjesztett 880...915, illetve 925...960 MHz-es tartományával. A csatornaosztás 200 kHz.

A vivőfrekvenciák:

$f_{up}(n) = (876 + 0{,}2 \times n)$ MHz
(a mobil készülék adási frekvenciái) és

$f_{down}(n) = (f_{up}(n) + 45)$ MHz
(a bázisállomás adási frekvenciái),

ahol $0 < n < 19$.

Egy-egy rádiófrekvenciás csatornán 8 forgalmi csatorna (időrés) kerül átvitelre. Az átviteli sebesség 16 kbit/s, amiből legfeljebb 14,4 kbit/s a hasznos átvitel sebessége. A GSM-R-ben is rendelkezésre áll a nagysebességű vonalkapcsolt és a csomagkapcsolt adatátviteli szolgáltatás (HSCSD, illetve GPRS).

A GSM-R hálózatokban a fix hálózat kialakítását a vasút speciális jellemzői és követelményei határozzák meg. Ilyen jellemző az, hogy az ellátandó terület a vasúti pálya nyomvonalának viszonylag szűk környezetére terjed ki. A bázisállomás által egy adott frekvencián lefedett terület, a cella alakja elsősorban a sugárzók kialakításától függ. Vasútvonalak lefedésére általában szektorsugárzókat, nagy kiterjedésű állomások ellátására körsugárzókat alkalmaznak.

A fix hálózat kialakítása befolyásolja a hívásátadások sikerességét is. Sikeresnek azokat a hívásátadásokat kell tekinteni, amelyek során a hívásátadás alatti burst adatátviteli hibák nem haladják meg az erre specifikált értéket, és a hívásátadást követő 10 sec alatt az adatátvitel hibamentes (nem történik többszörös hívásátadás). Az EIRENE specifikáció szerint a tervezésnél figyelembe vett terhelésnél a vasútvonal mentén 99,5%-ban sikeresnek kell lennie a hívásátadásnak.

Annak érdekében, hogy a nagysebességű vonatok miatt se kelljen nagy cellaátlapolást megvalósítani, és ezáltal rontani a sikeres hívásátadások arányát a lassú vonatok esetében, a hívásátadási folyamat optimalizálására van szükség.

Az optimalizálásra
- a hálózattopológia megfelelő kialakítása,
- a hívásátadási szakaszok megfelelő megválasztása és
- a hívásátadás idejének csökkentése kínál lehetőséget.

Vasúti rendszereknél el kell kerülni, hogy a hívásátadási területek megállóhelyekre, állomásokra vagy olyan pályaszakaszokra essenek, ahol a vonatok lassan haladnak, és ily módon többszörös hívásátadásnak legyenek kitéve.

A vasúti alkalmazások nyomvonalhoz kötött rendszere és a nagy megbízhatósági igény miatt a bázisállomásokat célszerű gyűrű topológia szerint csatlakoztatni a bázisállomás-vezérlőkhöz. Az átviteltechnikai hálózat adottságainak megfelelően egy gyűrűre általában 4-6 bázisállomást fűznek fel.

A hálózat kialakításánál figyelembe kell venni a rendelkezésre álló vasúti távközlési infrastruktúrát is, amely felhasználható a GSM-R távközlési infrastruktúrájának kialakítására. A vasúti távközlési rendszer általában a vasútállomásokon rendelkezik a GSM-R rendszer bázisállomásainak csatlakoztatására alkalmas leágazásokkal. A bázisállomásoknál minden rádiófrekvenciás egység (TRX) egy teljesítményosztón keresztül két, a vonal két irányába sugárzó szektorsugárzó antennára csatlakozik, és létrehoz egy, két térbeli szektorból álló, kompozit cellát. Így elérhető, hogy a hívásátadási területek ne az állomások közelébe essenek.

4. Hálózatépítés, önműködő vonatbefolyásolás

A GSM-R gyakorlati alkalmazása érdekében több vasútnál kísérleti szakaszok épültek. A sikeres vizsgálatokat követően a belga, a finn, a holland, a német, az olasz, a svájci, a spanyol és a svéd vasutaknál megkezdődött és további nyolc országban hamarosan megkezdődik a GSM-R vasúti mobil rádiós hálózat országos kiépítése.

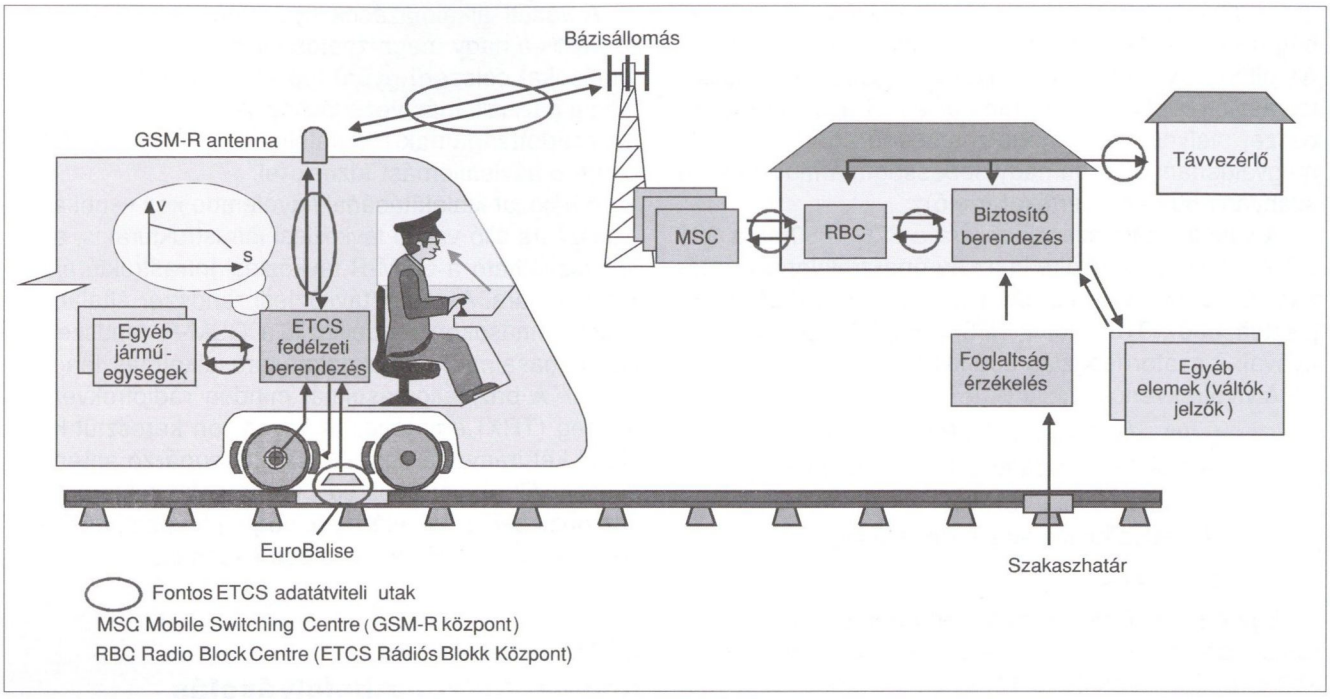
Magyarországon a GSM-R rendszer országos kiépítése még nem kezdődött meg. Elkészült viszont egy pilotrendszer a transzeurópai IV. korridor 100 km hosszúságú szakaszán, Szolnok és Békéscsaba között. A műszaki, szolgáltatásminőségi tesztek befejeződtek, és kiváló eredményeket mutattak.

Szlovákiában a Bratislava és Kuty közötti 70 km-es szakaszon épül egy pilotrendszer. Az európai vasúti pályahasználat liberalizálása, illetve ezzel összefüggésben az interoperabilitás iránti fokozott igény megkívánja, hogy a közeli években, a többi vasúthoz hasonlóan, a ŽSR és a MÁV is legalább a Transzeurópai Hálózathoz (TEN) tartozó vonalain kiépítse a GSM-R hálózatot.

Amint már említettük, az egységes európai vonatbefolyásoló rendszer (ERTMS/ETCS) 2. és 3. szintjén a forgalomirányító központ és a vonatok közötti kommunikáció is a GSM-R technológián alapul.

Az ETCS 2. szint rendszerfelépítése a túloldali *ábrán* látható.

A biztosítóberendezések ellenőrzik az egyes állomási és vonali vágányszakaszok foglaltsági állapotát, vezérlik a váltókat és jelzőket, majd ennek alapján adják meg az egyes vonatok számára a továbbhaladáshoz a menetengedélyt. Az egyes körzetek biztosítóberendezéseitől összegyűjtött információk az ETCS biztosítóberendezési központon (RBC) és a GSM-R kapcsolóközponton (MSC) keresztül jutnak el a megfelelő bázisállomásra, majd onnan a megcímzett vonatra, az



Az ETCS 2. szint rendszerfelépítése

ETCS fedélzeti berendezéséhez. A menetengedély a pálya meghatározott pontjáig szól. Ahhoz, hogy a fedélzeti berendezés ki tudja számítani az ún. sebességprofilt, azaz a vonat számára megengedett maximális sebességet a menetengedélyben szereplő határponttól való távolság függvényében (v-s görbe), szükség van a vonat pillanatnyi helyének meghatározására. Ehhez a pálya meghatározott pontjain elhelyezett, transzponder elven működő, úgynevezett Eurobalise-ok, mint „elektronikus kilométerkövek" nyújtják az alapinformációt, és a mozdonykerékre szerelt jeladó révén határozható meg a legutóbb érintett balise elhagyása óta megtett út. A fedélzeti berendezés a fékezés automatikus kiváltásával őrködik azon, hogy a vonat ne lépje túl a számára megengedett sebességet, illetve hogy a menetengedélyben előírt pont előtt biztonsággal megálljon.

Az ETCS 3. szintje annyiban tér el a 2. szinttől, hogy a nagy beruházási igényű és üzemeltetési költségű hagyományos foglaltságellenőrzést (sínáramkörökkel vagy tengelyszámlálókkal) a hozzá tartozó kábelhálózattal együtt elhagyják, és a fedélzeti berendezés közli a rádiós központon keresztül az érintett biztosítóberendezéssel a vonat helyét.

Az ETCS 1. szintjén a vonatok a menetengedélyt nem rádió útján, hanem a pálya felől, a forgalomszabályozó jelzők állásától függő információt továbbító baliseoktól kapják. Mivel azonban ezeket a jeladókat csak a pálya bizonyos pontjain telepítik, célszerű lehet az adott vasútvonalon működő GSM-R segítségével kétkét ilyen pont között a fedélzeti berendezés számára úgynevezett in-fill információ átvitele.

A közelmúltban pilotprojektek keretében Európa számos vasútján végeztek ETCS rendszerteszteket, néhány szakaszon megindult a rendszer üzemszerű alkalmazása is. A MÁV eddig az V. transzeurópai korridor részét képező Zalalövő-Hodos szakaszon helyezett üzembe ETCS rendszerű vonatbefolyásolást (1. szint), és megkezdődött a rendszer kiépítése a Budapest-Hegyeshalom fővonalon is.

A többi európai vasút elképzeléseihez hasonlóan, az elkövetkező években a transz-európai vonalhálózat teljes szlovákiai és magyarországi részén is fokozatosan kiépül az ETCS rendszere. Így a GSM-R bázisú ETCS európai szintű elterjedésével belátható időn belül elérhetővé válik a határon átlépő forgalom vonatkozásában a teljes körű interoperabilitás.

Irodalom

[1] Balás E.:
A vasúti mobilrádiózás jelene: a GSM-R,
Vezetékek Világa, VII (2002) 3., pp.2-4.

[2] Deutsche Bahn:
Europa-Premiere –
ETCS startet Serienerprobung bei Tempo 200
http://www.lok-report.de/

[3] Mosóczi L., Tóth P.:
Main Streams of Railway Telecommunication and Signalling Development in Hungary ŽEL 2003,
Žilina Railways ont he Edge of the 3th Millenium
„On the way towards the 'European' Railway"
Žilina, Szlovákia, 2003. május 27–28.

[4] Pachl, J.: Systemtechnik des Schienenverkehrs,
Teubner, Stuttgart/Leipzig/Wiesbaden, 2002.

[5] Tarnai G.:
Az informatika szerepe a vasúti forgalomirányításban,
Híradástechnika, 2003. szeptember

Nincs királyi út

Beszámoló a World Telecom 2003-ról

DR. LAJTHA GYÖRGY
lajtha.gyorgy@ln.matav.hu

Kulcsszavak: ITU, Telecom Forum, kiállítás

Négyévenként az ITU Genfben világkiállítást rendez, és ehhez kapcsolódik a Telecom Forum, melyen hat napon keresztül kiemelkedő egyéniségek tartanak előadásokat a szakmai aktuális kérdéseiről. Ennek a hagyománynak idei állomása sok tekintetben eltért az évtizedes szokásoktól, és a mostani, 9. World Telecom számos gondolkodásra késztető változással lepte meg a résztvevőket.

1. Első benyomások

A kiállításon végig sétálva hiába kerestük az Ericsson, Alcatel, Siemens, Motorola, Nortel, AT&T, DT, France Telecom, British Telecom stb. pavilonját, mert nem voltak jelen ezen a világméretű megmérettetésen. A konzervatív nézelődő ezután nem tudta, hogy a távközlés fejlődéséről hol szerezhet reális képet. Sok, eddig soha nem hallott név, apró pavilonokban várta a látogatókat. A körülbelül 700 kiállító közül 650-nek a neve eddig ismeretlen volt a World Telecom korábbi látogatói előtt. Ennyi helyre bemenni, megkérdezni, hogy mit csinálnak, mi az újdonság és ebből kiválogatni a valódi újdonságot, reménytelen vállalkozásnak látszott.

Jelentős, nagy pavilonnal mutatkozott be az Intel, a Furukawa, az Ecotel, a Sagem, az alkatrész gyártó cégek közül pedig a Microsoft, a TANDBERG és még néhányan a szoftveriparból. Jelen volt a szórakoztató ipar számos képviselője (Samsung, Toshiba, Sony, Sanyo, Panasonic). ők építették a legnagyobb pavilonokat. Érezhető volt, hogy legtöbb cég igyekszik több lábon állni. A korábban jellegzetesen szoftvertgyártók és szórakoztató elektronikát készítők nemcsak a saját területükön, hanem a távközlésben is részt kívánnak szerezni. Múltjuk és jelenük alapján a jelenleg legnagyobb gazdasági sikerrel kecsegtető tartalomipar megalapozói és irányítói is ebből a körből fognak majd kikerülni.

A távközléssel kapcsolatban a japán NEC, az NTT és DoCoMo valamint a Korea Telecom és SK Telecom Co., Ltd., a kínai Huawei és a ZTE Corporation gyártók, szolgáltatók mutatkoztak be több emeletet kitevő anyagokkal. Ezekből is látszik, hogy Európa és Észak-Amerika visszavonult és átvette az uralmat a távol-kelet.

Ennek a változásnak valószínűleg *Yoshio Utsumi, az ITU főtitkára,* a World Telecom főszervezője és vezéregyénisége örült a legjobban. E japán jogász nem csak a kiállításra nyomta rá a bélyegét, hanem a fórum fő mondanivalójára is. Korábban körülbelül 70-80%-ban műszaki újdonságok, érdekes szolgáltatások megvalósítása, hálózattervezés, fényvezető-technika és űrtávközlés töltötte ki a programot. Jelenleg öt fő téma szerepelt: Távközlés-politika, Üzleti kérdések, Technológia, Fejlődő országok távközlése és a Plenáris szekció. Ez utóbbi jelentősége minden eddiginél nagyobb volt, mert a kezdő napon, vasárnap reggel 10-től délután 5-ig csak plenáris ülések voltak, a további négy napon pedig reggel 9-től 12.30-ig szintén ezeken az üléseken hangzottak el olyan témák, mint a liberalizációk haszna, a piac változásai, beruházási stratégiák, a fejlődő világ számára használható technológiák, új üzleti modellek és bevételi források. Természetesen nem hiányzott a sorozatból az információs társadalom világkonferenciájának beharangozása sem.

Bár volt néhány kiváló előadó és hangzottak el érdekes politikai, gazdasági és szervezési nézetek, de mint minden társadalom- és gazdaságtudományi kérdés, nem vehető át kritika nélkül. Látszólag ezen kívánt segíteni a módszer, hogy a plenáris üléseken volt egy moderátor, két vezérelőadó és két-három hozzászóló. Sajnos azonban igazi vita nem alakult ki. A 1,5 órás szekciókban a jó szervezés hatására a hozzászólók főként az előadó nézeteit igyekeztek támogatni, vagy példákkal aláhúzni.

Ezzel kapcsolatban még visszatérünk az egyik fő problémára, a fejlődő világ kérdéseire. Ennek felvezetéseképpen többször elhangzott, hogy a világ 6 milliárd lakosa közül 3 milliárd egyáltalán nem rendelkezik távközlési hozzáféréssel. Ez a számarány többször felmerült kiegészítve azzal, hogy az a 3 milliárd, aki rendelkezik hozzáféréssel, annak nagy része, körülbelül fele sem teljes körű kapcsolat és általában nem közvetlenül személyre szóló.

2. A feltörekvők

Végigjárva a standokat és hallgatva az előadásokat úgy látszott, hogy a fejlődés talán csak Távol-Keleten folyamatos. A ismertetett műszaki megoldásokat is főként e terület vállalatai mutatták be. Így például érdekes újdonság volt a hatalmas pavilonban, különböző bemutatókkal, gyártmány- és szolgáltatás-ismertetőkkel megjelenő Huawei Technologies, amelynek nevét nagyon kevesen hallották korábban. Ide sorolhatjuk az LG-t is, melynek monumentális pavilonjában folyamatos műsor szórakoztatta a látogatókat. Ugyancsak váratlan újdonság volt a Sony, a Sanyo, a Sharp és a Panasonic megjelenése a professzionális elektronikai piacon. Kínát a ZTE és a Huawei képviselte. Viszont érdekes, hogy Finnország egyáltalán nem mutatkozott be jellemző cégeivel, például nem volt jelen a Nokia sem.

Úgy nézett ki ezek után a bemutatott termékek sora, mintha a feltörekvők elfoglalták volna mindazokat a területeket, amelyekről a befutott, elismert távközlési gyártók és szolgáltatók kivonultak. A nagy változás azonban nem jelentett egyértelmű előrelépést. Az új cégek döntő mértékben úgy képzelték el a világ fejlődését, hogy csak az általuk gyártott terméket kellene mindenkinek használni.

Itt jelentkezett először, hogy nincs egyetlen olyan módszer, amely mindenkinek, mindig megfelelő lenne. Hiába akarták elhitetni a mobilgyártók, hogy övék a jövő és szélessávú professzionális célokra is csak mobilt fognak használni. Az informatikai cégek szerették volna bemutatni, hogy Internet alapon minden információ eljut egészen a felhasználó asztaláig, és ezzel az egy csatlakozással a gazdasági élet, a szórakozás és a társadalmi kapcsolatok egyaránt megvalósíthatók. Az elmúlt négy év feltörekvő jelszava az Ubiquitous vagy más néven Pervasive Networks a mindenhol elérhető, hozzáférhető hálózat szintén többször elhangzott és volt, aki ezeknek jósolt világméretű sikereket. Ugyanezt ígérték a WLAN-gyártók is, és nehéz volt megérteni, hogy e három név, vagyis a mindenütt elérhető, a bármikor elérhető és a vezeték nélküli helyi hálózat, mely szintén mindenhonnan lehetővé teszi a kapcsolatok létrehozását, miért különbözik egymástól.

A feltörekvők tehát igyekeztek a látogatókat és a fórum hallgatóit meggyőzni arról, hogy újat és egyedül üdvözítőt találtak ki, gyártanak és adnak el. De nem biztos, hogy a forradalmiak többet tudnak, mint a konzervatívok. Egyértelmű volt azonban, hogy lényegesen agresszívebben igyekeznek eladni magukat és termékeiket.

3. A fejlődő világ problémája

A piac és a gazdaság kérdéseivel foglalkozó előadások előtérbe helyezték azt a 3 milliárd embert, akinek egyelőre még nincs távközlési kapcsolata. Afrika, Ázsia és Dél-Amerika területén olyan hatalmas piac kínálkozik, amely a nehéz helyzetben lévő gyártók és szolgáltatók számára hosszú évekre feladatot ad. Ezzel kapcsolatban számos lelkes előadás hangzott el. De nem jelentkezett ennek a közösségnek egyetlen egy képviselője sem, aki elmondta volna, hogy pontosan mire van szükségük. Nem biztos, hogy amit a legfejlettebb országok leggazdagabb gyárai kitalálnak, az valóban boldogabbá teszi azokat a forró égövi embereket, akik eddig kunyhóikban néhány állataikkal és az őserdő bőséges kínálatával körülvéve is boldogok voltak.

Nem látszott az az egyetlen, olcsó, egyszerűen kezelhető, könnyen telepíthető megoldás, ami ezt a közösséget gyorsan bevonná a távközlési szolgáltatások használatába és összekapcsolná a világ többi részével. Többször hangsúlyozták, hogy ez a kapcsolat első lépésben oktatási, egészségügyi és kereskedelmi előnyökkel járna, melynek következménye képpen megtermelnék azt a pénzt, amellyel a távközlési eszközöket ki lehet fizetni. A felvázolt modell meglehetősen optimistán itt be is fejeződött. Nem merült fel az a kérdés, hogy a megtérülés 5-10 évére milyen bank, vagy milyen vállalkozás merne hitelt adni. Nem kaptunk arra sem választ, hogyha majd megérkezik a berendezés és ennek segítségével megkezdődik az oktatás, kellően karban tudják-e tartani és üzemeltetni az oda telepített rendszert. Ennek a hatalmas piacnak a megszerzése csak akkor lehet sikeres, ha ehhez az ott élők aktív közreműködését is meg tudják szerezni és szakmai képzettségüket kellő szintre tudják növelni.

4. Nehéz az informatikát kiállítani

A kiállítással kapcsolatos problémák lehet, hogy nem is elháríthatóak. Egy autókiállításon bemutathatók a gépkocsik, különböző érdekes módon megismerhetjük a teljesítményüket, amint látjuk, hogy a felemelt hátsó kerék hogyan tud néhány tonnás ólomtömböt felemelni, és volt már példa arra, hogy a Volvo-t percenként mártották bele sós vízbe és emelték ki, és bárki megszemlélhette, hogy sem a kárpit, sem a fémszerkezet nem változott ennek hatására. Ugyancsak sok érdekességet lehet látni építészeti kiállításokon, ahol a sok új forma, szín, anyag mind az esztétikai benyomást, mind az épület minőségét garantálja.

Az Infocom mindkét komponense, az informatika és a távközlés is nehezen szemléltethető pavilonokban. A szoftver intelligenciája, vagy a hardver megbízhatósága nem olyan, hogy az arra sétáló figyelmét magára vonná. Nem alakult ki az a módszer, amely színekkel, mozgással egyértelműen érdekesen, szakszerűen és meggyőzően mutatná be az adott termék, hálózat, vagy szolgáltatás tudományát. Nincs még meg az Infocom kiállítások kultúrája. Az arra sétálókat nem tudja becsalogatni egy képernyő éles színekkel és kontrasztokkal, vagy önmagában egy jó zene a pavilon előtt. Az eredményeket csak akkor tudják a látogatóknak bemutatni, ha azok bemennek a pavilonba és ott a szubjektív összehasonlítására is mód nyílik és a szakértők felhívják a figyelmet azokra a módszerekre, amelyekkel elérték a kiváló kép és hang minőségét. Ehhez sok esetben speciális filmek és hanghatások szükségesek. Nem valószínű, hogy egy nagy képernyő ma már bárkit is arra késztetne, hogy abba a pavilonba, vagy bokszba bemenjen, és bent a fentieknek megfelelően értékelhetné a jobb minőséget szolgáltató technikát.

Ennek következtében kevés látogató volt a standok és tárlatok kapujában, és aránytalanul sokan igyekeztek a tanácstalanul sétálókat becsábítani. Betérve a pavilonba már leírásokkal és a vitrinekben lévő elemekkel dokumentálták a kiállítók, hogy termékük, vagy szolgáltatásuk a legjobb a világon. Ez azonban az emberi erőforrások gazdaságtalan kihasználásához és sok lézengő szakemberhez vezetett.

Érdemes megemlíteni, hogy Magyarországot közvetlenül egyetlen cég, a Hungarocom képviselte, amely szellemesen mutatta be ábrákon és berendezéssel a világítási hálózat távközlési felhasználását (Power Line Communication, PLC). Közvetve magyar érdekeltség jelentkezett a Consultronics pavilonban, ahol a kanadai cég képviselője elmondta, hogy tulajdonosa magyar és bemutatott számos hálózatvizsgáló műszert, melyek nagy része magyar fejlesztések eredménye.

5. A fórum előadásai

A szekciókban sokan beszéltek szabályozási kérdésekről. A Magyarországon is jól ismert Bob Bruce egy valóban érdekes szekciót vezetett, melynek 1,5 órájában a szabályozás gazdasági háttere és politikai fontossága kellő arányban szerepelt. Ez az előadás a különböző fejlődési szinten és politikai rendszerben élő országok számára is tanulságos volt. Kevésbé volt egyértelmű a 3G frekvenciasávjának értékesítése és ennek haszna az állam vagy a szolgáltatók számára. A szekcióban megjelent a fejlődő világ kérdése, hangsúlyozva, hogy milyen módon lehet bekapcsolódni az ottani politikai és szabályozási munkába. Igyekeztek a távközlési kérdéseket más területeken (út- és vízépítési) szerzett tapasztalatokkal alátámasztani.

Az egyik szekció megpróbálta a felhasználó igényeit felmérni és ehhez illeszkedő megoldást ismertetni. Itt már nagyon erősen kiütköztek az üzleti érdekek. Az előadók háttere meghatározta, hogy milyen módszert

tart egyedül üdvözítőnek. Természetesen, ha több előadást sikerült meghallgatni, akkor kiderült, hogy sok „egyedül üdvözítő út" van.

Mind a műszaki szekció, mind a fejlődő világ számára ajánlott előadások között számos olyan volt, amelyet nyolc évvel ezelőtt még leparancsoltak volna a pódiumról. Egyértelmű és szigorú elv volt a válogatások során, hogy ez a fórum szakmai tudományos nézetek terjesztésére, és nem gyári propaganda céljára szerveződik. A válogatás során kiestek mindazok a javaslatok, melyeknél félni lehetett, hogy az előadó munkaadó gazdájának akar reklámot csinálni. Az elvek igen szigorúak voltak. A programbizottság elnöke a kanadai Keith Hoffmann, az 1987-es fórumon ott ült az első sorban, és ha néhány mondat után azt tapasztalta, hogy az előadó nem a benyújtott előadást mondja el, hanem reklámszöveggel igyekszik a hallgatóságot félrevezetni, szólt a szekció elnökének, aki 2-3 perc után felállt, és felhívta az előadó figyelmét, hogy nem ezt az előadást fogadta el a bizottság, ezért legyen olyan kedves távozzon a pódiumról és adja át a helyét a következő előadónak. Félek, hogy az idei évben Hoffmann úrnak nagyon sok dolga lett volna...

A fő mondanivaló azonban mégis nyomot hagyott a hallgatóság fülében. Így például a digitális azonosítók és azok kiosztásáról számos megfontolásra érdemes szempontot hallottunk. A szélessávú technológiák egységes IP kezelése szintén érdekes koncepció volt, de nem biztos, hogy mindenütt és minden körülmények között szabad követni. A Voice over IP témája is megjelent ebben a sorozatban és az előadó sok érdekes szempontot mutatott be a hang egységes kezelésére. Különböző ajánlások és szabványok ezt lehetővé teszik, de folyamatosan felmerült, hogy mindig és mindenütt az egységes kezelés jelenti-e az optimumot.

A műszaki szekció számos előadója a fejlődők ellátásának a kérdéseit mobil-rádiós technikával javasolta megoldani. Ennek során találkoztunk az Ubiquitous távközlés technológiájával, a WLAN egyszerűségének bemutatásával és a 3G várható gyors terjedésével. Különösen ez utóbbi keltett a hallgatóságban kétségeket, mert bár a példák azt mutatták, hogy a GSM sokkal gyorsabban terjedt, mint bárki azt elképzelte volna, de lehet, hogy csak egyszer volt Budán kutyavásár.

A szervezőket dicséri, hogy egy új szekciót létesítettek, melyben csak fiatalok tarthattak előadást. A hallgatóság is főként fiatalokból állt, mindazokból, akik valamelyik témában érdemleges gondolatokban gazdag előadást, vagy cikket nyújtottak be. Az elképzelés igen sikeres volt. Olyan élménnyel gazdagodhattak, ami valószínűleg egész pályájukra hatással lesz. Látókörük szélesedett és kapcsolatkörük túlterjedt az országhatárokon. Ezt a kezdeményezést mindenképpen érdemes lesz folytatni.

6. A háttér

Átnézve az előadók, elnökök, hozzászólók jegyzékét talán még soha nem találkoztunk annyi név előtt a His Excellency megjelöléssel, mint most. A megnyitó ünnepségen és az esti fogadáson részt vett a spanyol király, akit mindenhová a többszáz éves díszöltözékében felvonuló svájci gárda tagjai kísértek. A gárda zenekara is bemutatta tudományát. Az előadások közti szünetekben, valamint amikor a spanyol király bejött, vagy kiment a teremből, indulókkal szórakoztatták a közönséget.

Igen sok ország minisztere, miniszterelnöke vállalt szerepet a Telecom sikerének előmozdítása érdekében. Ezek közül többen előadást is tartottak, természetesen nem a szakmai részletekről, hanem a vezetés, és a politika szempontjából szükségesnek, fontosnak tartott kérdésekről. Különös érdeklődésre tartott számot a HP elnökasszonyának előadása, aki a gazdaságpolitikát, a humánpolitikát és a műszaki eredményeket élvezetes előadásban ötvözte.

Furcsa benyomás alakult ki azokban, akik a régebbi professzorok, főmérnökök és kutatók helyett a politikai és gazdasági élet vezetőit látták a programban. Láttunk felvonuló csapatot zászlóval, amelyre az van írva, hogy előre a tudás társadalmáért, de mindenki tudja, hogy a felvonulás a pénz uralmáról szól. Bizonyos jóindulattal össze lehet kötni a zászló jelmondatát a valódi céllal, ugyanis a tudás megszerzéséhez pénz kell és a pénz sok esetben alkalmas a tudás megszerzésére. Itt azonban sok esetben még ez a kapcsolat is háttérbe szorult. Nagyobb hangsúlyt kapott a piac, az értékesítés és a vállalatok fellendülése. Szűkebb értelemben pedig a World Telecom 2003 anyagi támogatását várták a különböző területen hatalommal és támogatási lehetőséggel rendelkező vendégektől.

Ennek ellenére felmerült, hogy esetleg változtatnak a Telecom rendszerén. Egyik lehetőségként kínálkozik, hogy Genf helyett Barcelona lenne a következő kiállítás és fórum színhelye. Erre utalt a királyi látogatás is. Kérdéses a négyéves periódus fenntartása is. A következő World Telecom az előzetes hírek szerint 2006-ban lenne, vagyis a négy év helyett három év múlva. Ennek indoka a gyorsan változó technika. Nem látszik egyértelműen, hogy a földrészekre kihelyezett Telecomok mennyiben előnyösek a World Telecom szempontjából. Ezt a kérdést is várhatóan a pénz fogja eldönteni.

Genf talán a világ legdrágább városa, de ugyanakkor a város és a kanton is mindent megtett annak érdekében, hogy a vendégek jól érezzék magukat. A tömegközlekedés mindazok számára ingyenes volt, akik a fórum részvételt igazoló emblémát kitűzték a kabátjukra. Igyekeztek a fórumhoz igyekvőket, vagy onnan haza igyekvőket, a járatok sűrítésével és rendkívül sok kedves rendező eligazításával, tanácsával támogatni. Látszott, hogy nemzetközi összejövetelek szervezésében a város valóban profi. A Palexpo területén is barna egyenruhás lánykák siettek azonnal a segítségére mindenkinek, aki egy pillanatig is tanácstalanul nézett szét.

7. Összefoglalás – nincs királyi út

A távközlés területén a tanulságok azt mutatják, hogy minden ország, minden társadalmi réteg, minden feladat más módszereket tudna leginkább használni. A konvergencia inkább azt jelenti, hogy bizonyos eszközök bármely megoldásra rendelkezésre állnak. Így például a széles sávú gerinchálózat hullámhossz-osztású fényvezetőkkel alkalmas a legtöbb szolgáltatás megvalósítására. Még a mobil rendszerek gerinchálózatának megvalósítására is ez a leggazdaságosabb módszer. Ezen belül valószínűleg a szálak és a hullámhosszak döntő többsége Internet protokoll alapján csomagok átvitelével használható ki legjobban. Az átvivő protokoll azonban már nem biztos, hogy egységes, némely esetben az új SDH konténerek, az MPLS protokoll, vagy az ETHERNET lehet előnyös.

Ezen túlmenően a felhasználók igénye szabja meg, hogy milyen információkat és milyen formában akarnak elérni? A beszédátvitel területén a mobil technikának egyértelmű előnye van. Kérdéses azonban, hogy ki kívánja a szélessávú elérést is mobil készülékkel megvalósítani. Így vannak hívei a 3G, vagy UMTS technikának, de sokan ezeket az információkat inkább lakásukban vagy irodáikban szeretnék elérni. Így az adatátvitelre, távszolgálatokra, ezen belül kiemelkedően a távoktatásra és több munkahelyen egyidejűleg végzendő közös munkára az IP látszik előnyösnek. A szélessávú szórakoztató műsorok pedig akár műholdon, akár fényvezetőn keresztül eljuthatnak a lakásba, és nem látszik még tisztán, hogy kell-e az MPEG3, vagy MPEG4 komprimált jelét még csomagolni is, vagy esetleg közvetlenül átvinni, de lehet gyorsabban letölteni és bármikor megfelelő minőségben megnézni.

A probléma megoldása a felhasználóktól függ, miért és mennyit hajlandók fizetni. A kérdés sokakban felvetődött, de Marko Jagodits annyira komolyan vette ezt a problémát, hogy a szlovén egyetemmel, távközlési gyárral és szolgáltatóval együtt konferenciát szervez 2004 májusában Next Generation User címmel. Az ötlet nem csak új, hanem lehet, hogy számos felmerülő kérdésre a világ minden részéből érkező felhasználók, valamint egyetemi és ipari szakemberek gyakorlatilag is alkalmazható ötleteket fognak megfogalmazni. Nyilvánvaló, hogy ez sem lesz egységes, mindenkire ráhúzható, de legalább talán kialakul, hogy melyik szolgáltatás milyen módon legyen elérhető, és ehhez milyen eszközökkel kell a hálózatot továbbfejleszteni.

8. Függelék

Néhány jellemző adat
az ITU World Telecom 2003 kiadványaiból.

8.1. Kiállítók száma országonként

Ausztrália	2
Ausztria	3
Azerbajdzsán	1
Belgium	28
Brazília	1
Bulgária	1
Kanada	27
Kína	6
Costa Rica	1
Csehország	3
Egyiptom	16
Faroe-szigetek	1
Finnország	20
Franciaország	87 *
Németország	23
Görögország	1
Hong-Kong, Kína	5
Magyarország	1
Izland	1
India	11
Írország	16
Izrael	36
Olaszország	18
Japán	24
Jordánia	1
Korea	9
Kuvait	1
Lettország	3
Libanon	1
Malaysia	1
Monaco	1
Hollandia	12
Új-Zéland	1
Norvégia	3
Lengyelország	1
Románia	1
Orosz Szövetség	36
Szlovénia	2
Dél-Afrika	1
Spanyolország	27
Svédország	12
Svájc	52
Törökország	5
Ukrajna	2
Arab Emirátus	2
Nagy-Britannia	143
USA	80

Megjegyzések:

** Itt jelent meg számos nemzetközi testület.*

*** Több ország (Finn, Angol, Francia, Orosz, Spanyol, Svájc, USA) számos kis kiállítónak lehetővé tette, hogy egy közös ország-pavilonban állítson ki. Ezzel a kis cégek költségei jelentősen csökkentek.*

8.2. Néhány szakterület szerepe a kiállításon

Nagyon tanulságos átnézni, hogy milyen fő címek alá csoportosították szakmai szempontból a kiállítókat. Mivel ez a kiadványban közel 30 oldalt tesz ki, ezért úgy gondoltam, hogy elég megadni, hogy hány hasábot foglalnak el a különböző területek.

Alkatrészek és szerelvények **9 hasáb**

Jelentős területet foglalt el a fotonikai elemek gyártása (Furukawa Electric, Sagem), másik kiemelkedő terület az antennák és annak szerelvényei, de itt találhatók az egyenirányítók, a napelemek, az integrált áramkörök és a napelemek is (Fujikura, Intel, Sony Memory Stick).

Végponti berendezések **12 hasáb**

Melyben kiemelkedő szerepet kaptak a mobil eszközök 2,5 G (Sony és ZTE), általában a mobil terminálok területén ugyancsak az előbbiekben már említett cégek játszottak vezető szerepet. A komputer-telefon integrációban is jelentős cégek igyekeztek bemutatni termékeiket. Szakmailag új terület volt az interaktív beszéd válaszadó berendezés, és számos intelligens, titkosított rendszer bemutatása.

Hálózati infrastruktúrák **26 hasáb**

Szinte minden cég valamilyen módon igazolni akarta, hogy távközléssel is foglalkozik, ezért mindazok, akik már korábban jelentkeztek, mint alkatrész vagy végberendezés szállítók megjelentek az infrastruktúra fejezetben is. A rengeteg jelentkező közül legtöbben mobil készülékeket, szélessávú rendszerek eszközeit, adatátviteli végberendezéseket, DSL rendszereket mutattak be. Itt is szerepeltették magukat a fényvezetősök, az optikai elemek készítői és a felügyeleti rendszerek műszereit bemutató kisebb-nagyobb vállalkozások. Érdekes, hogy az NGN (a következő generációs hálózatok) alatt meglátogatott cégek valóságban nem tudtak semmi meglepően újat bemutatni.

Szatellit termékek és szolgáltatások **3 hasáb**

Itt 3 fő témakör jelent meg: a szatellit távközlés, műsorszórás és helymeghatározás. Számos nagy antennát lehetett látni és a mobil berendezések gerinchálózata kapott még szerepet.

Kisegítő szolgáltatások **14 hasáb**

Melyek közül a számlázás és az OSS voltak talán csak igazán kiállításra érdemes témák. Itt jelentkeztek ugyanis a Call Center megoldások, a tanácsadó cégek, a felhasználók megnyerésére szakosodott egyéb tanácsadók, a nemzetközi szervezetek, a hálózattervezők, az újság és könyvkiadók.

Vizsgáló és mérőműszerek **3 hasáb**

Itt láthattunk valóban működő kiállított eszközöket, meglepő újdonságokkal azonban nem találkoztunk.

Értéknövelt szolgáltatások **13 hasáb**

A távközlés alkalmazásának számos területét lefedték, mint például konferencia rendszereket, pénzügyi szolgálatokat, hitelkártyákat, tájékoztatást, Internet hozzáférést, üzenetközvetítést mutattak be, melyek sok apró újdonságra világítottak rá.

8.3. A kiállítók tájékoztatói

Legtöbb kiállítónak nem volt akkora helyisége, hogy ott sajtótájékoztatót tarthatott volna. A konferencia-helyiségek környezetében voltak 20-40 fős kisebb termek, melyeket kibéreltek, és ahol egy-egy termékről, szolgáltatásról bemutatót láthattunk vagy előadást hallhattunk. Ismert cégek meghirdetett összejövetelein megteltek a termek, sőt a Cisco tájékoztatón például pótszékek voltak és többen álltak. Ha az újságírók nem ismerték a céget, nem voltak nevezetes termékeik, akkor még a 20 fő befogadására alkalmas termek sem teltek meg.

Jellemző az is, hogy kevés volt a látogató és az újságírók is csak 3-4 napot töltöttek el Genfben. Úgy érezték, hogy ennyiből elegendő információt szereztek olvasóik tájékoztatására.

Hírek

A World Wide Web Consortium Magyar Iroda, az MTA SZTAKI (Magyar Tudományos Akadémia Számítástechnikai és Automatizálási Kutatóintézete) és az Axelero Internet által szervezett **„Tartalom és információs infrastruktúra" elnevezésű műhelykonferencia** a digitális magyar valóság jelenlegi és a közeljövőben létrehozandó infrastruktúrális rendszereit vizsgálta, elemezve a meglévő társadalmi gyakorlatot, a hálózati rendszereket és az intézményeket. Az eddigi gyakorlat szerint a kormányzati, ágazati stratégiák leginkább a digitális információhoz való hozzáférés (internethozzáférések száma) vagy az általános számítógép-használati képességek fejlesztéseinek irányába mozogtak, a felhasználókat azonban a tartalom érdekli leginkább. Alapvető cél tehát a digitalizálás, a digitalizált nemzeti vagyon/kultúra országos méretű technikai-technológiai hátterének megteremtése és az ehhez szükséges országos, intézményi, közösségi szinten jelentkező infrastruktúrák kialakítása.

Az Axelero Internet szerint az internettel foglalkozó vállalatoknál az internetpenetráció növeléséhez a magyar nyelvű tartalmat kell fejleszteni annak figyelembe vételével, hogy nem csupán a meglévő felhasználók igényeit kell kielégíteni, hanem azt a több millió embert is, akik nem interneteznek még. Ezért támogat a vállalat minden olyan kezdeményezést, amely elősegíti a magyar tartalom és internetkultúra erősödését. Jó példa erre az Axelero Internet által kiadott [origo], amely a rengeteg tematikus oldal mellett idén áprilisban kiegészült egy bevásárlóközponttal, vagy a Mindentudás Egyetemének az [origo] szerkesztésében készülő internetes portálja.

Az internetszolgáltatók jelenleg még domináns hozzáférés-szolgáltatói szerepe a jövőben meghaladható, és még komolyabb szerepet kell vállalniuk a hálózati kommunikáció világában, hiszen az új technikák által biztosított tartalom fontosabb és érdekesebb, mint maga az infrastruktúra. A tartalom megfelelő minőségű használatához szükséges technikai fejlesztéseket, informatikai erőforrásokat olyan módon kell az internetszolgáltatónak integrálnia és infrastruktúraként felkínálnia, hogy mindez láthatatlan legyen a tartalomszolgáltatók és tartalomfogyasztók számára.

A W3C Magyar Iroda 2002-ben alakult meg az MTA SZTAKI Elosztott Rendszerek Osztályán. Az MTA SZTAKI a W3C-vel együttműködve azon dolgozik, hogy hazánkban is meghonosítsa azokat a szabványos megoldásokat, amelyekkel lehetővé válik az internetes tartalom jóminőségű és széleskörű elterjedése és hozzáférhetősége. Olyan projektekkel vesz ebben részt, mint például az Elosztott digitális hangtárak a közösségi rádiózásért (StreamOnTheFly), online szótár, plágiumkereső rendszer, internetes szavazások.

Távközlési Ifjúsági Világfórum 2003, Genf

KONTOR KORNÉLIA, *kontor.kornelia@sch.bme.hu*

Kulcsszavak: ITU, Telecom Forum, nyilatkozat

A Nemzetközi Távközlési Egyesület Telecom World 2003 kiállítása és Fóruma történetében idén először tartottak ifjúsági fórumot. Az ITU 189 tagállama két-két – az ITU tevékenységi körének megfelelő felsőfokú tanulmányokat folytató – fiatalt delegálhatott az ifjúsági fórumra, melyen ösztöndíjasként, Magyarország képviseletében vehettem másodmagammal részt.

A 20. század ipari társadalma apránként átalakul a 21. század igényeinek és lehetőségeinek megfelelő információs társadalommá. Ebben a változásban kulcsszerepet játszanak az információs- és távközlési technológiák (ICTs), melyek segíthetnek az életminőség javításában, gazdasági növekedésben, szociális és kulturális fejlődésben. Eszközként szolgálhatnak a nyomor, tudatlanság és betegségek elleni harcban, ellensúlyozhatják a globalizáció okozta károkat. Fontos szerepet játszanak a tudásterjesztésben, oktatásban, médiában, kikapcsolódásban, ugyanakkor hatással vannak a társadalmi kölcsönhatásokra, gazdasági- és üzleti folyamatokra.

Mind a Világfórum, mind az Ifjúsági Fórum lehetővé tette, hogy a fejlődő országok igényei, szükségletei találkozhassanak a fejlett országok által kínált lehetőségekkel. Megteremtette az interaktív kommunikáció lehetőségét a polgári-, ipari-, üzleti körök, kormány-, stratégiai döntéshozó szervek, nemzetközi szervezetek képviselői között, hogy közösen találjanak megoldást az észak-dél, városok-vidéki területek, kulturális különbségek által keltett szakadékok áthidalására. Alkalmat teremtett szabványok előkészítésére, fontos stratégiai döntéseket meghozatalára.

A világfórum programja délelőttönként plenáris üléseken, délutánonként – a még részletesebb tárgyalás érdekében három tárgykörre (technológia, üzleti élet, szabályozás és államvezetés) bontott – vitákon, konferenciákon való részvételt kínált a résztvevőknek. Az előadások és az azokat követő viták globális kérdéskörök felvázolását, széles körre kiterjedő problémák megoldásának keresését tették lehetővé. A különböző országokat, kontinenseket képviselő előadók tudatos megválasztása nagymértékben segítette a problémák több aspektusból történő megvilágítását, körüljárását.

Az ifjúsági fórum az ipar jeles képviselőinek előadásai, vitadélutánok és egyéb kulturális-, társadalmi rendezvények révén próbálta megvilágítani a fórum jelmondatának fontosságát. 'Helping the world communicate', azaz segítsük a világot a kommunikációban. Ahogyan a fórum egyik kiadványában olvasható, biztosítani kell a feltételeket, hogy minden ember egyenlő eséllyel férhessen hozzá a néha életet jelentő kommunikációs csatornákhoz, hogy megteremthessünk egy virágzó és békés világot.

Az ifjúsági fórum résztvevőinek feladata volt egy nyilatkozat elkészítése is. A nyilatkozat azon problémák, valamint megoldásukra irányuló alternatívák felvázolását tartalmazza, melyeket a 189 – különböző földrajzi-, gazdasági-, politikai-, társadalmi-, természeti-, kulturális adottságokkal rendelkező – országból érkező fiatalok döntő többsége a legsürgetőbbnek talált, s melyek megoldásában kulcsfontosságúnak tartottuk az egész világra kiterjedő együttműködés megvalósulását. A dokumentumban kifejtettük az alapkövetelményeket az információs és távközlési technológiák alkalmazása érdekében, melyek a gazdasági és szociális fejlődés elsődleges mozgatói. A nyilatkozat továbbá tartalmazza a kommunikáció, illetve az információhoz való hozzáférés, mint alapvető emberi jog biztosításának szükségességét. Kiemelt fontosságúnak ítéltük meg a szabályozás, finanszírozás, befektetés, infrastruktúra és oktatás területeivel való foglalkozást is. A nyilatkozat a *http://www.itu.int/wsis/newsroom/news/telecom/YF%20Declaration.doc* címen érhető el.

A kiállításon felkereshettem olyan standokat, melyek egy jelenleg még kissé futurisztikusnak tűnő, ám hamarosan Magyarországon is valósággá válható képet villantottak fel. A konferenciák az előadók jelentősen eltérő szemléltének és megközelítésének köszönhetően fontos összefüggésekre világítottak rá. A társadalmi rendezvények kapcsolatok, ismeretségek kialakításában játszottak fontos szerepet.

Az ifjúsági fórum ülésein és a fiatalokkal folytatott beszélgetések alkalmával szó esett az afrikai régiókat sújtó problémáktól kezdve, az egyes távol-keleti országok virágzásáig bezárólag számtalan dologról, élethelyzetről. Egyes országok fiatal küldöttei olyan körülményekről, fejlettségi szintről számoltak be, melyek a világ nagy része számára még álomképek csupán. Mások, az ellenkező pólust megtestesítő, küzdelmekkel és szenvedésekkel teli életről, infrastruktúra- és tudáshiányról tájékoztattak. Ezek egymást kiegészítve, ellensúlyozva segítettek nekünk fiataloknak egy reális kép, nézőpont kialakításában.

Könnyen átérezhettük a kommunikáció, nyitottság, globális szemléletmód, információ befogadására vonatkozó igény / hajlandóság, kompromisszum, tolerancia, segítőkészség szükségességét egy olyan koncentrált, világot magába sűrítő környezetben, mint amit ez a 189 országból érkezett közel négyszáz fiatal teremtett meg. Célunk megmutatni másoknak is ezek fontosságát, hogy mindenki számára világossá válhasson, nem problémákkal szembesülünk nap mint nap, hanem lehetőségekkel. A kettő közötti transzformáció kulcsa pedig nem más, mint a kommunikáció.

Könyvet ajánlunk

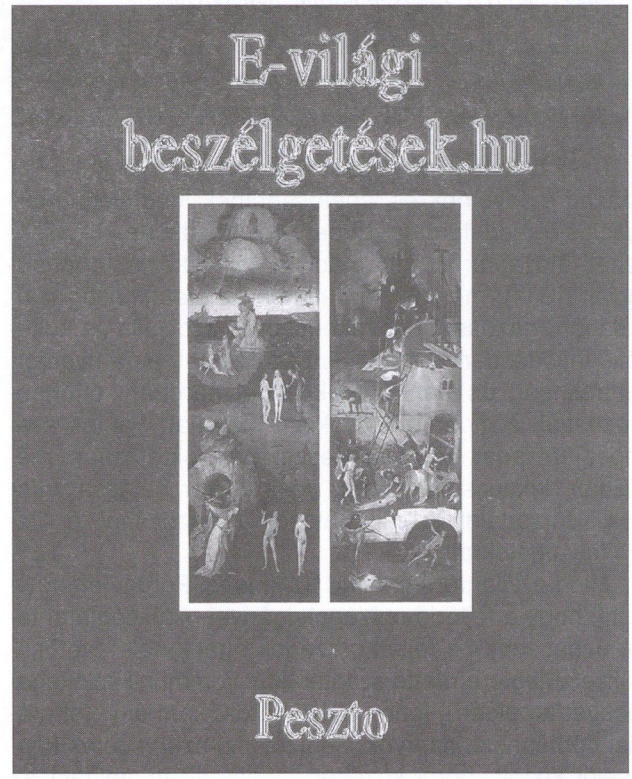
E-világi beszélgetések.hu

Október végén jelent meg a Hovanyecz László által „lejegyzett", a hazai informatika történetét különböző szemszögekből bemutató 254 oldalas könyv, melyet Talyigás Judit szerkesztett. A könyvben tíz magyar tanár, tudós, informatikus mutatkozik be beszélgetés formájában, miközben az olvasóban kialakul a kép arról, hogy mit tettek az informatikáért, majd végül egy kerekasztal-beszélgetés jegyzőkönyve összegzi a problémákat, teendőket. A könyv azonban több, mint egy tudományág megszületésének hű kronológiája.

A beszélgető partnerek (Székely Iván, Talyigás Judit, Mozjes Imre, Megyery Károly, Pap László, Gordos Géza, Havass Miklós, Bakonyi Péter, Dömölki Bálint és Farkas János – a sorrend a legfiatalabbtól tart kor szerinti sorrendet) nem csak a szűk szakmáról beszélnek. Megismerjük fiatalságukat, környezetüket, egyébirányú érdeklődésüket. Megtudhatjuk a könyvből, ki mire büszke és a vájt fülű olvasó azt is megtudja, mi az amiről nem szívesen beszélnek. A kép amit a szerkesztő és a beszélgetések feljegyzője kialakít az olvasóban az lényegesen több, mint egy életrajz, vagy egy pályázathoz melléklendő szöveg.

Olvasva a könyvet kialakul az a kép, ami segíti az olvasót, hogy a szereplőkkel ügyesen tudjon kapcsolatot teremteni. Erről eszembe jut Dale Carnegie (1888-1955) könyve „A karrier iskola". A 30-as évek végén az ilyen jellegű könyv újdonságnak számított. Számos hasznos tanácsa között egyik, amit érdemes volt megjegyezni, hogy mielőtt elmegyünk lényeges szakmai, üzleti tárgyalásra, ismerjük meg partnerünket. Rendkívül jó hatást tesz, ha tájékozottak vagyunk hobbijáról, családjáról, szakmai eredményeiről és ambicióiról. Azonnal könnyebben kezdődhet egy beszélgetés, ha tudjuk, hogy szereti a zenét, vagy maga is zenél. Vagy sportol és nemzetközi eredményeket is elért, esetleg színjátszóként, vagy újságíróként ért el sikereket. Ezeket szóba hozva bizonyosak lehetünk abban, hogy a társalgás könnyebben indul meg, feloldjuk a kezdeti feszélyezettséget és ezután nézeteinket, kívánságainkat szívesebben hallgatja meg.

Ha ezen túlmenően fel tudjuk mérni kapcsolatait, ars poétikáját és stílusát, akkor már egészen biztosak lehetünk a sikerben. Tíz emberről mindezt megtudhatjuk a könyvből. Bizonyára nem ez volt a szerzők, szerkesztők célja, de ez mint melléktermék önállóan is érdekessé teszi a könyvet. Bár mind a tizen tisztelik, becsülik egymást és a Tahi Baráti Kör be nem jegyzett és hivatalosan nem ismert egyesület tagjai, még sem lehet érezni semmilyen irányba elfogultságot. Inkább azt tudjuk kiolvasni az interjúkból, hogy a kör tagjainak tudása, képességei egymást jól kiegészítik. Mindez közre játszott abban, hogy az informatikáról,



az információs társadalomról sikerült a közvéleményben egy vonzó képet kialakítani.

Mindezek ellenére Magyarországon a telekereskedelem, távgyógyászat, távoktatás, elektronikus pénzforgalom és elektronikus közigazgatás nem fejlődik olyan gyorsan, mint számos más hasonló gazdasági helyzetben lévő országban. Ezt a szereplők is látják és a kerekasztal beszélgetésben különböző szempontok alapján igyekeznek az akadályozó tényezőket feltárni és a fejlesztés gyorsítását előirányozni. Többen hangsúlyozzák, hogy az Internetes csalások és a felhasználók etikátlan viselkedése miatt sokan nem merik ezen lehetőségeket kihasználni. Sajnos nincs a könyvben vastag betűkkel kiemelve, hogy többet kellene tennünk a legfiatalabbakban is az etikus viselkedés érdekében. Mivel valamennyien társadalmilag elismert szakemberek és többségük olyan pozícióban van, ahol sokat tehet a problémák elhárítása érdekében, reméljük, hogy ez az összegező könyv gyorsítani fogja a régóta várt folyamatokat.

Mindenkinek gratulálunk, aki a könyvben a 20-22 oldalas beszélgetések során sok konstruktív gondolattal járul az olvasó világképének bővítéséhez, de elsősorban Talyigás Juditnak, aki a Tahi Baráti Kör megszervezésével, és a könyv szerkesztésével értékesen és hasznosan járult hozzá az előttünk álló feladatok rendszerezéséhez.

Xyscom™

EISLER PÉTER

hungarocom@hungarocom.hu

Kulcsszavak: PLC, vidéki hálózat, internetelérés

*A Ξ rendszer (**K**istérségi **Sz**élessávú **I**ntegrált távközlési rendszer) kistérségek, kistelepülések részére korszerű, szélessávú távközlési szolgáltatásokat biztosító hálózati infrastruktúra. Biztosítja a lakossági és intézményi hozzáférést, a KözHáló kialakítását, ezzel egy adott kistérség távközlési elzártságának megszüntetését. Funkcióját tekintve az előfizetőkhöz legközelebbi hozzáférési hálózatot, valamint a hálózatok összekapcsolását biztosító kapcsoló egységet tartalmazza. Szolgáltatások tekintetében alkalmas önálló távbeszélő hálózat létrehozására is, így a szélessávú internet alapú szolgáltatások mellett országos keskenysávú távbeszélő, valamint egyéb hozzáadott értékű szolgáltatások (pl. mérőóra leolvasás, vagyonvédelem) megvalósítására.*

Kistérségi szélessávú integrált távközlési rendszer

A Xyscom™ mint információs infrastruktúra alapját képezheti az intelligens régióknak, ezzel jelentős mértékben hozzájárulhat az információs társadalom kialakításához. A kistérségek távközlési infrastruktúrájának a távközlési és a szélessávú átvitelt biztosító informatikai hálózatokkal való összekapcsolása biztosítja a régiók jobb elérhetőségét és a lakosság legszélesebb köreinek hozzáférését a korszerű infokommunikációs szolgáltatásokhoz.

A rendszeren bevezethető szolgáltatások a vidéki lakosság életvitelének, a helyi gazdasági tevékenység feltételeinek a javítását, a helyi ügyekben való tájékozottságának növelését, összességében a település és kistérség megtartó erejének a növelését. A rendszer szolgáltatásai lehetővé teszik az e-közigazgatás elterjesztését, azaz a központi és a helyi közigazgatás tevékenységeinek, költségeinek és dokumentumainak nyilvánossá tételét, a biztonságos elektronikus ügyintézés lehetőségének széleskörű megteremtését, a kormányzati tevékenységgel összefüggő nyilvánosság megvalósítását, továbbá a régiók és országok összekapcsolhatóságát, az információk globális cseréjét.

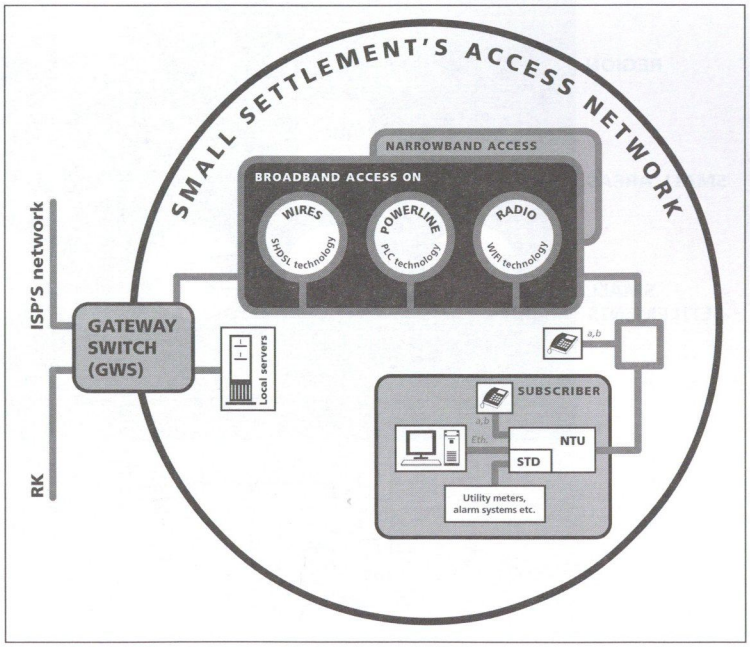
A Xyscom™ új, alternatív távközlési technológia, új infrastruktúra megteremtését kínálja, lehetőséget nyújtva egyben új szolgáltatói szervezetek, szolgáltatói üzleti konstrukciók kialakításához. Magába foglalja a kistelepülési hálózatot, az internet szolgáltatók IP alapú hálózatához és a közcélú távbeszélő hálózathoz (PSTN) hozzáférést biztosító GWS átjáró kapcsoló egységet, valamint a kistelepülések távbeszélő forgalmát összekapcsoló, a társszolgáltatók hálózatával való együttműködést biztosító RK kistérségi és regionális kapcsoló egységet.

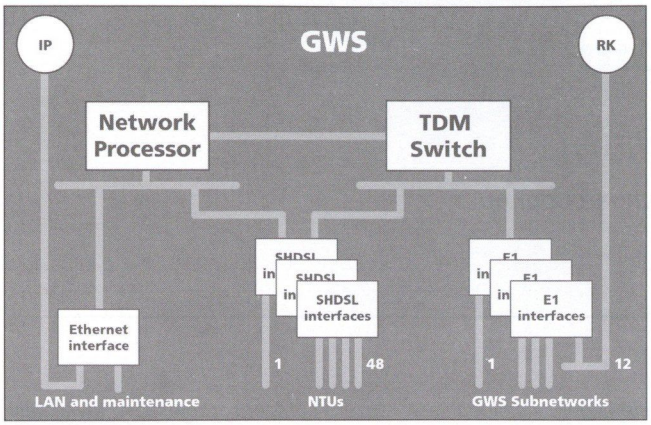
A kistelepülési hálózat a hozzáférési hálózatból, valamint az előfizetőknél elhelyezett egységekből (NTU) áll. A hozzáférési hálózat hagyományos keskenysávú kapcsolódást biztosít normál telefon előfizetők részére (POTS), valamint szélessávú kapcsolódást nyújt az arra előfizetők körének. A szélessávú kapcsolódás biztosítja az IP alapú adatátviteli és beszéd szolgáltatásokat.

A szélessávú hozzáférésre a rendszer három technológiát használ:

- vezetékes hálózaton a G.shdsl-t (ETSI: SDSL),
- erősáramú hálózaton a PLC-t,
- rádión a Wi-Fi (WLAN) technológiát.

Ezek a technológiák egy adott kistelepülési hálózatban egyidejűleg is használhatók, alkalmazásukat a kistelepülés szerkezete, az előfizetők eloszlása, a meglévő infrastruktúrák használhatósága, azaz mindenkor a leggazdaságosabb megoldás kiválasztásának lehetősége határozza meg.





Szélessávú szolgáltatást igénylő előfizetők esetén az NTU egység alkalmazkodik a hozzáférési technológiához, azaz elvégzi az előfizetőnél lévő informatikai és egyéb eszközök illesztését a hozzáférési hálózaton használt átviteli technológiához. A számítástechnikai eszközök hagyományos 10BaseT Ethernet felületen kapcsolódnak, az egyéb eszközök az STD jelű terminál illesztő egységen keresztül. Az előfizetőnél csak keskenysávú szolgáltatások igénybevétele esetén normál telefonkészülék csatlakoztatható. Az STD egységhez kapcsolódhatnak például a közüzemi mérőórák a fogyasztás távleolvasása céljából, valamint előfizetői riasztó központok. Ezen a felületen kapcsolódhatnak az „intelligens otthon" egyéb eszközei is. PLC és Wi-Fi technológiák esetén a beszédátvitel VoIP-vel történik, G.shdsl technológia esetén hagyományos időréses eljárással.

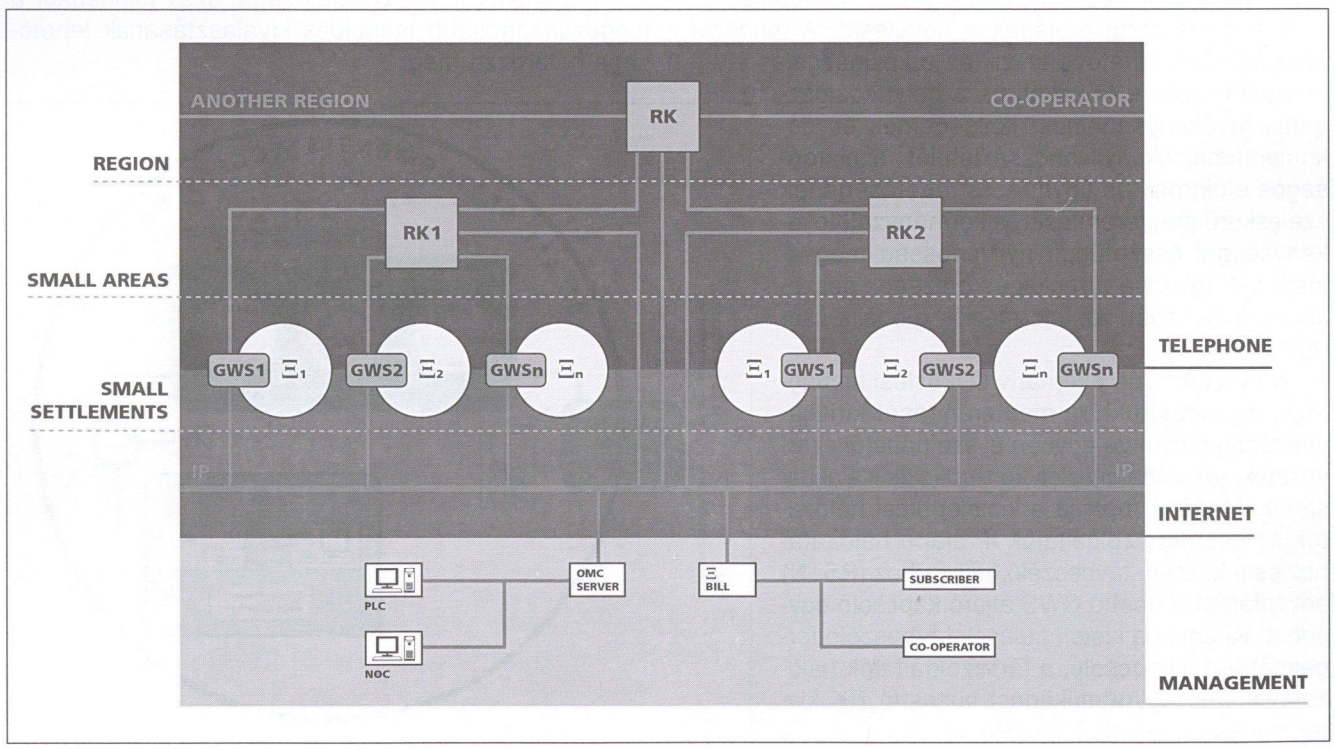
A kistelepülési hálózat részét képezi a GWS átjáró kapcsoló egység, amelynek feladata a hálózat előfizetőinek illesztése a szolgáltatók IP alapú, és PSTN alapú hálózatához. Ez az egység biztosítja a kistelepülés belső forgalmának lebonyolítását, a VoIP és időréses kommunikáció konverzióját, továbbá ehhez kapcsolódhatnak a kistelepülési helyi szolgáltatók informatikai szerverei.

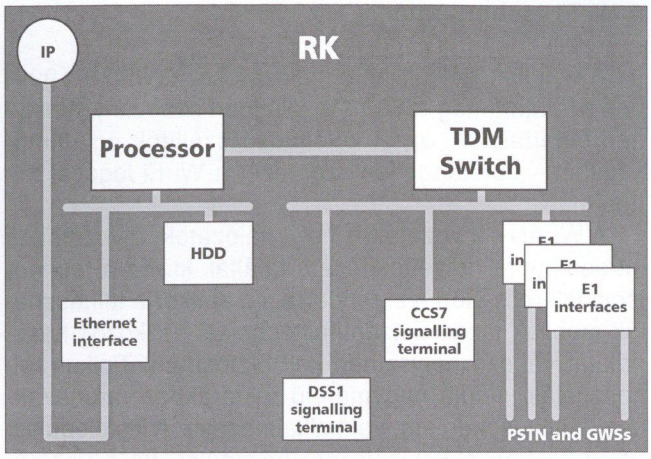
A Xyscom™-ból kialakítható teljes hálózati struktúra három szintből áll. Az első két szint a felettes hálózati struktúra, azaz a szolgáltatásoknak megfelelően az IP alapú internet hálózat, valamint a keskenysávú időrés alapú távbeszélő hálózat (PSTN). A harmadik szint a teljes hálózat üzemeltetését szolgáló OMC üzemviteli központból, valamint a hálózatba bekapcsolt előfizetők, illetve a társszolgáltatók egymás közötti díjelszámolását végző informatikai rendszerekből áll.

A távbeszélő szolgáltatás tekintetében a kistérségi-regionális hálózati csomópontban elhelyezett kapcsoló eszköz (RK) biztosítja a távbeszélő társszolgáltatók hálózatához való csatlakoztatást. A kistérségek egymás közti forgalmát az RK egység bonyolítja, a kistelepülések saját előfizetői közötti forgalmat a GWS.

Az RK-hoz kapcsolódó összeköttetések biztosítják saját régión belüli alrendszerek összekapcsolását. A saját hálózaton kívülre irányuló forgalmakat a társszolgáltatók hálózatán kell lebonyolítani, a mindenkor érvényes szabályok szerint. Az önkormányzatok és közintézmények egymás közötti forgalmát át lehet terelni az új hálózatra. A megyei, vagy regionális önkormányzatok alközpontjának – ha van, önkormányzati hálózatának – összekötetéseit is csatlakoztathatjuk az RK-hoz.

A rendszerből így felépíthető igény esetén a közintézmények távközlő hálózata, illetőleg ha ezt a hálózatot más rendszerből építik ki, a kistérségi rendszerek, így a kistérségi közigazgatás előfizetői az RK-n keresztül csatlakoztathatók tetszőleges országos különcélú hálózathoz.





Az internet-szolgáltató csomagkapcsolt hálózata biztosítja az IP alapú összeköttetéseket. Rendelkezésre bocsáthatja célszerűen a kistérségeket, illetve más hálózati csomópontokat összekapcsoló PSTN gerinchálózati összeköttetéseket is.

A rendszer szolgáltatásai az alábbiak:

- Hozzáférés az országos és nemzetközi szélessávú hálózatokhoz.
- Hozzáférés az országos és nemzetközi közcélú távbeszélő és mobil hálózatokhoz .
- Szélessávú hozzáférés helyi szerverekhez: közösségi információ (közigazgatás, reklám stb.) olvasása, helyi hirdetés feladása.
- Helyi távbeszélő szolgáltatás a kistérségen, kistelepülésen belül.
- Egészségügyi szolgáltatások, segélykérés.
- Vagyonvédelmi információk átvitele.
- „Intelligens otthon".
- Közüzemi mérőórák csatlakoztathatósága távleolvasás céljából.
- PBX előfizetők csatlakoztatása.

A rendszer lehetővé teszi a hírközlési szolgáltatók részére a Hírközlési Törvényből és más vonatkozó Kormányrendeletekből levezethető valamennyi kötelező érvényű szolgáltatás biztosítását:

- Az egyetemes hírközlési szolgáltatás keretein belül:
  - fax és adatátvitel biztosítása (csak keskenysávú szolgáltatásnál, szélessávúnál ez természetes),
  - nyilvános távbeszélő állomás felkapcsolási lehetősége,
  - ingyenes segélyhívás lehetőségének biztosítása.
- Időmérésen alapuló szolgáltatási díj.
- Alapkiépítésű monitoring alrendszer.
- Számhordozhatóság biztosítása átadó és átvevő szolgáltatóként egyaránt.
- Szolgáltató választás biztosítása előválasztással és hívásonkénti előválasztással.
- Az országos tudakozó szolgálat elérésének biztosítása.
- Az ügyfélszolgálat és a hibabejelentő elérésének díjmentes biztosítása.
- Előfizetői hívószám megváltoztatása esetén az új hívószámról meghatározott szövegkészletből tájékoztatás adása.
- Előfizetői szolgáltatások korlátozási lehetősége.
- A hívó előfizető azonosító kijelzésének biztosítása.

Az alkalmazott hozzáférési technológiák

A G.shdsl technológia

Egyetlen előfizetői sodrott érpáron nagysebességű szimmetrikus digitális előfizetői vonal létesítésére a G. shdsl ITU-T szabvány (G.991.2.), SDSL néven ETSI szabvány (TS 101524) határozott meg technikát. A G.shdsl technika azért jelentős, mert előirányozza a megbízható nagysebességű és szimmetrikus átviteli lehetőséget az üzleti alkalmazások céljára. A G.shdsl több hagyományos DSL technológia konvergenciáját jelenti egyetlen nemzetközileg elfogadott ipari szabványban és az alábbi kiemelkedő tulajdonságokkal rendelkezik:

- Sebesség/távolság adaptivitás, amely jóval a sodrott érpár tradicionális határain túl is előfizetői hozzáférést biztosít. Egyetlen 0.4 mm átmérőjű sodrott érpáron 1.8 km-6 km működési tartomány (2.3 Mb/s-192 kb/s) érhető el.
- A G.shdsl tisztán digitális implementáció, lehetővé teszi E1 frakcionális szolgáltatások kialakítását, valamint üzleti alkalmazásokhoz több hangcsatorna átvitelét .
- Spektrális kompatibilitás ugyanabban a kábelben egyidejűleg működő más szolgáltatásokkal.
- Együttműködési képesség más rendszerekkel többszállítós környezetben, költséghatékony, versenyképes hálózati megoldások alkalmazhatósága érdekében.
- Robosztusság, amely zajos környezetben is lehetővé teszi alkalmazását előre megjósolható teljesítmény mellett.

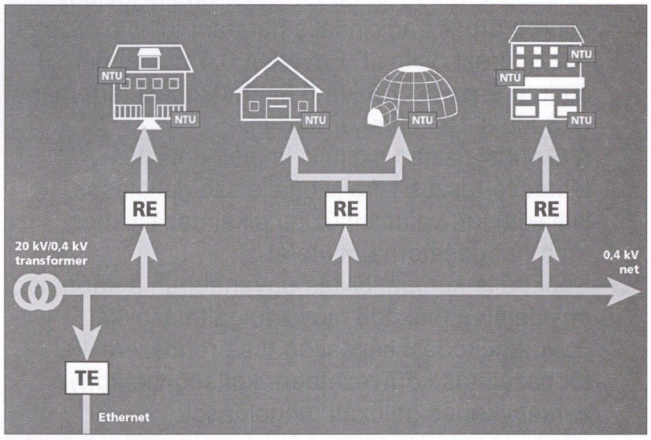
A PLC technológia

A PLC technológia a kisfeszültségű (0,4 kV) erősáramú hálózat felhasználása távközlési célokra. Az erősáramú hálózat talán a legkiterjedtebb hálózat, amely szinte mindenhol elérhető. Mivel ezt a hálózatot 50 Hz frekvencián történő teljesítmény átvitelre optimalizálták, ezért a nagyfrekvencián történő adatátvitel jelentős kihívásokat jelent. Az erősáramú hálózat különféle vezeték típusokat és keresztmetszeteket használ tetszőlegesen összekötve egymással, így sokféle karakterisztikus impedancia előfordul a hálózatban. A hálózat kimenő impedanciája változik a távközlésre alkalmazott frekvencia szerint, valamint időben is, a fogyasztók terhelésétől függően. Ez az impedancia illesztetlenség mély letöréseket jelent bizonyos frekvenciáknál. A nagy csillapítás mellett az erősáramú hálózat az elektromosan legzavartatottabb közeg, amely a távközlési célú

igénybevételt jelentősen megnehezíti. A legfőbb zajforrások az elektromos fogyasztók amelyek olyan zajkomponenseket generálnak amelyek spektruma a nagyfrekvenciás tartományba esik.

A fenti problémák leküzdésére az erősáramú hálózaton történő kommunikáció céljára hatékony hibajavító és modulációs eljárásokat kell alkalmazni. A PLC hozzáférés az OFDM *(Orthogonal Frequency Division Multiplexing)* eljárást használja amelynek alapelve, hogy az átvinni kívánt nagysebességű jelet részekre bontva egyidejűleg, párhuzamosan visszük át speciálisan kiszámított ortogonális vivő frekvenciákon, azokat különkülön modulálva. Az eljárás lehetővé teszi a bitek dinamikus hozzárendelését az egyes rész-csatornákhoz. Az átvitt információ maximalizálása érdekében a kisebb zajú rész-csatornákhoz több bitet oszt ki.

A távközlési célra használt nagy sávszélességű digitális eszközök az 1-30 MHz közötti frekvenciasávot használják. Az ezen sávot használó eszközöknek meg kell felelni a kisugárzott teljesítményre vonatkozó előírásoknak, ugyanis az erősáramú hálózat ebben a frekvencia tartományban antennaként működik.



Egy részhálózat végpontja a 20kV/400V transzformátor, mivel az alkalmazott nagyfrekvenciás jelet nem viszi át. Az előfizetőnél kerül elhelyezésre az NTU egység, amely tartalmazza az erősáramú hálózaton való átvitelhez szükséges egységeket. A távolságok és a mindenkori zavartatási viszonyoknak megfelelően RE jelű jelismétlőket kell a hálózatban elhelyezni, az erősen csillapított és zavart jelek regenerálása céljából. A TE egység az alhálózat vezérlő része, amely az egységek közötti kommunikáció vezérlésére és menedzselésére szolgál. Ez azt jelenti, hogy alhálózatonként valamennyi NTU egységre elosztva a maximális adatsebesség 45 Mb/s lehet.

Több alhálózat (egy transzformátor állomás alá tartozó előfizetők) összekapcsolható egymással a GWS egységen keresztül a TE egység Ethernet interfészének felhasználásával. A transzformátor állomásokon elhelyezett TE és a GWS egység között összeköttetés szükséges, amely megvalósítható pont-pont rádió, optikai összeköttetés (4 Mb/s-nél nagyobb adatsebesség igény esetén), vagy fizikai érpáron a korábban ismertetett G.shdsl segítségével.

A Wi-Fi technológia

A vezeték nélküli helyi hálózatokra (WLAN) 1999-ben született meg a 802.11b jelű ipari szabvány, amelynek betartását – ezzel különböző szállítók együttműködését – egy független szervezet a Wi-Fi logóval minősít.

A WLAN-t a vezetékes helyi hálózatok, a vezetékes infrastruktúra helyettesítésére találták ki. Ez a technológia jelentős előnnyel rendelkezik, amikor a felhasználók mobilak, azaz a számítástechnikai eszközök használatát változó helyszínen kell biztosítani. Tipikus felhasználási módja nagyméretű raktárakban, áruházakban, kiállításokon stb. való alkalmazása. A kistelepülési hálózatokban akkor célszerű használni, ha a vezetékes technológiák alkalmazásánál olcsóbb megoldást ad, ugyanis a felhasználók mobilitása nem igény. Bizonyos esetekben gazdaságosan használható pont-pont közötti bérelt vonali jellegű összeköttetések létesítésére.

Az eredeti szabvány 2.4 GHz frekvencián maximum 11 Mb/s adatátviteli sebességet irányozott elő. A jelenleg bevezetés alatt lévő szabványok az 5 GHz-es tartományt és az 54 Mb/s sebességet irányozzák elő magasabb biztonsági és szolgáltatás minőségi követelményekkel.

Rádiófrekvenciás szempontból a rendszer direkt sorrendű szórt spektrumú (DSSS) átviteli technikát használ, MAC protokolként többszörös elérésű, ütközésmentes (CSMA/CA) technikát. Megjegyezzük, hogy a bevezetendő új WLAN szabványok modulációs eljárásként a PLC technológiánál bemutatott OFDM-et használják.

A 2.4 GHZ frekvencia alkalmazásánál problémát jelent, hogy a globálisan kijelölt ipari, tudományos és orvosi célra használt frekvenciasávba esik, az 5 GHz-es rendszerek pedig az úgynevezett nem engedélyhez kötött nemzeti infrastrukturális sávba.

Tekintettel arra, hogy ezek a frekvenciák nem az engedélyhez kötött tartományba esnek sokfajta vezeték nélküli eszköz pl. mikrohullámú sütők, biztonságtechnikai eszközök, zsinórnélküli telefonok is működhetnek ebben a sávban. A rendszer telepítése tehát nem frekvencia-engedély köteles, viszont adott helyen garantálva sincs zavarmentes felhasználása. Wi-Fi technológiát a kistérségi hálózatban csak nagyon gondos előzetes mérések alapján valóban indokolt esetben, nagy körültekintéssel célszerű alkalmazni és mindezt csakis akkor, ha az gazdaságosság szempontjából egyáltalán indokolt.

Tarifálás, díjelszámolás

A rendszer biztosítja a korrekt díjelszámolás alapjául szolgáló hívásadatok rögzítését. Ezeket a primer hívásrekordokat az RK egységből egy hívásadat gyűjtő rendszer kérdezi le. A hívásrekord tartalmazza az adatforgalomra jellemző értékeket is. A hívásadat-gyűjtő

rendszer csatlakoztatható a telefonszámlák elkészítését végző informatikai rendszerhez. A rendszer biztosítja, hogy az internet szolgáltató, valamint társszolgáltatók (pl. MATÁV) felé irányuló hívások esetén a rendszerhez csatlakoztatott előfizetők közötti elszámolás pontosan, visszakövethető módon történjen. Ilyenkor a társszolgáltatók által benyújtott számlát kell a hívások arányában elosztani a rendszerre kapcsolt kistérségi előfizetők között.

A rendszer nagyobb hálózatok kialakításánál lehetővé teszi rugalmas saját tarifapolitika kialakítását.

Üzemvitel és hálózat menedzselés

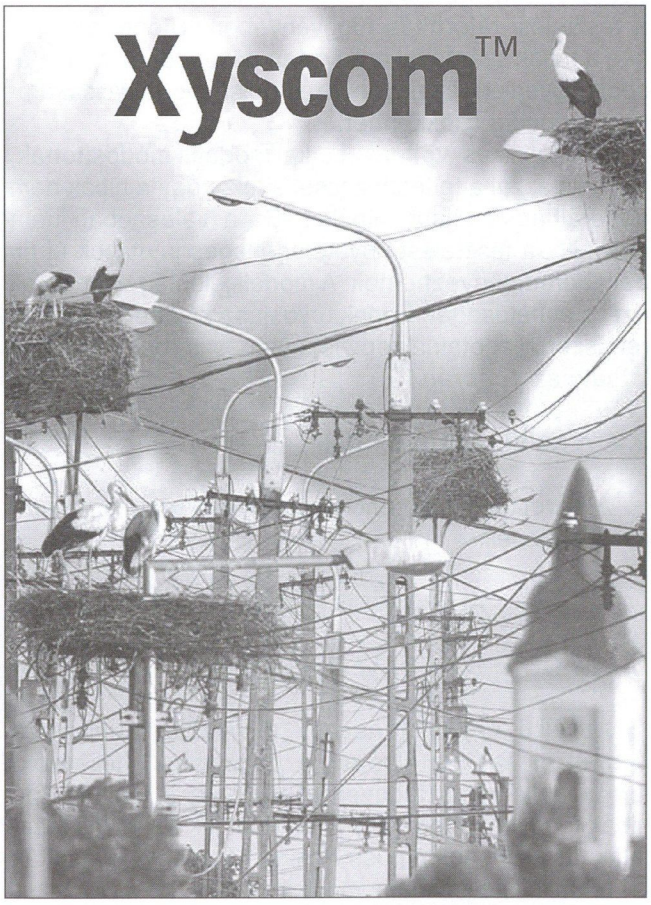
A centralizált üzemfelügyeleti és hálózat menedzselő rendszer szolgál a kistérségi hálózatok üzemeltetésére.

Az üzemeltetésen az alábbi funkciókat értjük:

- konfiguráció-menedzselés,
- riasztások vétele, archiválása,
- hibabehatárolás,
- előfizetői adatbázis kezelés, szolgáltatás-menedzselés,
- a rendszer teljesítményének ellenőrzése,
- forgalommérés.

Az üzemeltetés az IP hálózaton történik, valamennyi eszköz SNMP menedzselt.

A cél távolról, az előfizetői egységekig kiterjedően a fenti funkciók elvégzése.



Hírek

Egy felmérés során 16 európai ország – köztük Magyarország – huszonöt, korábban monopolhelyzetben lévő, illetve új alternatív szolgáltatójának üzleti stratéiáját vizsgálták. A tanulmány szerint a válaszadó szolgáltatók számára az árbevétel növelése (55%) és a költségek csökkentése (32%) a legfontosabb szempont. Kétharmaduk (67%) szerint a hagyományos hangátvitel részesedése 2006-ra árbevételük 50%-a alá esik, és a jövőbeni növekedés kulcsának az új szolgáltatások kifejlesztését tekintik (45%). A válaszadók már jelenleg is biztosítanak IP-telefóniás szolgáltatást, vagy a következő három év során tervezik annak bevezetését (83%); amely rávilágít arra, hogy felismerték a végfelhasználók növekvő igényét a konvergens szolgáltatások iránt. A felmérés arra is rámutat, hogy a távközlési piacon komoly erőeltolódás tapasztalható, és egyre hangsúlyosabb szerepet kapnak az ügyfelek igényei. A szolgáltatók egyre inkább az ügyfelek igényeiből indulnak ki, és megalapozott üzleti tervek alapján indítják be új szolgáltatásaikat.

A **Cisco Systems** bemutatta a 100 főnél kisebb vállalkozások, kis- és fiókirodák számára fejlesztett, a Cisco IOS® szoftverre épülő, hívásfeldolgozási szolgáltatásokat biztosító Cisco CallManager Expresst, valamint hangposta- és automatikus kezelői szolgáltatásokat nyújtó megoldását, a Cisco Unity Expresst. A Cisco mindkét megoldást routerekbe integrálta, így egyszerű, könnyen telepíthető IP-kommunikációs megoldást biztosít a száznál kevesebb alkalmazottal rendelkező vállalatok számára. A termékek a díjnyertes Cisco IP telefonok felhasználásával egészítik ki a Cisco meglévő IP-kommunikációs rendszerportfolióját.

A **Sun** szolgáltatásait és technológiáit választotta a Shell a HomeGenie nevű új, integrált lakásfelügyeleti megoldáshoz. Ez Java technológiákra épülő egyszerű, webes távoli hozzáférést biztosít háztartási rendszerekhez és eszközökhöz, szélessávú internet-kapcsolatra és egy kiegészítő készülékre (OSGI alapú lakossági átjáró) van szükség azok távoli – számítógépes vagy mobiltelefonos – működtetéséhez. Így gyakorlatilag bármikor és bármilyen webes számítógépről vagy mobiltelefonról kezelhetik azokat. A lakástulajdonosok szabályozhatják és beprogramozhatják például az otthoni hőmérsékletet, a lámpákat és bizonyos berendezéseket, valamint figyelhetik a lakás bizonyos területeit, illetve képeket rögzíthetnek a mozgásérzékelőt is tartalmazó Wireless Camera használatával.

Meddig teszteljünk?

STIKKEL GÁBOR, *stiko@compalg.inf.elte.hu,*

SZEDERKÉNYI GÁBOR, *szeder@sztaki.hu*

Reviewed

Kulcsszavak: szoftver-megbízhatóság, hibakeresés

Tesztelési és ráfordítási költségek időbeli változását dinamikus rendszerekkel modellezve próbálunk megoldást találni szoftverprojektek jellegzetes problémájának megoldására: meddig teszteljünk, hogy jó minőségű rendszer kerüljön piacra. A megoldást analízis előzi meg, melynek keretében vizsgáljuk a rendszerek stabilitását és paramétereinek becsülhetőségét. Rendszerelméleti eszközökön alapuló módszerünk alkalmazhatóságát valós adatokon teszteljük.

1. Bevezetés

A szoftverprojektek erőforrásainak jelentős részét fenntartási és tesztelési költségekre fordítják. Ez a tény motiválja a fenntartási és tesztelési költségek tervezésének, becslésének és nyomon követésének kutatását.

A költségek modellezésére Calzolari és társai [2] mutattak be egy ígéretes megközelítést a közelmúltban. Modelljük a szoftverhibákat olyan áldozatoknak tekinti amelyek környezeti beavatkozást és módosító akciókat indukálnak. A tesztelők és fejlesztők pedig a ragadozók, akik felfedezik és eltávolítják az áldozatokat. A hibák számának tesztelés alatti vagy forgalomba hozás utáni dinamikus változása hasonló a ragadozó-áldozat versengéshez. Az egyetlen különbség Calzolariék szerint az, hogy a hibák nem reprodukálnak hibákat.

Hasonló modelleket találhatunk az irodalomban. Lehman és társai [6] dinamikus modellek segítségével írták le a releváns szoftvermetrikák fejlődését vizsgálva a szoftverrendszerek méretének időbeli változását.

Az itt bemutatandó megközelítéshez nagyon hasonlót találunk Abdel-Hamid [1] és Madachy [8] munkáiban. A szerzők átfogó modelljét alkotják a teljes szoftverfejlesztési folyamatnak. Szimulációs eredményeik elősegítik az előrejelzést és döntéshozást, ugyanakkor eme modellek előállítása és paramétereinek becslése nehéz feladat. Kivétel ez alól a ragadozó-áldozat modellek paraméterbecslése, mely automatizálható.

2. A tesztelési folyamat modellezése differenciálegyenletekkel

A klasszikus ragadozó-áldozat modellben, melyet V. Volterra és A. J. Lotka javasolt, két differenciálegyenletből álló rendszer modellezi a populációk változását. Calzolari és társai ezt a modellt alkalmazták [2] a fenntartási és tesztelési tevékenységekre: a javításokat a szoftverhibák zsákmányul ejtésének tekinthetjük. A következőkben a modell lineáris majd nemlineáris változatát mutatjuk be.

2.1. A lineáris modell

A lineáris modellt a következő differenciálegyenletek írják le [2]:

$$\dot{x}_1 = \quad -ax_2 \tag{1}$$

$$\dot{x}_2 = bx_1 - cx_2. \tag{2}$$

Az első változó a szoftverben maradó hibákat, míg a második tesztelési, fenntartási költséget jelöl. Az *a, b* és *c* paraméterek pozitívak. Az első egyenletből kiolvasható, hogyan csökken a fennmaradó hibák száma a tesztelési ráfordítás függvényében. Utóbbi mennyiség a hibák számával arányosan növekedhet (lásd második egyenlet), az úgynevezett belső mortalitással arányosan pedig csökkenhet.

A klasszikus Volterra-Lotka modellt módosították, ugyanis azzal a feltételezéssel éltek, hogy a hibák nem generálhatnak újabb hibákat. Ez a valóságban nem helytálló: a tesztelést követő esetleges javítások új hibákat eredményezhetnek. A modell jelenleg nem kezeli ezt az eshetőséget. Ennek orvoslása jövőbeli célunk. A rendszer állapotainak egy lehetséges időbeli változása látható az *1. ábrán.*

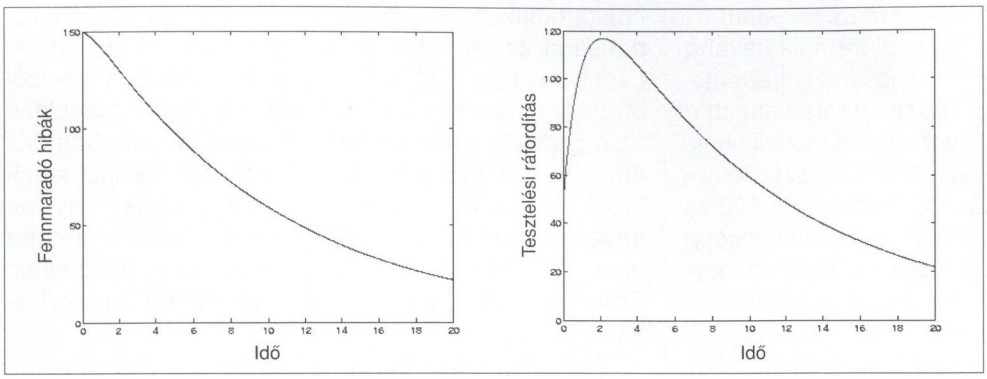
2.2. A nemlineáris modell

A következő differenciálegyenletek írják le a nemlineáris modellt:

$$\dot{x}_1 = -h(x_1)x_2 \tag{3}$$

$$\dot{x}_2 = eh(x_1)x_2 - mx_2. \tag{4}$$

Az első egyenlet negatív tényezője tartalmazza $h(x_1)$-et és x_2-t. Az első tag a „ragadozók" (tesztelők) funkcionális válaszfüggvényét mutatja: a fennmaradó hibák függvényében hány hibát találnak az egyes tesztelők. Itt a második típusú Holling függvényt javasolták [2] a funkcionális válasz modellezésére:



1. ábra A lineáris modell változóinak időbeli alakulása a=0.1, b=1 és c=1.1 paraméterértékek mellett

$$h(x_1) = \frac{ax_1}{b + x_1}.$$

Az *a* paraméter az aszimptotikus hibajavítási ráta, míg *b* az a hibaszint, mely mellett a hibajavítás rátája feleződik. A második egyenlet két részre bontható. Az aktuális hibajavítás ráta az *e* hatékonysági tényező segítségével ráfordítássá konvertálódik. Az egyenlet második fele a ráfordítás csökkenését mutatja az úgynevezett mortalitási tényezővel. A változók lehetséges trajektóriái az *2. ábrán* láthatók.

3. A lineáris modell állapotainak megfigyelése

3.1. A megfigyelőelmélet elemei

A lineáris időinvariáns rendszerek elmélete a következő diferenciálegyenlet rendszer vizsgálatával foglalkozik:

$$\dot{x} = Ax + Bu \tag{5}$$

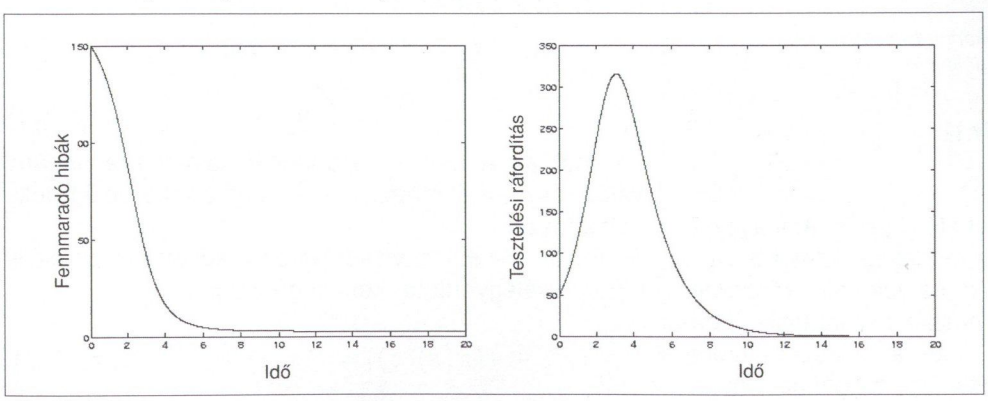
$$y = Cx \tag{6}$$

ahol *x* a rendszer állapota, *u* a be-, míg *y* a kimenete.

Az olasz szerzők által javasolt modell mátrixai a következők:

$$A = \begin{bmatrix} 0 & -a \\ b & -c \end{bmatrix}, \qquad B = 0, \qquad C = [0 \;\; 1].$$

2. ábra A nemlineáris modell egy lehetséges trajektóriája a=0.5, b=130, e=6 és m=0.7 paraméterértékekkel



Rendszerelméleti szempontból érdekes kérdés, hogy vajon a rendszer állapota előállítható-e a bemenet és a kimenet segítségével. A válasz igenlő, ha a rendszer *megfigyelhető,* azaz azonosan nulla kimenet, csak nulla kezdeti érték mellett kapható. Lineáris rendszer megfigyelhetősége ekvivalens azzal, hogy a

$$\begin{bmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{bmatrix}$$

mátrix nulltere csupán a nullvektorból álljon.

A megfigyelés állapotmegfigyelővel [7] hajtható végre, ami egy dinamikai rendszer a következő alakban:

$$\dot{\hat{x}} = A\hat{x} + Gu + Hy. \tag{7}$$

Az (7) rendszert állapotmegfigyelő a (5) rendszerre nézve, ha bármely x_0, $\hat{x}_0$ kezdeti állapotok és bármely *u* input esetén

$$\lim_{t\to\infty} \hat{x}(t) - x(t) = 0.$$

3.2. Megfigyelő-tervezés

A *G* és *H* mátrixok kiszámítására vonatkozólag [7] ad útmutatást. Belátható, hogy esetünkben *G* = *H* = 0, azaz

$$\dot{\hat{x}} = A\hat{x}$$

a (5) rendszer állapotmegfigyelője.

A megfigyelő hatékonysága az $\hat{x}(0)$ kezdeti értéktől függ. Ha a projektmenedzser eltalálja az $x_1(0)$ pontos értékét, akkor $x_2(0)$ ismeretében a megfigyelő kezdeti állapota $\hat{x}(0) = [x_1(0)\; x_2(0)]^T$, a becslési hibája $(\hat{x} - x)$ pedig azonosan nulla lesz. Így a menedzser a fennmaradó hibák számát pontosan tudja követni. A gyakorlatban azonban lehetetlen pontos becslést adni az első változó kezdeti értékére. Eme probléma kezelésére két módszer kerül bemutatásra.

3.3. Hogyan becsüljük a megfigyelő kezdeti állapotát?

3.3.1. Szakértői vélemény

Ahelyett, hogy a pontos kezdeti érték becslésének nehéz feladatára vállalkoznánk, lehetőségünk van a tesztelésből nyert adatokat felhasználni. Adott időpon-

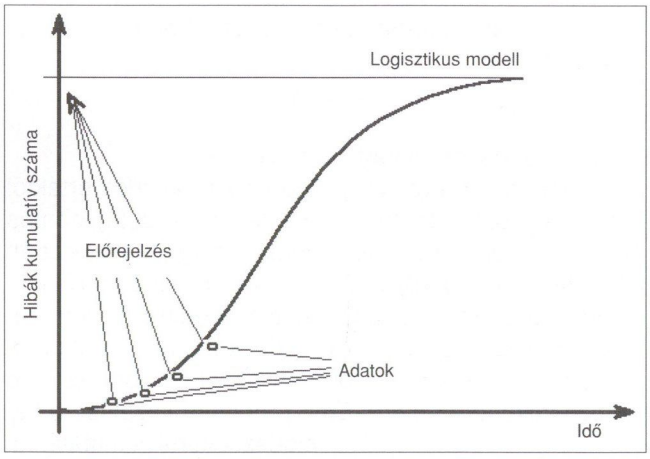
tig talált hibák száma alsó becslésként szolgálhat x_1 kezdeti értékére nézve és a projekt előre haladtával a menedzser egyre pontosabb alsó becsléseket adhat.

Tegyük fel, hogy eredetileg 150 hibát tartalmazott a rendszer. Ezt a kezdeti értéket használva a modell becslése alapján 21 körül lesz a hibák száma a tesztelés huszadik napján. A projektmenedzser kezdetben 100-ra becsüli a hibák számát. A szimuláció eredményeképp adódik, hogy 14 körül lesz a hibák száma a huszadik napon. Ugyanakkor a tizedik nap után már 68 hibánál tartanak a tesztelők, ami a menedzsert becslésének változtatására kényszeríti. Ezek után úgy gondolja, hogy körülbelül 170 hiba lehetett eredetileg a rendszerben. Ezzel a kezdeti értékkel 24 hibát jelzünk előre a huszadik napra, ami már közelebb áll a valósághoz mint az első próbálkozás.

3.3.2. Szoftver-megbízhatósági modell alapú becslés

A másik módszer a Satoh [11], [12] által bemutatott szoftver-megbízhatósági modelleken alapszik (bármely más megbízhatósági modell alkalmazható, Satoh eredményei a legújabbak). Ezek a modellek a tesztelés során talált hibák kumulatív számát ábrázolják az idő függvényében, majd logisztikus és Gompertz-féle differenciálegyenletekkel közelítik a valós adatokat. A cél: néhány kezdeti adat (általában az összadat ötöde) beérkeztével becsüljük meg a tesztelés végére talált hibák várható számát.

Paraméterbecsléssel tehetjük ezt meg, majd az állapot-megfigyelő kezdeti értékének a becslése következik. A módszert a *3. ábra* illusztrálja. A fennmaradó hibák előrejelzésére további módszerek található [3]-ban.



3. ábra A megfigyelő kezdeti értékének becslése a logisztikus görbével modellezve

4. A nemlineáris modell stabilitási analízise

Rövid stabilitásvizsgálat olvasható [2]-ban. Ami a lineáris modellt illeti: ha valamennyi modellparaméter pozitív, akkor a rendszermátrix sajátértékeinek valós része negatív, amiből következik a rendszer aszimptotikus stabilitása. Ez utóbbi azt jelenti, hogy a rendszer állapotváltozói időben a kezdeti értékektől függetlenül nullához tartanak. Az egyensúlyi pont további kvalitatív tulajdonsága az *attraktivitás*. Az egyensúlyi pontot attraktívnak nevezzük, ha létezik olyan környezete, amelyből bármely pontot kezdeti értékként választva a megoldás az egyensúlyi ponthoz tart. Könnyen látható, hogy az attraktív egyensúlyi pontoknak izoláltaknak kell lenniük. A nemlineáris modell egyensúlyi pontjait egy félegyenes alkotja, így [2] megállapításával ellentétben ezek az egyensúlyi pontok nem lehetnek attraktívak. Érdemes tehát a stabilitást részletesebben is megvizsgálnunk.

A feltételezések szerint a nemlineáris modell mindkét állapotváltozója nemnegatív értékeket vehet fel. Látható, hogy $ea - m \leq 0$ esetén a második állapotváltozó csökken, ami némileg ellentmond a valós életben megfigyelhető folyamatnak (a tesztelési tevékenységre fordított erőforrások ilyenkor egy darabig növekednek). Ezért a további vizsgálatokat a $ea - m > 0$ feltételezéssel végezzük.

A (3) egyensúlyi pontjait a $\dot{x}_1^* = 0$ és $\dot{x}_2^* = 0$ egyenletek megoldásával határozhatjuk meg. A megoldás $(x_1^*, 0)$, ahol x_1^* nemnegatív. Az egyensúlyi pontok tehát egy félegyenest alkotnak, ami miatt csak lokális stabilitási vizsgálatnak van értelme. A további vizsgálatokhoz a rendszer állapotváltozóit a következőképpen centráljuk:

$$\dot{x}_1 = -\frac{a(x_1 + x_1^*)x_2}{b + x_1 + x_1^*} \tag{8}$$

$$\dot{x}_2 = \frac{ea(x_1 + x_1^*)x_2}{b + x_1 + x_1^*} - mx_2. \tag{9}$$

A stabilitásvizsgálathoz szükség van még a rendszer Jacobi mátrixára:

$$F = \begin{bmatrix} 0 & -h(x_1^*) \\ 0 & -m + h(x_1^*). \end{bmatrix}$$

A Jacobi mátrix sajátértékei 0 és $-m + h(x_1^*)$.

A második sajátérték negativitásának feltétele tehát $x_1^* < mb/(ea - m)$, azaz a $(x_1^*, 0)$ egyensúlyi pont $x_1^* \geq mb/(ea - m)$ esetén instabil.

Ha a rendszer Jacobi mátrixa negatív valós részű és nulla sajátértékekkel rendelkezik, akkor a stabilitás vizsgálatához hatékony segédeszköz lehet a központi sokaságok elmélete (Center Manifold Theory).

A [4] könyvben található állítás alkalmazásához a rendszert a következő alakban kell felírni:

$$\dot{y} = Ay + Pz + g(y, z) \tag{10}$$

$$\dot{z} = Bz + f(y, z), \tag{11}$$

Ahol az A mátrix valamennyi sajátértéke negatív valós részű, a B mátrix összes sajátértéke pedig nulla valós részű.

Ekkor a stabilitásvizsgálathoz a következő parciális differenciálegyenletet kell megoldanunk:

$$\frac{\partial \pi}{\partial z}(Bz + f(\pi(z), z)) = A\pi(z) + Pz + g(\pi(z), z).$$

Tétel 1 *A következő egyenlet nulla egyensúlyi pontjának (aszimptotikus) stabilitásából a központi sokaságokra vonatkozó tétel alapján következik a (10) rendszer (y, z) = (0, 0) pontjának (aszimptotikus) stabilitása.*

$A = -m + eh(x_1^*)$, $P = 0$, $g(y,z) = \frac{ea(z+x_1^*)y}{b+x_1^*+z} - eh(x_1^*)y$, $B = 0$, $g(f,z) = -\frac{a(z+x_1^*)y}{b+x_1^*+z}$

közönséges, egyetlen megoldása pedig a triviális megoldás, azaz $\pi(z) \equiv 0$.

Ennek alapján a redukált egyenlet az alábbi egyszerű alakú lesz:

$$\dot{\zeta} = 0$$

Ebből pedig látható, hogy a $0 \le x_1^* < mb/(ea - m)$ feltételt kielégítő valamennyi egyensúlyi pont stabil.

5. Paraméterbecslés

5.1. A lineáris modell paramétereinek becslése

Tekintsük ismét a tesztelési erőforrások és a szoftverhibák dinamikus változását leíró lineáris modelljét! A modell három konstans paraméterrel rendelkezik, így a paraméterbecslési feladat ebben az esetben *a, b* és *c* meghatározása a második állapotváltozóra vonatkozó mérési adatokból.

Tételezzük fel, hogy x_2 állapotváltozó értékeit a mérésekből diszkrét időpillanatokban ismerjük. Jelöljük a mérési sorozatot a következőképp: $\hat{x}_2(0)$, $\hat{x}_2(1)$,...., $\hat{x}_2(N)$. A paraméterek értékeit szeretnénk úgy meghatározni, hogy a következő négyzetes becslési hiba minimális legyen:

$$\sum_{i=0}^{N} (x_2(i) - \hat{x}_2(i))^2$$

A modell dinamikus szimulációját Matlab környezetben valósítottuk meg, a paraméterbecsléshez pedig a szimplex-módszert felhasználó beépített numerikus algoritmust használtunk. A jó minőségű becsléshez olyan adatsorra van szükségünk, amelynél látható a tesztelési erőforrás görbe csúcsa.

5.2. A nemlineáris modell paramétereinek becslése algebrai eliminációval

A nemlineáris rendszerek viselkedése gyakran nem írható le a modellezési célnak (pl. irányítás) megfelelő pontossággal.

Így van ez esetünkben is, ezért ebben a szakaszban a (3)-(4) egyenletek által leírt nemlineáris modell paramétereinek becslésével foglalkozunk.

5.2.1. Nemlineáris bemenet-kimenet modell kiszámítása

Feltételezésünk szerint a (3)-(4) rendszerben az egyedüli mérhető állapotváltozó x_2. Ez alapján a bemenet-kimenet modellt a következő alakban írjuk fel:

$$F(y, \dot{y}, \ddot{y}, u, \dot{u}) = 0 \qquad (12)$$

ahol *y* jelöli a mérhető kimenetet (azaz $y = x_2$), *u* pedig egy ismertnek feltételezett fiktív bemenet. A további számítások szempontjából a legegyszerűbb, ha *u*-nak a (4) egyenletben szereplő *m*-et választjuk.

A cél ezek után az, hogy a nem mérhető állapotváltozót, azaz x_1-et eliminálju az állapotegyenletekből, és így olyan modellt kapjunk, amely alakjában megfelel (12)-nek. Ehhez írjuk át az állapotegyenleteket és a fiktív kimeneti egyenletet a következőképp:

$$\dot{x}_1 + \frac{ax_1x_2}{b + x_1} = 0 \qquad (13)$$

$$\dot{x}_2 - \frac{eax_1x_2}{b + x_1} + ux_2 = 0 \qquad (14)$$

$$y - x_2 = 0 \qquad (15)$$

(15)-ből és (9)-ből kapjuk, hogy

$$\dot{y} - \frac{eax_1x_2}{b + x_1} + ux_2 = 0,$$

amiből x_1 kifejezése a következőt adja:

$$x_1 = \frac{b(\dot{y} + ux_2)}{-\dot{y} - ux_2 + eax_2} =: \frac{n(t)}{d(t)} \qquad (16)$$

ahol *n* és *d* a (16) kifejezés számlálóját illetve nevezőjét jelöli. (16) idő szerinti differenciálásával kapjuk:

$$\dot{x}_1 = \frac{\dot{n}(t)}{d(t)} - \frac{n(t)\dot{d}(t)}{d^2(t)}. \qquad (17)$$

A (17) és (13) egyenletek, illetőleg a (16)-ben szereplő jelölés felhasználásával x_1-et eliminálni tudjuk az állapotegyenletekből, azaz

$$-\frac{a\frac{n(t)}{d(t)}x_2}{b + \frac{n(t)}{d(t)}} = \frac{\dot{n}(t)}{d(t)} - \frac{n(t)\dot{d}(t)}{d^2(t)}, \qquad (18)$$

melyet a következő alakba tudunk átírni:

$$-\frac{an(t)x_2}{d(t)b + n(t)} = \dot{n}(t) - \frac{n(t)\dot{d}(t)}{d(t)}. \qquad (19)$$

n és *d* idő szerinti deriváltjának kiszámításával kapjuk a kívánt bemenet-kimenet modellt, amely az alábbi alakba írható: (20)

$$-\frac{\dot{y} + uy}{ey} = b(\ddot{y} + u\dot{y}) - \frac{b(\dot{y} + uy)(-\ddot{y} - u\dot{y} - \dot{u}y + ea\dot{y})}{-\dot{y} - uy + eay}.$$

Kihasználva, hogy modellünk esetében az $u = m$ paraméter konstans, és így $\dot{u} = 0$, még egyszerűbb alakot kapunk:

$$-\frac{\dot{y} + uy}{ey} = \frac{bea(y\ddot{y} - \dot{y}^2)}{-\dot{y} - uy + eay}. \qquad (21)$$

Vezessük be a következő transzformált paramétereket:

$$c_1 = be^2a, \qquad c_2 = ea \qquad (22)$$

Ezek felhasználásával a modell az alábbi alakú lesz:

$$(\dot{y} + uy)^2 = c_1(y\ddot{y} - \dot{y}^2) + c_2y(\dot{y} + uy), \qquad (23)$$

amely *paraméterekben lineáris*. Így c_1 és c_2 bármely hagyományos módszerrel megbecsülhető az x_2-re vonatkozó mérési adatokból.

5.2.2. Paraméterbecslés

A paraméterbecslés gyakorlati kivitelezéséhez hasznos, ha a (23) folytonos idejű modellt átírjuk diszkrét idejűvé. Ehhez először vezesük be a δ operátort az Euler-közelítéssel kapott numerikus deriváltak jelölésére

$$\delta z(k) = \frac{z(k+1) - z(k)}{t_s}, \tag{24}$$

ahol z tetszőleges diszkrét idejű jelsorozat, t_s pedig a mintavételi idő.

A δ operátor felhasználásával az (23) modell diszkrét idejű alakja az alábbi lesz: (25)

$$(\delta y(k) + uy(k))^2 = c_1(y(k) \cdot \delta^2 y(k) - (\delta y(k))^2) + c_2 y(k)(\delta y(k) + uy(k))$$

amely a szokásos regressziós alakban van

$$w(k) = \phi^T(k)\theta \tag{26}$$

ahol

$$w(k) = (\delta y(k) + uy(k))^2 \tag{27}$$

$$\phi^T(k) = [y(k) \cdot \delta^2 y(k) - (\delta y(k))^2 \quad y(k)(\delta y(k) + uy(k))] \tag{28}$$

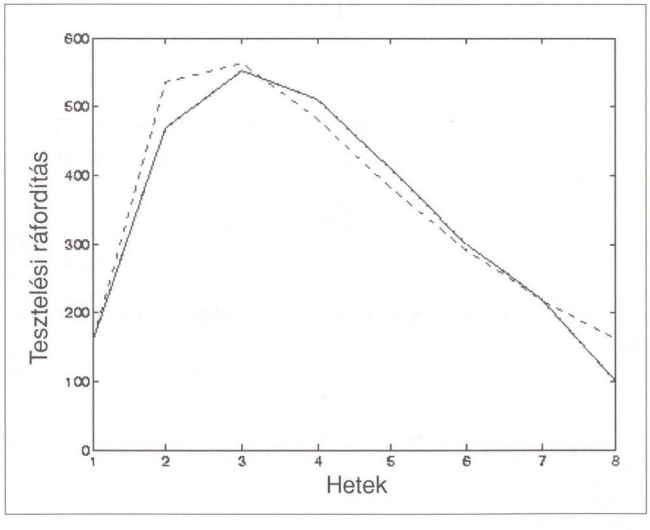
$$\theta = [c_1 \quad c_2]^T. \tag{29}$$

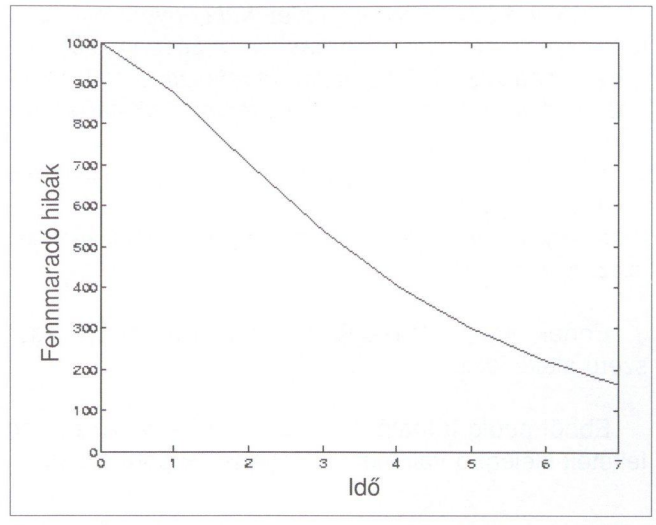
Így c_1 és c_2 például a jól ismert legkisebb négyzetes módszerrel becsülhető a következő kvadratikus kritériumfüggvény θ-ra nézve történő minimalizálásával:

$$V(n,\theta) = \frac{1}{N}\sum_{i=1}^{N}(w(i) - \phi^T(i)\theta)^2 \tag{30}$$

Megjegyezzük, hogy a fentiekhez azt kell feltételeznünk, hogy az *a, b* és *e* modellparaméterek közül legalább egyet ismerünk, és ezután tudjuk megoldani (22)-t a fennmaradó ismeretlen paraméterekre. Ez rontja paraméter-becslés alkalmazhatóságát, de a javasolt módszerrel az előzőleg (például lineáris modellel) megbecsült paraméterek tovább finomíthatók.

4. ábra Ráfordítási adatok (folytonos) és a modell a becsült paraméterekkel (szaggatott; a=0.31, b=0.9 és c=1:22)





5. ábra Szimulációs eredmények: fennmaradó hibák száma x_1

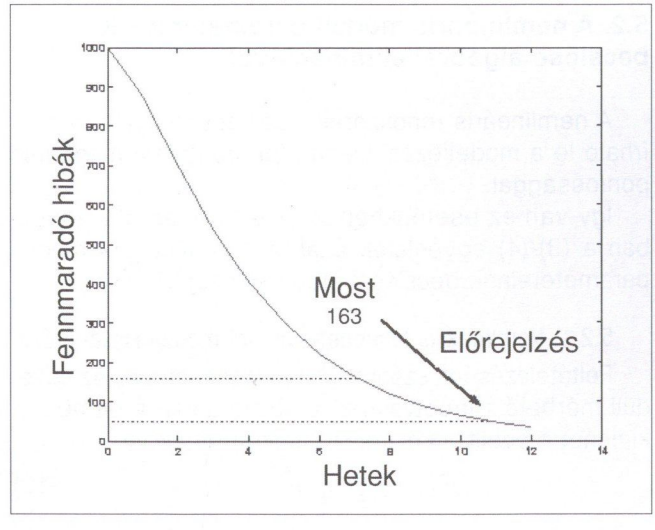
6. Alkalmazás

Az általunk vizsgált projekt keretében egy nyílt, szabványokon alapuló, moduláris és elosztott rendszert fejlesztettek. A C++ forráskód hossza meghaladta a 250 ezret, előállításához 75 ezer emberórára volt szükség. A projekt 13 hónapig tartott és részletes ráfordítás adatok álltak rendelkezésre, melyekből a modellparamétereket becsülni lehetett *(4. ábra)*.

A megfigyelő hatékonysága ellenőrizhető volt: a fennmaradó hibák számának egyeznie kellett a becsült kezdeti érték ($x_1(0)$) és a tesztelés során talált hibák számának összegével.

A tesztelés során 848 hibát találtak. Az első javasolt módszert követve 1000-re becsültük a fennmaradó hibák kezdeti értékét. Így a modellt akkor fogadjuk el, ha 152 körülire becsüli a teszt után fennmaradó áldozatok számát. A szimulációs eredményeket az *5. ábra* mutatja, melyről leolvasható, hogy a modell szerint 163 hiba maradt a rendszerben. A hiba mértéke kevesebb, mint tíz százalék.

6. ábra Az első változóra vonatkozó szimulációs eredmények



Tegyük fel, hogy a menedzser addig szeretné folytatni a tesztelést, amíg a fennmaradó hibák száma 50 alá nem csökken. Meddig kell még tesztelni? A szimulációt még tovább futtatva a *6. ábra* kapható. A modell szerint a tesztelésnek még négy további héten át folytatódnia kell, ahhoz hogy a termék a kívánt minőséget elérje.

7. Összegzés

Tesztelési és fenntartási ráfordítások Lotka-Volterra alapú modeljét vizsgáltuk rendszerelméleti szempontból. A lineáris változatra tervezett állapotmegfigyelő alkalmasnak bizonyult a szoftverrendszerben fennmaradó hibák számának előrejelzésére. Emellett hasznos segédeszköz a projektmenedzser kezében, aki segítségével a tesztelés befejezésének időpontját határozhatja meg a kívánt minőség elérésének érdekében.

Mindemellett a modell használható még a tesztelési ráfordítás és a szoftverminőség közötti kompromisszumot érintő „mi lenne ha..."-típusú kérdések megválaszolásában. A jövőben a modellel kapcsolatos korlátozásokat (például hibák nem generálhatnak új hibákat) próbálunk feloldani.

Köszönetnyilvánítás

A szerzők ezúton mondanak köszönetet Asztalos Domonkosnak (Ericsson Magyarország) és Bártfai Gusztávnak (volt Ericsson Magyarország) a vizsgálódás tárgyát képező projekt adataival kapcsolatos kérdésekben nyújtott segítségükért.

Irodalom

[1] T. K. Abdel-Hamid:
The dynamics of software project staffing: a system dynamics based simulation approach. IEEE Transactions on Software Engineering, 15(2). 1989. 109–119.

[2] F. Calzolari, P. Tonella, G. Antoniol:
Maintenance and testing effort modeled by linear and nonlinear dynamic systems. Information and Software Technology, 43(2001). 477–486.

[3] M. Grottke, K. Dussa-Zieger:
Prediction of Software Failures Based on Systematic Testing. Electronic Proc. 9th European Conference on Software Testing Analysis and Review (EuroSTAR), Stockholm, 2001.

[4] A. Isidori:
Nonlinear Control Systems. SpringerVerlag, 1995.

[5] M. M. Lehman, D. E. Perry, J. F. Ramil:
Implication of evolution metrics on software maintenance. Proceedings of the International Conference on Software Maintenance, Bethesda, MD, 1998, pp. 208–217.

[6] M. M. Lehman, D. E. Perry, J. F. Ramil:
On evidence supporting the feat hypothesis and the laws of of software evoution. Proceedings of the Fifth International Symposium on Software metrics, Bethesda, MD, 1998.

[7] J. M. Maciejowski:
Multivariable Feedback Design. Addison-Wesley, 1989. Wokingham, U.K.

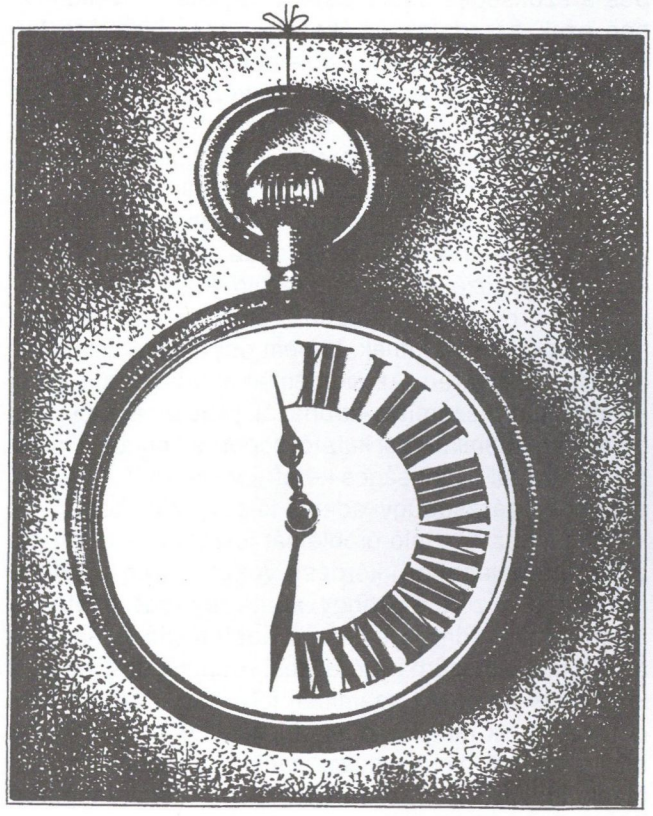
[8] R. Madachy:
System dynamics modelling of an inspection-based process, Proceedings of the International Conference on Software Engineering, Berlin, 1996. pp. 376–386.

[9] Y.K. Malaiya, J. Denton:
Requirements volatility and defect density, Proceedings of International Symposium on Software Reliability Engineering, Boca Raton, Florida, USA, 1999.

[10] J. D. Musa, A. Iannino and K. Okumoto:
Software Reliability: Measurement, Prediction, Application, McGrawHill, 1990.

[11] D. Satoh:
A Discrete Gompertz Equation and a Software Reliability Growth Model. IEICE Transactions on Information and Systems E83(2000) No. 7. 1508–1513.

[12] D. Satoh, S. Yamada:
Parameter Estimation of Discrete Logistic Curve Models for Software Reliability Assessment Japan Journal of Industrial and Applied Mathematics 19(2002) No. 1. 39–53.



Rejtjelező homomorfizmusok

LIMBEK RÉKA, SZIKLAI PÉTER *

ELTE TTK Információs Rendszerek Tanszék, Operációkutatás Tanszék

E-mail: lreka@elte.hu, sziklai@cs.elte.hu

Reviewed

Kulcsszavak: adatbiztonság, számítás-átruházás, adat-átruházás, kódolás

A rejtjelező homomorfizmusok arra valók, hogy megbízhassunk egy céget olyan számítások elvégzésével, melyeknek mind kiinduló adatai, mind a végeredménye bizalmasak, és emiatt csak titkosított (kódolt) formában kommunikálhatóak. Ehhez olyan speciális rejtjelezést kell alkalmazni, hogy az elvégzendő műveletek végrehajthatóak legyenek a kódolt adatokon, és az eredményt visszakapva, majd dekódolva azt a végeredményt kapjuk, mintha a titkosítatlan adatokkal számoltunk volna. Ebbe a témakörbe vezet be a cikk, bemutatva az alapvető módszereket és vázolva az esetleges támadási (törési) problémákat is.

Bevezetés

A rejtjelező homomorfizmusok fogalmát Rivest, Adleman és Dertouzos [6] vezette be 1978-ban, eredetileg a *számítás-átruházás* (computing delegation) problémájának a megoldására. Ez tipikusan olyankor áll fenn, amikor az adatok birtokosa csak korlátozott számítási kapacitással rendelkezik, azaz vagy túl bonyolultak számára az elvégzendő számítások, vagy akkora mennyiségű adattal kell dolgoznia, amelyet már nem tud kezelni. Ilyenkor kénytelen az adatait például egy számítóközpontnak kiszolgáltatni (adatkezelő), amely képes a szükséges számítások elvégzésére. Amennyiben ezek az adatok érzékenyek, azaz bizalmas természetűek, nyilvánvaló problémát jelent az, hogy az adatok kikerülnek egy olyan környezetbe, amely nem feltétlenül megbízható. Ez a helyzet nagyon sok internetes alkalmazás kapcsán előadódik, tipikusan amikor valamilyen távoli szolgáltatást veszünk igénybe. Ide tartozhat már egy egyszerű valutaátváltást számító vagy útvonal-tervező szoftver is, de az igazán klasszikus példák közé a portfolió-kezelő és jövedelemadó-számító programok tartoznak, amelyek nem a saját számítógépünkön futnak, hanem egy mások által üzemeltetett szerveren. Az akadémiai kutatás területén is előfordulhat a számítás-átruházás problémája, például ha egy egyetemi orvosi kutatócsoport az oktatási intézmény nem túl biztonságos keretrendszerét használja a bizalmas egészségügyi adatok feldolgozásához.

A fentihez hasonló problémát jelent az *adatátruházás* (data delegation) kérdése. A különbség a kétféle átruházás között az, hogy adatátruházás esetén a számítások eredménye nem az adattulajdonos, hanem az adatkezelő számára érdekes. A tulajdonos részéről közömbös az egész számítási folyamat, gyakran nem is rendelkezik megfelelő lehetőségekkel a számítások elvégzéséhez, ő csak „kölcsönadja" az adatait a számítások idejére. Az adatkezelő pedig nem magát a nyers adatot akarja birtokolni, hanem a feldolgozott adatot (például statisztikai elemzések eredményét). Érzékeny adatok esetén azonban ismét problémát jelent, hogy a „kölcsön" idejére ezek kikerülnek egy nem feltétlenül megbízható környezetbe.

Adatátruházásra jellemzően a szövetkezeti felépítésű szervezeteknél kerül sor. Az állami közigazgatás is általában ilyen struktúrájú, de hasonlóan jó példa erre a szerkezetre az Európai Unió vagy az Egyesült Államok is. A tagállamok mindegyike rendelkezik a saját adataival (állami költségvetés, lakossági nyilvántartás, stb), amit egy központi szervezet például elemzés céljára szeretne felhasználni. Az adatszolgáltatásért cserébe a tagállamok igényelhetik, hogy ők is elemezhessék az összegyűjtött adatokat. Gyakran azonban adatvédelmi szempontok miatt nincs lehetőségük más tagállamok adatait tárolni, továbbá megfelelő számítási kapacitásuk sincs a kívánt számítások elvégzésére. A központi szervnek viszont, amelynek ezek közül egyik sem jelent problémát, nincs fölösleges kapacitása arra, hogy minden egyes tagállam számára elvégezze a kért számításokat. Hogyan, milyen formában lehet az összegyűjtött adatokat átadni a tagállamoknak, hogy mindezen problémákat áthidaljuk?

Az adatátruházás biztonságos megoldása az intelligens kártyák (smartcard) felhasználásának a lehetőségeit is bővítené. Így ugyanis nem jelentene problémát, ha a kártyán tárolt adatokon egy erőforrás-igényes alkalmazásnak kellene futnia. A kártya egyszerűen exportálná a számításokhoz szükséges adatokat az alkalmazást futtató egységnek.

Mindkét átruházási esetben kétféle adatbiztonsági kérdés merül fel. Egyrészt meg kell akadályozni az illetéktelen hozzáférést az adatok továbbítása közben, másrészt biztosítani kell, hogy a számítás-átruházás esetében a számításokat végző szoftver, komputer és annak személyzete, az adatátruházás esetében pedig a tagok ne jussanak (jogtalanul) értékes információhoz

* *Kutatásainkat az Egyetemközi Távközlési és Informatikai Központ (ETIK) támogatta*

a nyers adatokat illetően a rendelkezésre bocsátott adatok alapján. Az előbbi kérdés már az Internet elterjedése előtt is egy jól kutatott területnek számított, főleg a katonai és nemzetbiztonsági alkalmazások miatt. A világháló egyre szélesebb körű használata miatt kicsit másképp kellett megfogalmazni ugyanezt a kérdést, de a nyilvános kulcsú rejtjelezés bevezetésével és megfelelő implementálásával a továbbítandó adatok biztonsága lényegében megoldódott.

A cikk az itt felmerült második adatbiztonsági kérdést járja körül. Mindkét esetben léteznek hardver illetve adatbázis-kezelési megoldások is, mint például fizikailag védett processzor vagy adattöredékek használata [8]. A számunkra érdekes kriptográfiai megoldást azonban a *rejtjelező homomorfizmusok* alkalmazása jelenti, amelyek lehetővé teszik, hogy az adatokat rejtjelezett formában továbbítsuk a nem megbízható szintre (számítóközpont, tagállamok), és ott a megfelelő számításokat az adatok *dekódolása nélkül,* rejtjelezett formában végezzék el. Miután a számítások eredménye rejtjelezett formában visszakerül a megbízható szintre (korlátozott kapacitású felhasználó, központi szervezet), ott dekódolás után *ugyanazt az eredményt* kapjuk, mintha a számításokat az eredeti formában hajtottuk volna végre.

A különböző megoldások egymással kombinálhatók a nagyobb biztonság elérése érdekében, de ezekre a lehetőségekre itt nem térünk ki.

Terminológia

Azokat az adatokat, amelyek mindenki számára értelmezhető alakban tűnnek fel, a kriptográfia az adat típusától függetlenül *nyílt szövegnek* nevezi. A nyílt szöveg titkosítását *kódolásnak* vagy *rejtjelezésnek* hívjuk, és ennek eredménye a *rejtjelezett vagy rejtjeles szöveg.* Ha a rejtjeles szöveget a legitim felhasználó dekódolja, akkor a rejtjeles szöveg *visszaállításáról* beszélünk. Ennek eredménye az eredeti nyílt szöveg. Ha egy támadó kísérli meg a rejtjeles szöveg dekódolását, akkor a szöveg *feltöréséről* beszélünk. A dekódoló eljárás a kódoló eljárás egyfajta inverze.

A rejtjelezést egy *rejtjelező algoritmus* valósítja meg, amely rendelkezik egy paraméterrel, a *kulccsal.* Rendszerint a visszaállító algoritmus is ugyanezzel a kulcsparaméterrel rendelkezik. Ha a két kulcs azonos, akkor az eljárást *szimmetrikus vagy titkos kulcsú rejtjelezésnek* nevezzük. Ha a két kulcs különböző, akkor *aszimmetrikus vagy nyilvános kulcsú rejtjelezésről* beszélünk, ebben az esetben ugyanis általában a kulcsok egyike nyilvános, azaz mindenki számára hozzáférhető.

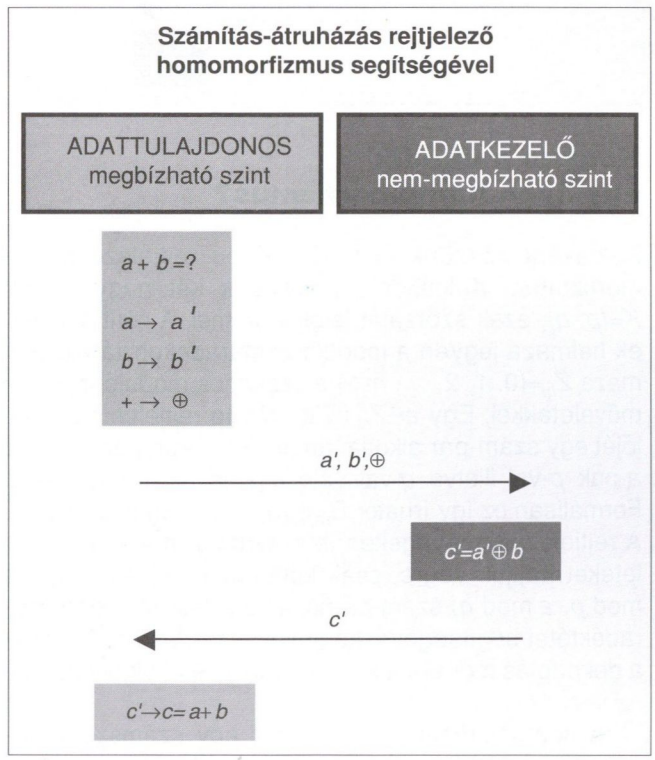
Amikor a támadó a kódot vagy a rejtjelező algoritmust akarja feltörni, akkor az elsődleges célja a lehallgatott rejtjeles szöveg feltörése, de lehetőség szerint a kódoláshoz használt titkos kulcs meghatározása is. Egy rejtjelező algoritmus biztonsága, azaz a támadásokkal szembeni ellenálló képessége sohasem múlhat azon, hogy maga az algoritmus közismert-e vagy sem, ezért mindig feltesszük, hogy a támadó ismeri a rejtjelezés menetét. A támadó számára a nyílt szöveg és a használt kulcs meghatározása a fontos.

Rejtjelező homomorfizmusok

A rejtjelező homomorfizmusok a rejtjelezett adatokon történő számítások elvégzéséhez használhatók. Tulajdonképpen ezek a homomorfizmusok úgy rejtjelezik az adatokat, hogy rejtjelezett állapotukban is ugyanúgy lehet rajtuk műveleteket végrehajtani, mint egyébként.

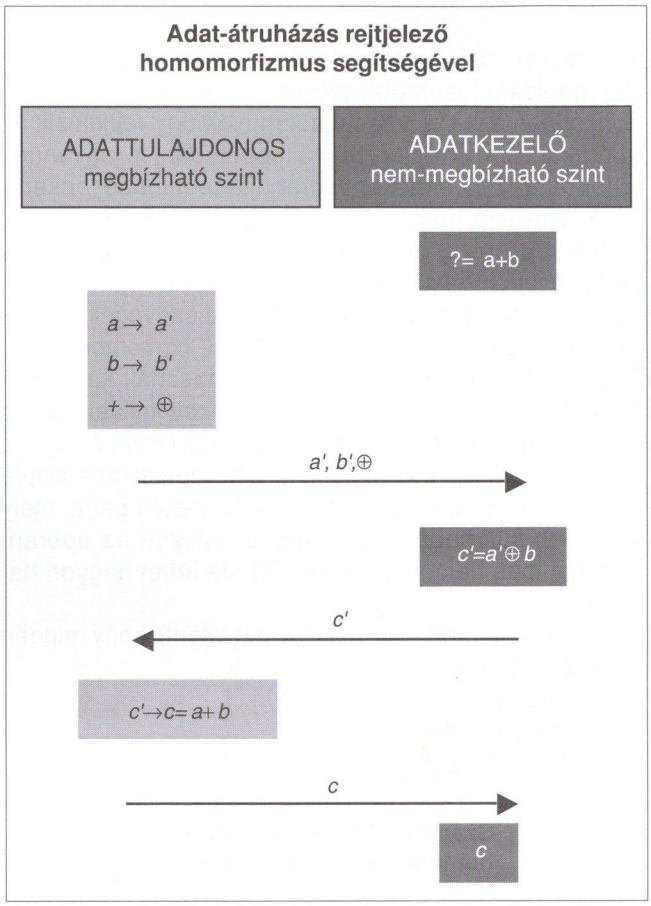
A rejtjelező homomorfizmus egy művelettartó rejtjelező leképezés a nyílt szövegek halmazáról a rejtjelezett szövegek halmazára. Formálisan, ha S a nyílt szövegek halmaza, S' pedig a rejtjelezett szövegek halmaza, akkor definiálható egy $E_K: S \rightarrow S'$ homomorfizmus, ahol K a függvény paramétereként használt kulcs. Legyenek az S-en, illetve S'-n értelmezett műveletek és predikátumok $f_1, f_2, \ldots, f_k$ és $p_1, p_2, \ldots, p_l$ illetve $f'_1, f'_2, \ldots, f'_k$ és $p'_1, p'_2, \ldots, p'_l$. Minden S-beli műveletnek illetve predikátumnak megfelel az S'-n értelmezett párja, mely általában különbözik az eredetitől (hiszen az operandusokat más halmazból vesszük), de lehet nagyon hasonló is.

E_K művelettartása formálisan azt jelenti, hogy minden $a, b, \ldots \in S$ és minden $i=1,\ldots,$ **k**
$E_K(f_i(a, b,\ldots)) = f'_i E_K(a), E_K(b),\ldots),$
továbbá minden $j=1,\ldots,$ **l**
$p_j(a, b,\ldots) = p'_j(E_K(a), E_K(b),\ldots).$



A rejtjeles szöveg visszaállítását (dekódolását) egy $D_{K'}: S'' \rightarrow S$ függvény hajtja végre, ahol S'' az E_K homomorfizmus értékkészlete és K' a kulcs. A D függvény E inverzének felel meg, így ez is egy művelettartó leképe-

zés. Ez a tulajdonság biztosítja, hogy a rejtjeles szövegen elvégzett számítások után a visszaállítás során a várt eredményt kapjuk, azaz minden $a, b, \ldots \in S$ és i, j esetén $f_i(a, b, \ldots) = D_{K'}(f'_j(E_K(a), E_K(b), \ldots))$ és $D_{K'} p_j(E_K(a), E_K(b), \ldots)) = p_j(a, b, \ldots)$



Hogyan működik egy ilyen homomorfizmus?

Példaként nézzünk egy RSA-alapú rejtjelező homomorfizmust. Kulcsként válasszunk két nagy prímet $K=(p, q)$, ezek szorzatát jelöljük m-mel. A nyílt szövegek halmaza legyen a modulo m maradékosztályok halmaza $Z_m=\{0, 1, 2, \ldots, m-1\}$ a szokásos modulo m +, -, x műveletekkel. Egy $a \in Z_m$ nyílt szöveg rejtjeles megfelelőjét egy szám-pár alkotja, amelynek a komponensei az a-nak p-vel illetve q-val való osztás utáni maradéka. Formálisan ez így írható: $E_{(p, q)}(a) = (a \bmod p, a \bmod q)$. A rejtjelezett szövegeken is a modulo m +, -, x műveleteket hajtjuk végre, csak komponensenként. Egy (a mod p, a mod q) szám-párból az eredeti a-t a kínai maradéktétel segítségével kapjuk vissza *[lásd fent]*, azaz a dekódolás menete a kínai maradéktétel alkalmazása.

A homomorfizmus működését egy számszerű példán keresztül mutatjuk be, és mivel célunk a szemléltetés, a gyakorlat számára reménytelenül kis paramétereket kellett választanunk. A titkos kulcs legyen (3, 11), m=33. Tegyük fel, hogy a kiszámítandó formula (12+4) x2 (modulo 33 műveletekkel), a három nyílt szöveg tehát 12, 4, 2, a várt eredmény pedig 32 mod 33. A nyílt szöveget rejtjelezve küldjük el a következő alakban: $E_{(3, 11)}(12)=(0, 1)$, $E_{(3, 11)}(4)=(1, 4)$, $E_{(3, 11)}(2)=(2, 2)$.

Természetesen azt is tudtára adjuk a számítást végző félnek, hogy az első két tag összegét szeretnénk a harmadik tényezővel megszorozni. Ennek megfelelően ők kiszámolják ((0, 1)+(1, 4))x(2, 2) értékét, ahol ezek a műveletek a komponensenként vett modulo 33 műveletek. A számítás így a következőképpen alakul: ((0, 1) +(1, 4))x(2, 2)=(0+1, 1+4)x(2, 2)=(1, 5)x(2, 2)=(2, 10). Visszakapjuk az eredményt rejtjelezett alakban: (2, 10), amelyet a kínai maradéktétel segítségével dekódolunk. Meg kell tehát oldanunk az $x \equiv 2 \pmod 3$, $x \equiv 10 \pmod{11}$ kongruencia rendszert. A megoldást $x=3y+11z$ alakban keressük. Mivel $3y$ osztható 3-mal, $11z \equiv 2 \pmod 3$ kongruenciának kell teljesülnie. Hasonló okokból $3y \equiv 10 \pmod{11}$. Ezekből pedig $z=1$ illetve $y=7$ adódik, vagyis $x=3x7+11=21+11=32 \pmod{33}$.

A rejtjelező homomorfizmus tehát azért válik nagyon hasznossá a számítás- és adat-átruházási problémák kapcsán, mert a nyílt szövegnek megfelelő rejtjelezett szövegen lehet elvégezni a „nyílt műveleteknek" megfelelő „rejtjelezett műveleteket", és az így kapott rejtjelezett eredményt visszaállítva a megfelelő „nyílt eredményt" kapjuk.

Kínai maradéktétel

Ha $m_1, m_2, \ldots, m_k$ páronként relatív prímek, akkor az

$$x \equiv a_1 \ (m_1)$$
$$x \equiv a_2 \ (m_2)$$
$$\ldots$$
$$x \equiv a_k \ (m_k)$$

kongruencia rendszer megoldható, és a megoldás egyértelmű mod $m_1 \times m_2 \times \ldots \times m_k$.

Példa:

$$x \equiv 1 \ (3)$$
$$x \equiv 3 \ (5)$$
$$x \equiv -1 \ (7)$$

A megoldást $x=35y_1+21y_2+15y_3$ alakban keressük. Ekkor a kongruencia rendszer ala pján

$$35y_1 \equiv 1 \ (3)$$
$$21y_2 \equiv 3 \ (5)$$
$$15y_3 \equiv -1 \ (7)$$

Ennek egy megoldása:
$y_1=-1$, $y_2=3$, $y_3=-1$, amelyből $x=13$ adódik.

Mitől jó egy rejtjelező homomorfizmus?

Egy rejtjelező homomorfizmusnak először is megfelelőnek kell lennie az adott alkalmazáshoz, azaz azokat a műveleteket kell megtartania, amelyekre szükség van az alkalmazás szempontjából. Ezen túl a rejtjelező homomorfizmussal szemben alapvetően *hatékonysági és biztonsági* elvárásaink lehetnek. Az előbbi kategóriába tartozik, hogy könnyű legyen magának a függvénynek a kiszámítása, és ugyanez érvényes legyen a visszaál-

lító leképezésre is. További hatékonysági követelmény, hogy a nyílt szöveg műveleteinek illetve predikátumainak megfelelő f'_i-k illetve p'_i-k számítása gyorsan menjen, és hogy a rejtjelezett szöveg helyigénye ne legyen sokkal nagyobb, mint a nyílt szövegé.

Kriptográfiai szempontból izgalmasabbak a biztonsági kérdések. Ehhez azt kell áttekintenünk, hogy milyen (passzív) támadások érhetik a rendszert.

Támadások

A rejtjelező homomorfizmusokat illetően lényegében háromféle támadásról beszélhetünk. Mindhárom passzív olyan értelemben, hogy a támadó nem próbál meg adatokat módosítani vagy például fizikailag ellehetetleníteni a számításokat, hanem bizonyos adatok birtokában értékes információhoz akar jutni a nyílt szöveggel, a rejtjelező algoritmussal vagy a kulccsal kapcsolatban. Az előbbiekben már utaltunk arra, hogy a rejtjelező homomorfizmus, de bármilyen rejtjelező rendszer biztonsága sem függhet attól, hogy a támadó ismeri-e a rejtjelező algoritmust vagy nem. A rejtjelezés során használt kulcs természetesen titkos, magáról az algoritmusról (vagy leképezésről) azonban mindig feltesszük, hogy nyilvánosan hozzáférhető (bár ezt a hozzáférést nem kifejezett célunk biztosítani).

A legegyszerűbb esetben a támadónak a legkevesebb a kiindulási alapja, azaz ilyenkor a legnehezebb a dolga. Ugyanazzal a K kulccsal rejtjelezett szövegek állnak a rendelkezésére, ezért is nevezik ezt a támadást *rejtjelezett szöveg alapú* támadásnak. A támadó célja ilyenkor ebből a „tudásbázisból" minél több információ levezetése a nyílt szöveget és a használt kulcsot illetően.

Az *ismert nyílt szöveg alapú* támadás esetén $(a, E_K(a))$ nyílt-rejtjeles szövegpárok alapján próbál a támadó a K kulcsra (és a rejtjelező algoritmusra) vonatkozó információkra szert tenni.

A támadó a legtöbb információval a *választott nyílt- vagy rejtjeles szöveg alapú* támadás során rendelkezik. Ebben az esetben a támadó megválaszthatja, hogy milyen nyílt- illetve rejtjeles szöveghez kéri a megfelelő rejtjeles- illetve nyílt szövegpárt, és ennek alapján próbál rájönni, hogy hogyan és milyen kulccsal működik a rejtjelező algoritmus.

A támadások nehézsége a fenti sorrendben csökken, hiszen egyre több kezdő információval rendelkezik a támadó. Úgy is mondhatjuk, hogy a támadások erőssége ebben a sorrendben növekszik, mivel a támadó egyre erősebb, egyre nagyobb a fegyvertára. A támadásra való felkészülés szempontjából viszont fordított lehet az osztályozás, mivel a rejtjelezett szöveg alapú támadáshoz elég a kommunikációs csatornát lehallgatni, míg egy választott szöveg alapú támadásnál ennél nyilvánvalóan többre van szükség. Egy rejtjelező homomorfizmus biztonsági fokát a „természetes" módon határozzuk meg: a homomorfizmus annál biztonságosabb, minél erősebb támadásnak tud ellenállni.

Általában egy rejtjelező homomorfizmus annál jobb, minél magasabb szintű a biztonsága. A szükséges biztonsági szint azonban nagyban függ az adott alkalmazástól. Az adatátruházás nagyobb fokú biztonságot követel, mint a számítás-átruházás. Utóbbi esetben az adatkezelő megkapja a rejtjeles szöveget, elvégzi a szükséges számításokat, majd visszaküldi a rejtjeles eredményt.

Az adatok kódolását és dekódolását az adattulajdonos hajtja végre, és a dekódolás után az adott adatokra vonatkozóan nem folytatódik tovább a kommunikáció. Világos tehát, hogy az adatkezelő csak rejtjelezett szövegekkel találkozik, tehát csak rejtjelezett szöveg alapú támadást tud indítani, amely a támadások közül a leggyengébb. Tovább gyengíthető ez a támadás, ha az adattulajdonos minden újabb számítási igény esetén más kulcsot használ az adatok kódolásához.

Adatátruházás esetében a tulajdonos és az adatkezelő közötti kommunikáció nem ér véget a rejtjeles számítási eredmény visszaküldésével, a dekódolt eredményre ugyanis az adatkezelő tart igényt. Az adattulajdonos tehát a dekódolás után visszaküldi az adatkezelőnek az eredményt nyílt formában.

Ez azt jelenti, hogy teljesen normális működés esetén is az adatkezelő (nyílt, rejtjeles) szöveg-párok birtokába jut, tehát rendelkezik az alapfeltételekkel ahhoz, hogy esetleg egy ismert nyílt szöveg alapú támadást indítson a rejtjelező homomorfizmus ellen. A gyakori kulcscsere ebben az esetben is hasznos a támadás gyengítésében.

Az RSA alapú homomorfizmus támadása

Az RSA alapú homomorfizmus ismert nyílt szöveg alapú támadással feltörhető, azaz p és q értéke megismerhető. A támadás menete a következő: rendelkezésre állnak az $M1, M2, \ldots Mr$ nyílt szövegek, továbbá ezek $E_{(p, q)}(M_i)=(C_i, D_i)$ rejtjeles megfelelői, ahol $M_i=C_i \bmod p$, $Mi=Di \bmod q$ és $i=1, 2, \ldots r$.

A kongruencia definíciója szerint nyilván $p|C_i-M_i$, $i=1,\ldots, r$. Vegyük ezen különbségek legnagyobb közös osztóját, ez legyen $p'=\text{lnko}\{C_i-M_i : i=1,\ldots, r\}$. Hasonlóan definiáljuk q'-t. Mivel p illetve q osztója a C_i-M_i illetve a D_i-M_i különbségeknek, ezért ezek legnagyobb közös osztójának (p' illetve q') is osztója, azaz $p|p'$ és $q|q'$. Még kis r esetén is nagy a valószínűsége, hogy $p'=p$ és $q'=q$. Ha ez nem áll fenn, akkor a támadó minden újabb $(M, (C, D))$ pár birtokában közelebb juthat a titkos prímekhez (azaz a kulcshoz) a $p''=\text{lnko}(C-M, p')$ illetve $q''=\text{lnko}(C-M, q')$ bevezetésével.

A homomorfizmus [4]-ben közölt általánosításával szerencsésen kivédhető ez a fajta támadás. Sőt, az RSA alapú rejtjelező homomorfizmus annyira „sikeres", hogy a későbbiekben ez szolgál megoldási alapul egy adat-átruházó rendszerhez. Az eredményekről bővebben a következő részben olvashatunk.

Mit tudunk a rejtjelező homomorfizmusokról?

A rejtjelező homomorfizmusok használatát talán leginkább megszorító tulajdonság már a kutatások kezdetén világossá vált. Ha a számításokat végző félnek lehetősége van arra, hogy tetszőleges konstansokat rejtjelezzen, és a ≤ predikátum segítségével össze tud hasonlítani rejtjelezett szövegeket, akkor a rejtjelező homomorfizmus nem biztonságos, azaz még a leggyengébb támadásnak, a rejtjelezett szöveg alapú támadásnak sem képes ellenállni. Ebben az esetben ugyanis az $a'=E_K(a)$ értékét egy bináris kereséssel meg lehet „fogni", és onnan a értéke könnyen meghatározható. A keresés indításához szükség van a rejtjelezett konstansokra, például ismert lehet, hogy $E_K(1)=1'$. Ebből a művelettartás miatt kiszámolható $2'=E_K(2)=E_K(1+1)=E_K(1)‡E_K(1)=1'‡1'$

Itt + jelöli azt a műveletet, amelyet a homomorfizmus megtart, ‡ pedig ennek a képtérbeli megfelelőjét. Ez az eljárás folytatható, amíg az összehasonlítás segítségével olyan $2'^n$-t találunk, hogy $2'^{n-1}≤a'≤2'^n$. Folytatva a keresést ellenőrizzük, hogy $a'≤2'^{n-1}‡2'^{n-2}$ teljesül-e. Ha igen, akkor az intervallumnak ebben a felében keresünk tovább a felező eljárással, azaz $a'≤2'^{n-1}‡2'^{n-3}$ feltétel ellenőrzésével; ha nem, akkor az intervallum másik felét felezzük tovább, és az $a'≤2'^{n-1}‡2'^{n-2}‡2'^{n-3}$ teljesülését vizsgáljuk. A keresés végére a' előáll a rejtjeles kettő-hatványok összegeként: $a'=2'^i‡2'^j‡…‡2'^m$. Azaz $a'=E_K(2^i)‡E_K(2^j)‡…‡E_K(2^m)$, ami a művelettartás miatt azt jelenti, hogy $a'=E_K(2^i+2^j+…+2^m)$, azaz $E_K(a)=E_K(2^i+2^j+…+2^m)$, vagyis $a=2^i+2^j+…+2^m$. Az egyenlőség jobb oldala kiszámolható, így a értéke meghatározható.

Az additív rejtjelező homomorfizmusokról [1]-ben bizonyították, hogy a választott rejtjeles szöveg alapú támadásoknak nem képesek ellenállni. Additív homomorfizmus esetén ugyanis a rejtjeles szövegek halmaza a {0, 1} test feletti vektortérnek tekinthető. Válasszunk ebben egy bázist (például rejtjeles „kettő-hatványokat"), és kérjük ennek az ősképét, azaz nyílt változatát. Rendelkezésünkre állnak tehát a következő párok: (1, 1'), (2, 2'), (2^2, $2'^2$),…

Ekkor ha adott egy $a'=E_K(a)$ rejtjeles szöveg, ami alapján meg akarjuk tudni a-t, akkor a' egyértelműen felírható a rejtjeles kettő-hatványok összegeként, azaz a választott bázisban: $a'=2'^i‡2'^j‡…‡2'^m$. Innen a támadás ugyanúgy folytatható, mint az előbb leírt esetben.

Ezt igyekszik kivédeni az additivitás megszorítása [3]-ban. Az r-additív rejtjelező homomorfizmusok segítségével legfeljebb r tag összeadására van csak lehetőség. Így ha$r$ elég kicsi, a rejtjeles szövegek halmaza pedig elég nagy, akkor a fenti támadás nem működik, és a homomorfizmus biztonságos rejtjelezett szöveg alapú támadás esetén.

A bemutatott RSA alapú homomorfizmus általánosításával ismerkedhetünk meg [4]-ben. A homomorfizmus már az eredeti alakjában megtartotta az összeadást és a szorzást, de mint láttuk, az ismert nyílt szöveg alapú támadással szemben nem volt biztonságos. Az általánosítás lényege, hogy az előbbi (a mod p, a mod q) rejtjeles szöveg bonyolultabb formában jelenik meg, és így nincs lehetőség az oszthatósággal kapcsolatos megfigyelések felállítására.

A megtartott műveletek számában jelent áttörést az [5]-ben bemutatott eredmény. Ez ugyanis egy olyan rejtjelező homomorfizmus, amely mind a négy alapművelet tekintetében művelettartó, és ellenálló a rejtjelezett szöveg alapú támadás esetén. Az [1]-ben bemutatott eredmények szerint azonban egy ilyen típusú homomorfizmus képes elérni azt a biztonsági szintet is, ahol az ismert nyílt szöveg alapú támadásnak is ellenáll.

Végül [2]-ben megjelent a [4]-ben bevezetett additív és multiplikatív homomorfizmus egy továbbfejlesztett változata, amellyel már az osztásra is lehetőség nyílik, továbbá bizonyíthatóan biztonságos az ismert nyílt szöveg alapú támadás esetén is. Ezt a homomorfizmust felhasználva alkották meg a prototípusát egy érzékeny statisztikai adatokat átruházó rendszernek, melyet a szerzők néhány éve „Method for secure delegation of statistical data" néven szabadalmaztattak [7], így a rendszer tulajdonságairól többet nem tudhatunk.

Az előbbi homomorfizmus alkalmas minden olyan számítás esetén, amikor az alapműveleteken kívül másra nincsen szükség. Bonyolultabb pénzügyi, mérnöki számítások kapcsán azonban előfordulhatnak további műveletek is, például logaritmus vagy hatványszámítás. További érdekes kérdés, hogy megoldható-e a személyi jövedelemadó számítás rejtjelező homomorfizmus segítségével. Természetesen az internetről letölthetők az adószámító szoftverek, amelyek segítségével a saját számítógépünkön biztonságban kideríthető, hogy melyik bevallás-variáció a legelőnyösebb, de talán kényelmesebb egy olyan alkalmazás, amely on-line lenne képes a kirótt adó összegét megadni, különböző bemenő adatok alapján. Mivel esetleg különféle értékekkel kísérletezne a felhasználó, ezeket az adatokat nem szívesen küldené el feldolgozásra nyílt formában.

Logaritmus-számítás rejtjelező leképezéssel

A logaritmus-számítás megoldható egy rejtjelező leképezéssel, amely szigorúan véve nem rejtjelező homomorfizmus. Legyen a nyílt és a rejtjelezett szövegek halmaza R^+, azaz a pozitív valós számok halmaza. A titkos kulcs legyen egy véletlenül választott pozitív egész r. Egy $a∈R^+$ rejtjeles változata $E_r(a)=a^r$. A dekódolás nem pontosan E inverze, mivel arra számítunk, hogy a kódolás és dekódolás között egy logaritmus-számítás is szerepel. Egy a' rejtjeles szöveg visszaállítását tehát $D_r(a')=a'^{1/r}$ adja.

Könnyen ellenőrizhető, hogy ha a kódolt szöveg logaritmusát dekódoljuk, akkor a nyílt szöveg logaritmusát kapjuk, hiszen $(\log(a'))/r=(r\times\log(a))/r=\log(a)$. Az is látható azonban, hogy ez nem egy klasszikus rejtjelező homomorfizmus, mivel esetünkben a nyílt szöveghalmazon értelmezett logaritmus művelete megegyezik a rejtjeles szöveghalmazon értelmezett párjával, és így nem

teljesül a következő egyenlőség: $E_r(\log(a))=\log(E_r(a))$, hiszen $(\log(a))^r \neq \log(a^r)$.

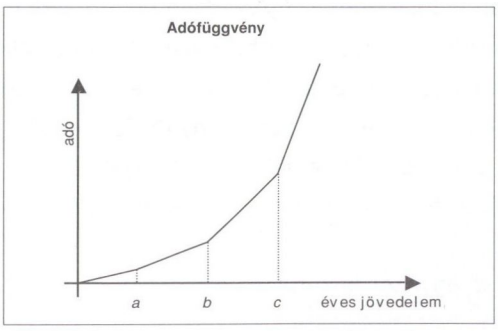
Az adószámítás nehézségei

Egy on-line személyi jövedelemadó-számító szolgáltatás a számítás-átruházás problémáját hordozza magában. Ebben a részben felvázolunk néhány olyan ötletet, amely segíthet a megfelelő homomorfizmus felkutatásában. A szolgáltatást fenntarthatja például egy könyvelő cég, amelyhez azért fordul az adózó, hogy megállapítsák a számára legelőnyösebb adózási formát. Az adózó nyilván nincs birtokában annak a kiterjedt tudásnak, amely ehhez szükséges, másrészt érthető okokból nem szívesen tárja fel nyíltan az anyagi helyzetét a szolgáltató előtt.

A számítások során az adóalapot, az adó mértékét befolyásoló tényezők tekintetbevétele után előbb-utóbb eljutunk arra a pontra, ahol az adótáblázat alapján a jövedelemhez meg kell adnunk a megfelelő adóösszeget. Az adófüggvény intervallumonként lineáris, a függvényérték meghatározásához tehát először meg kell állapítani, hogy a jövedelem milyen határok közé esik. Ehhez szükség van az intervallumok végpontjainak rejtjeles változatára, továbbá egy rejtjeles összehasonlító predikátumra is. Feltehető, hogy az adófüggvény nyílt formában ismert a szolgáltató előtt, ami azt jelenti, hogy az intervallum végpontok (nyílt, rejtjeles) szöveg-párjai egy esetleges támadás céljára rendelkezésére állnak.

Ilyen feltételek mellett a rejtjelező homomorfizmus nem lesz biztonságos, hiszen az összehasonlítás segítségével végrehajtható egy kereső támadás. Tegyük fel, hogy az adóalapot képező jövedelem rejtjeles képe $x'=E_K(x)$. Az adófüggvény segítségével az ehhez tartozó adó értékét akarjuk kiszámolni. Először meghatározzuk, hogy x' melyik adósávba, azaz milyen intervallumba esik. Az adófüggény töréspontjai legyenek 0, *a, b, c,* ezek rejtjeles megfelelői $0'=E_K(0)$, $a'=E_K(a)$, $b'=E_K(b)$, $c'=E_K(c)$. Feltehető, hogy $a' \leq x' \leq b'$. Ekkor az $[a', b']$ intervallumon a már leírt bináris kereséssel meghatározható x értéke.

Választható azonban az a megoldás is, hogy az adótáblázatot minden $[0, N]$ intervallumba eső jövedelemösszegre egyenként megadjuk. Ez azt jelenti, hogy adófüggvényt egy leszűkített értelmezési tartományon értékenként adjuk meg, természetesen rejtjelezett formában. Továbbra is feltehető, hogy a szolgáltató számára ismert a nyílt adótáblázat ebben az alakjában is,



azaz ismeri az $(x, t(x))$ párokat, ahol t az adófüggvény. Ugyan rendelkezésére bocsátjuk az $(x', t(x)')$ párokat is, de ezekből az adatkezelő plusz információk híján nem képes összeállítani az $(x, t(x), x', t(x)')$ négyeseket. Úgy tűnik tehát, hogy az adatkezelőt, mint esetleges támadót, nem hoztuk jobb helyzetbe azzal, hogy biztosítottuk a feltételeket egy ismert nyílt szöveg alapú támadáshoz. Felmerülnek azonban a nyilvánvaló hatékonysági kérdések (hatalmas mennyiségű adat rejtjelezése és továbbítása), amely ronthat ennek az elképzelésnek az alkalmazási lehetőségein.

A rejtjelező homomorfizmusok az adatátruházás és számítás-átruházás kapcsán kerültek bevezetésre, de mivel nagyon sok internetes szolgáltatás hordozza magában ezeket a problémákat, újra előtérbe került az alkalmazásuk lehetősége [8]. A rejtjelező homomorfizmusok sajátos korlátokkal rendelkeznek, a statisztikai jellegű számítások nem megbízható szinten való elvégzése azonban megoldott egy bizonyíthatóan biztonságos leképezés segítségével, amely mind a négy alapműveletet megtartja.

Egyelőre nincsen megfelelő homomorfizmus, amely bonyolultabb szolgáltatások, például logaritmus- vagy határérték-számítást magába foglaló alkalmazások esetén is megoldást jelentene. Cikkünk végén felvázoltunk néhány olyan elképzelést, amely remélhetőleg iránymutatóként szolgál a további kutatásokra nézve.

Irodalom

[1] N. Ahituv, Y. Lapid, S. Neumann: Processing Encrypted Data, Communications of the ACM, Vol. 30, No. 9, pp. 777–780, September 1987.

[2] J. Domingo-Ferrer: A Provably Secure Additive and Multiplicative Privacy Homomorphism, Information Security 2002, Lecture Notes in Computer Science, Vol. 2433, pp. 471–483.

[3] E. Brickell, Y. Yacobi: On Privacy Homomorphisms, Advances in Cryptology, EUROCRYPT '87, Lecture Notes in Computer Science, Vol. 304, pp. 117–125.

[4] J. Domingo-Ferrer: A New Privacy Homomorphism and Applications, Information Processing Letters, Vol. 60, No. 5, pp. 277–282, December 1996.

[5] J. Domingo-Ferrer, J. Herrera-Joancomartí: A Privacy Homomorphism Allowing Field Operations on Encrypted Data, Jornades de Matemàtica Discreta i Algorísmica, Barcelona, March 1998.

[6] R. L. Rivest, L. Adleman, M. L. Dertouzos: On Data Banks and Privacy Homomorphisms, Foundations of Secure Computation, pp. 169–179, New York, 1978.

[7] J. Domingo-Ferrer, Ricardo X. Sánchez del Castillo: „Method for secure delegation of statistical data", P9800608 számú spanyol szabadalom, 2000. dec.

[8] C. Boyens, O. Günther: Trust is not Enough: Privacy and Security in ASP and Web Service Environments, Advances in Databases and Information Systems, 6th East-European Conference, ADBIS 2002, Lecture Notes in Computer Science, Vol. 2435, pp. 8–22.

MTA-események

Neumann János születésének 100. évfordulója alkalmából a Neumann János Számítógéptudományi Társaság (NJSZT) centenáriumi Országos Neumann Kongresszus rendezett, amelyre október 15-17. között a Magyar Tudományos Akadémián került sor. A centenáriumi év fővédnöke Mádl Ferenc köztársaság elnök, a kongresszus szakmai védnöke Kovács Kálmán informatikai és hírközlési miniszter voltak.

A szervezők igyekeztek megtalálni azokat, akiknek valamilyen módon, közvetve vagy közvetlenül közük volt Neumann Jánoshoz. A kongresszus tiszteletbeli vendége dr. Marina von Neumann Whitman, Neumann János lánya volt, és Benoit Mandelbrot, Neumann tanítványa is előadást tartott. Nemcsak a szakma, hanem a közélet képviselői is elfogadták az NJSZT meghívását, és részt vettek, illetve feszólaltak a kongresszuson. Üdvözölte a résztvevőket Mádl Ferenc köztársasági elnök és Vizi E. Szilveszter, az MTA elnöke is.

A Neumann-kongresszus nem fogalmazott meg üzenetet a jövőre vonatkozóan, sokkal inkább összegzésre és a legfontosabb problémák megfogalmazására törekedett. Idén ez annál is inkább érvényes, mivel az Informatikai és Hírközlési Minisztérium ez idő tájt fejezte be Magyarország információs társadalom-stratégiájának kidolgozását, melynek során természetesen figyelembe vették a társaság szakértőinek véleményeit is.

A Magyar Tudományos Akadémia november 3.-án hétfőn a **Tudomány Napja** alkalmából ünnepi ülést tartott. A megnyitó beszédet Vízi E. Szilveszter az Akadémia elnöke tartotta, melyben kifejtette, hogy a hazai szellemi termékek értéke egyre jelentősebb. Hangsúlyozta, hogy Magyarország legjelentősebb nyersanyaga a szellemi tőke, amelyet mind az európai államok szorosabb együttműködése során, mind az új műszaki fejlesztések kidolgozásakor hasznosítani tudunk. Beszédében kitért a legjelesebb magyar eredményekre, és az előttünk álló feladatokra, melynek során szellemi tőkénkre kell a jövőben támaszkodnunk. A Tudomány Napját követő eseménysorozat fontosságát említve első helyen a Világ Tudósainak Fórumát (WSF) említette, mint nemzetközileg is jelentős tudományos összejövetelt.

Az üléssel egyidejűleg kezdődött meg Teller Ede temetése. Ez alkalomból egy rövidfilmmel emlékeztek meg a résztvevők az atomenergia és az atombomba fejlesztésének egyik meghatározó tudósáról.

Magyar Bálint oktatási miniszter beszédének lényege az volt, hogy már jövő évben jelentős összeget különít el az Oktatási Minisztérium a különböző fejlesztési munkákra. Törvényben igyekeznek meghatározni, hogy milyen célokra és milyen módon adnak támogatást. Jelentős újdonság lesz, hogy a régi OMFB, ami lassan elsorvadt és a Minisztérium egyik főosztályává vált, január 1-től ismét önálló hivatal lesz.

Petz Dénes egyetemi tanár a Neumann Centenárium alkalmából új oldaláról mutatta be a tudóst. Mint matematikus, nem műszaki eredményeit, a tárolt programvezérlésű számítógépet hangsúlyozta, hanem az operátorszámításokban elért eredményeit. Ezeket az utókor Neumann-módszerként tartja számon.

Végül akadémiai díjakat adtak át. Heten részesültek az Eötvös József-koszorú kitüntetésben. Ezután az „Arany János Közalapítvány a tudományért" díjait adták át.

Az alapítvány Simonyi Szakkuratóriuma **Dr. Zombory László egyetemi tanárt, a Híradástechnika főszerkesztőjét és a HTE elnökét tüntette ki** sokoldalú és eredményes szakmai munkájáért és tudományszervező tevékenységéért. Gratulálunk elnökünknek!

A Magyar Tudományos Akadémia ünnepi ülése hétfő délután is folytatódott. A WestEnd előtti parkban felavatták Kő Pál Kossuth-díjas szobrászművész domborművét, a Tudósok falát. A domborművön 300 kiemelkedő magyar tudós neve szerepel, arannyal kiemelve azok, akik Nobel-díjat is kaptak. Vízi E. Szilveszter avató beszédében megemlékezett a 21. század mecenatúrájáról, ami a művészetek és a tudomány fejlődésének újabb lendületet ad. Ennek során megköszönte Demján Sándornak, a Trigránit Rt. elnök-vezérigazgatójának, hogy ösztöndíjakkal, jutalmakkal támogatja a tudományt. Elgondolásai alapján és támogatásával készült el ez a dombormű is.

Reméljük, hogy szerzőink és leendő szerzőink közül többen is egyszer felkerülnek a tudósok falára.

LTRACK – Új mobilitás-menedzsment

IMRE SÁNDOR, SZALAY MÁTÉ, *BME, Híradástechnikai Tanszék*

imre@hit.bme.hu

Reviewed

Kulcsszavak: mikromobilitás, keresési idő, mikrocellák

Az LTRACK a „Location Tracking" rövidítése, és egy olyan újfajta mobilitás-menedzsment eljárást takar, melynek a legfontosabb mobilitási protokollok megoldásai a speciális esetei, általános esetben pedig egy hatékonyabb megoldás. Ennek háttere az, hogy jelzésforgalom-igényük kisebb.

1. Bevezetés

Az utóbbi években a mobil távközlés rohamos fejlődését tapasztalhattuk. A mobil hálózatok általában cellás felépítésűek, ahol egy bázisállomás (base station) „fed le", azaz szolgál ki egy cellát. A bázisállomásokat egymáshoz és a többi hálózathoz routerek kapcsolják – általában vezetékes összeköttetéssel. Ahogy a mobil mozog a hálózatban, mindig másik bázisállomáson keresztül kapcsolódik a hálózathoz. Azt az eseményt, amikor a mobil végpont bázisállomást vált, handover-nek vagy handoff-nak nevezzük.

A mobilitás protokolloknak két fontos problémát kell megoldaniuk. Az egyik a mobilitás menedzsment vagy elérhetőség (location management, reachability), a másik a kapcsolatok zökkenőmentessége, folytonossága (session continuity). A mobilitás menedzsment azt jelenti, hogy a mobil helyét valamilyen módon nyilván kell tartani a hálózatban, a kapcsolat folytonossága pedig azt, hogy a beszéd- vagy adatkapcsolatoknak nem szabad megszakadnia handover esetén sem. Mindkét problémára számos megoldás létezik az irodalomban [2,4,5,6]. Ebben a cikkben a mobilitás menedzsment problémájával foglalkozunk részletesen.

A mobilitás menedzsment a következő részproblémákra bontható [1]:

- Mikor frissítsük a mobil pozícióját?
- Ha hívás (vagy adatcsomag) érkezik a mobilnak, hogyan találjuk meg?
- Hogyan tároljuk a mobil pozíciójára vonatkozó információt és hogyan juttassuk el a megfelelő helyre?

Természetesen ezek a kérdések nem függetlenek egymástól, de jól lefedik a problémát. Nem külön-külön keressük a választ rájuk, hanem együtt.

A mobil hálózatok elterjedésének köszönhetően a frekvencia egy nagyon korlátozott erőforrássá vált, ezért a mobilitásban egyre hatékonyabb algoritmusokra van szükség.

A cikk második fejezetében áttekintjük napjaink mobil rendszereit, majd a harmadik fejezetben bemutatjuk az LTRACK-et.

Az LTRACK és a többi mobilitás menedzsment protokoll összehasonlítását a negyedik és ötödik fejezet tartalmazza, a hatodik fejezet a konklúziókat mutatja be.

2. Mobil rendszerek

Beérkező hívás esetén meg kell határozni a hívott mobil pontos pozícióját. Sok mobil rendszer, például a GSM is, „location area" (LA) alapú helymeghatározást használ [1,9]. Ebben a megoldásban több cella alkot egy LA-t, és a hálózatnak arról van információja, hogy a mobil melyik LA-ban tartózkodik, de arról nem biztos, hogy van, hogy pontosan melyik cellában. Mikor hívás érkezik, a hálózat valamilyen módon meghatározza, hogy az LA-n belül melyik cellában tartózkodik a mobil. Ezt az eljárást paging-nek nevezzük [1,9]. Ezzel a megoldással bizonyos hierarchiát viszünk a hálózatba, mely a modern mobilitási hálózatok fontos tulajdonsága. Például az IP mikromobilitási protokollok [2,7,8] hasonló hierarchiára épülnek egy IP hálózatban.

GSM

A GSM az európai mobiltelefon szabvány. Egy GSM hálózatban a „Home Location Register (HLR)" tárolja a hálózatban tartózkodó mobilok pozícióját. Ha a mobilnak nincsenek aktív kapcsolatai (nem folytat beszélgetést), akkor a HLR-nek nem kell a pontos pozíciót ismernie, elég, ha ismeri a megfelelő LA-nak az azonosítóját. Beérkező hívás esetén a LA-ban található összes bázisállomás paging üzenetet küld ki, amelyre a mobilnak válaszolnia kell. Ebből a válaszból tudja meg a hálózat a pontos pozícióját. Ha mobil az egyik LA-ból egy másikba lép, nyilván tudatnia kell ezt a hálózattal. Ennek a megoldásnak egy súlyos hátránya, hogy ha a mobil két olyan cella között mozog oda-vissza, amelyek különböző LA-hoz tartoznak, akkor nagyon sok jelzésüzenetet használ.

Mobile IP

Az IP (Internet Protocol) nem csak az Internet alapjául szolgál, hanem a távközlő hálózatokban a gerinc-

ben is többnyire IP megoldást alkalmaznak (pl. UMTS). A Mobile IP az IP szabványos mobilitás-kiegészítése. A Mobile IP megoldás esetén a mobil otthoni hálózatában (Home Network) az egyik router, az úgynevezett otthoni ügynök (Home Agent) ismeri a mobil mindenkori pozícióját, és továbbítja felé a részére érkezett IP csomagokat. A séma hátránya, hogy az otthoni ügynököt minden egyes handover esetén értesíteni kell az új címről, ami nagyon sok jelzést jelenthet gyakori handover esetén.

Hierarchikus Mobil IP (HMIP)

A Mobile IP-hez hasoló megoldás, csak egy otthoni ügynök helyett ügynökök hierarchiáját használja [3,4]. A fastruktúrába rendezett HA-ek közül mindegyik csak azt tudja, hogy a közvetlenül alatta lévő szinten merre felé kell továbbítani a csomagokat. A legalsó szintű ügynök pedig ismeri a mobil pontos pozícióját. Ezt a megoldást mutatja az *1. ábra*.

A MobileIP-hez hasonlóan a mobilnak itt is értesíteni kell a HA-eket minden handover alkalmával, de a handoverek lokálisabb szinten kezelhetőek, kevesebb jelzésüzenet használatával.

IP mikromobilitás

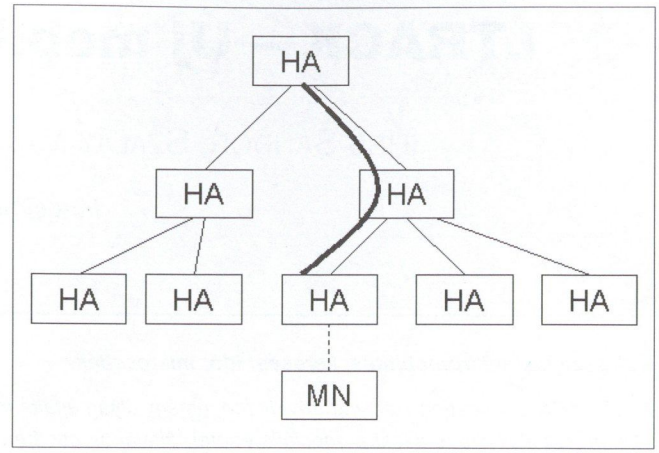
Mikromobilitás esetén is valamifajta hierarchiát alkalmazunk a hálózatban [7,8]. Az IP mikromobilitási protokollok általában együttműködnek a MobileIP-vel, mint makromobilitási protokollal. A hálózatot gerinchálózatra (backbone vagy core) és hozzáférési hálózatokra (access network) bontjuk, ahogy a *2. ábrán* látható. A HA-et csak akkor értesítjük, ha a mobil az egyik hozzáférési hálózatból a másikba lép át. Abban különbözik ez a megoldás a GSM-nél látottaktól, hogy a mobilnak a hozzáférési hálózaton belüli helyét is tároljuk, csak nem a HA-nél. A hozzáférési hálózat átjárója (gateway) a felelős azért, hogy a mobil készüléket az access hálózaton belül megtalálják.

3. LTRACK

Az LTRACK hálózat felépítése

Az LTRACK egy teljesen új megoldás. Az LTRACK hálózat LTRACK csomópontokból épül fel. A mobil egység az egyik LTRACK csomóponton keresztül kapcsolódik a hálózathoz, a hozzáférési pontját természetesen megváltoztathatja.

Az LTRACK keresési módszere valahol a GSM és a Mobile IP eljárások között helyezkedik el. Minden mobil egységhez tartozik egy bejegyzés a „Home LTRACK Register"-ben (HLR), azonban a HLR-nek nincs pontos információja a mobil pozíciójáról (ahogy a HA-nek Mobile IP esetében), a mobil pozíciója mégis pontosan meghatározható (a GSM-mel szemben, ahol csak a megfelelő LA-t ismerjük). A HLR az LTRACK-ben vagy ismeri a mobil pontos helyét, vagy tudja, hogy melyik másik csomópont tud pontos információval szolgálni a pozícióval kapcsolatban.



1. ábra HMIP ügynök-hierarchia

A mobil megtalálása

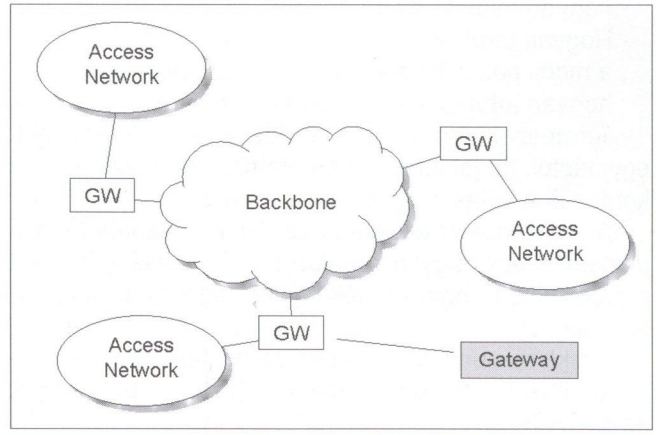
Az LTRACK-ben minden mobil egységnek egy általános egyedi azonosítója van, mint az IP-cím IP hálózat esetén. Ez az egyedi azonosító az otthoni címéhez kapcsolódik. A HLR minden mobilhoz tárolja annak az LTRACK csomópontnak a címet, ahonnan utoljára pozíció frissítést (location update) kapott a mobiltól. Ez a cím egy lépés (next-hop) a mobil felé. A mobil vagy ehhez az LTRACK csomóponthoz kapcsolódik, vagy ez az LTRACK csomópont tudja a következő lépést – egy újabb LTRACK csomópont címét. Az érkező hívást (vagy csomagot) egy sor LTRACK csomópont továbbítja a mobil felé, amelyek közül mindegyik csak a következő címét ismeri, a mobil pontos címét csak az utolsó tudja *(3. ábra)*.

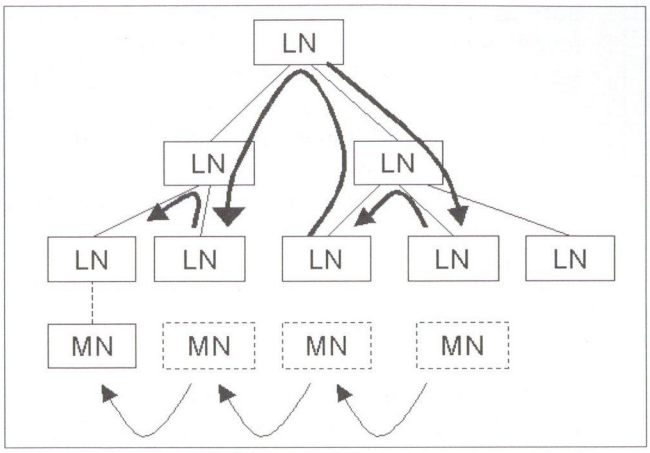
Az LTRACK megoldás esetén fontos, hogy egy LTRACK csomópont egy tetszőleges másik LTRACK csomópontnak üzenetet tudjon küldeni. Ez könnyen elérhető, ha az LTRACK-et egy IP hálózat felett valósítjuk meg.

Handover

Handover akkor következik be, ha a mobil az egyik LTRACK csomóponttól egy másikhoz megy át. Azt a csomópontot, amelyiktől elmegy a mobil, „régi" csomópontnak fogjuk hívni, amelyikhez átmegy, azt „új" cso-

2. ábra Mikromobilitás: gerinchálózat és hozzáférési hálózatok





3. ábra Az LTRACK pozíció-meghatározása

mópontnak. Két fajta LTRACK handover van: normál handover és követő (tracking) handover. Normál handover esetén a mobil a HLR-nek üzen, ott frissíti a pozíció információt. Követő handover esetén a mobil az új LTRACK csomópont címét juttatja el a régi LTRACK csomópontnak, a HLR-t nem értesíti. Egymás utáni követő handoverekből épül fel a lánc, ahol aztán a beérkező hívás végigfut, a normál handover mindig „nullázza" a láncot, ilyenkor a HLR-nek pontos információja van.

Előnyök

Ha csak normál handovert használunk az LTRACK-ben, akkor a Mobile IP-hez teljesen hasonló megoldást kapunk. A HLR játssza az otthoni ügynök szerepét, és mindig pontos információja van a mobil helyéről.

A normál handoverek hátránya, hogy sokkal több jelzési forgalmat generálnak, mint a követő handoverek. Az új LTRACK csomóponthoz a régi LTRACK csomópont általában sokkal közelebb van, mint a HLR.

A követő handoverek másik előnye, hogy ha egymás utáni tracking handoverek során a mobil többször látogatja meg ugyanazt az LTRACK csomópontot, a mobil megkeresésekor ez a „hurok kiesik". Az LTRACK csomópont egyből arra felé fogja továbbítani a kérést, amerre a mobil utoljára elhagyta. Tehát ha a mobil két csomópont között sokat mozog oda-vissza, normál handoverek esetén (Mobile IP séma) nagyon sok jelzési forgalmat generálunk, követő handoverek esetén nagyon keveset.

Ki dönti el, hogy mikor melyik handover-típust használjuk?

Ez a célkitűzéseinktől függhet. A mobil eldöntheti, hogy milyen handovert szeretne, de a hálózat is „ráerőltetheti" valamelyik követési típust a mobilra. Normál handovert bármikor használhatunk, a követő handover használatára nézve azonban vannak bizonyos megkötések. Követő handover esetén a mobilnak értesítenie kell a régi LTRACK csomópontot, tehát ezt a handover típust csak akkor használhatjuk, ha erre lehetőség van. Ez történhet közvetlenül a rádiós interfészen keresztül is (soft handover), vagy az új LTRACK node-on keresztül is (hard handover).

Tehát a követő handovereknek kisebb a jelzés igénye. Miért használjunk akkor egyáltalán normál handovert is?

Ha sok követő handovert használunk, akkor az útvonal a HLR-től a mobilig nagyon hosszú lesz. Tehát a mobil megtalálása sok időt fog igénybe venni, ami nyilván kerülendő. Fontos azonban látni, hogy sok követő handover használata még nem feltétlenül jelent hosszú útvonalat. Ha a mobil sok követő handovert csinál, de útja során csak 5 LTRACK állomást látogat meg (vagyis az öt között mozog oda-vissza), akkor az út nyilván nem lesz 5-nél hosszabb.

Milyen lehetőségek vannak tehát a handover-típusok használatát tekintve?

Korlátozhatjuk egyrészt a két normál handover között megengedett követő handoverek számát. Ha *n* követő handovert engedünk meg, akkor a megtalálási útvonal nem nőhet *n*-nél hosszabbra. Mint azt korábban láttuk, rövidebb lehet, de hosszabb nem. Korlátozhatjuk a két normál handover között eltelt időt is. Egy másik megoldás, hogy a lefedett területet feloszthatjuk LTRACKterületekre (LTRACK area, LTA), és akkor használunk normál handovert, ha a mobil másik LTA-ba halad át, amíg egy LTA-n belül mozog, addig követő handovereket használunk. Ennek a megoldásnak persze megvan az a hátránya, amit a GSM-nél láttunk, vagyis, ha két különböző LTA-hoz tartozó LTRACK csomópont között mozog a mobil oda-vissza, akkor nagy lesz a jelzési forgalom.

Az említett megoldások természetesen kombinálhatóak is. Tehát például LTA-kra osztjuk a területet, mindenképpen normál handovert használunk, ha a mobil új LTA-ba lép át, de ugyanakkor a két normál handover közötti követő handoverek számát is korlátozzuk.

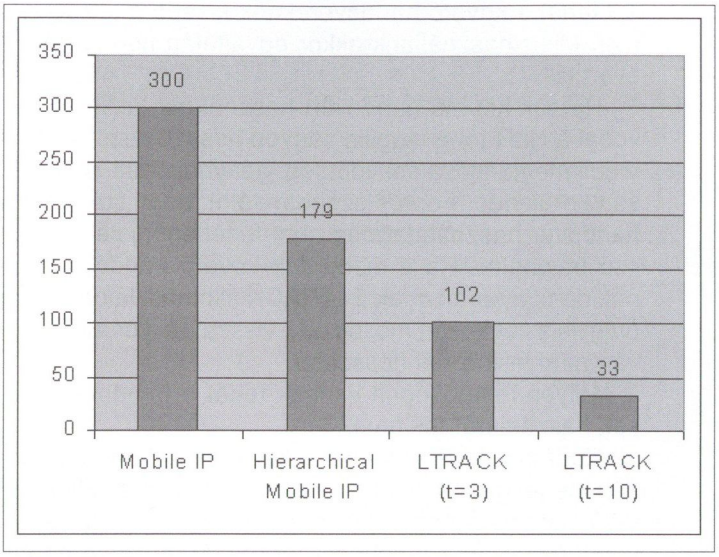
Funkciók

Hogyan „képezhető le" az LTRACK egy valódi mobil hálózatra? A hálózat útvonalválasztói nyilván LTRACK csomópontok. A kérdés az, hogy a bázisállomásokat minek tekintsük. Három lehetséges megoldás van:

- A bázisállomások is LTRACK csomópontok
- A bázisállomások LTRACK csomópontokhoz kapcsolódnak (vagyis az LTRACK csomópontok bázisállomás-vezérlő szerepet is betöltenek)
- Hierarchikus megoldás

Az első megoldásnál a második biztosan hatékonyabb. Ilyenkor amikor a mobil egy bázisállomástól egy másik bázisállomáshoz megy át, lehet, hogy LTRACK értelemben nem is történik handover, mert a két bázisállomás ugyanahhoz az LTRACK csomóponthoz kapcsolódik. Ilyenkor a „handover" egy LTRACK csomóponton belül adminisztrálható.

A hierarchikus megoldás azt jelenti, hogy az LTRACK-et csak gerinchálózati megoldásnak tekintjük, az LTRACK csomópontok pedig nem routerek, hanem hozzáférési hálózatok. Alacsonyabb szinten (tehát hozzáférési hálózaton belül) mikro-szinten kezeljük a mobilitást. Ez a mikromoiblitási megoldás akár lehet szintén LTRACK, ekkor többszintű LTRACK hálózatot hozunk létre.



4. ábra Különböző protokollok jelzésigénye

4. Kvalitatív analízis

A „klasszikus" mobilitás menedzsment megoldásoktól eltérően az LTRACK esetében lehetőség van különböző felhasználókhoz különböző (esetleg időben változó!) paramétereket rendelni, még hatékonyabbá téve ezzel a megoldást. A rendszer menet közben (on-the-fly) is hangolható különböző paraméterek mérése alapján.

Mivel a GSM és a Mobile IP az LTRACK speciális esetének tekinthető, új megoldásunk biztos, hogy nem rosszabb az említett megoldásoknál.

5. Kvantitatív analízis

Hogy mérhetővé tegyük az LTRACK előnyét, egy szimulációt készítettünk MATLAB-bal. A szimulációban a különböző mobilitás menedzsment megoldások jelzés forgalmát hasonlítottuk össze.

A szimulált hálózat 36 bázisállomásból állt, melyek egy 6x6-os négyzetrács mentén voltak elhelyezve és ezen kívül 14 fa-topológiába kötött routert tartalmazott. Az LTRACK előnyét valószínűleg tovább növelné, ha nem fa topológián futtatnánk a szimulációt, de a Hierarchical Mobile IP fa topológiára épül, ezért minden protokollt fa topológián futtattunk, hogy egyenlő pályán tudjuk őket összehasonlítani.

Minden futtatáskor egy mobil egységet vizsgáltunk, amely egy 100 handoverből álló véletlen útvonalon ment végig. Négy protokollt vizsgáltunk meg:

- Mobile IP
- Hierarchical Mobile IP
- LTRACK (t=3)
- LTRACK (t=10)

Ahol a t paraméter jelentése a két normál handover között megengedett követő handoverek maximális száma. A jelzési forgalmat hop-ban mértük. A szimuláció eredménye a *4. ábrán* látható.

Világosan látszik, hogy a jelzés-forgalom Hierarchical MoblieIP-nél sokkal kissebb, mint a MobileIP esetében, az LTRACK azonban mindkettőnél számottevően jobban teljesített kis t érték esetén is.

Hogyan tehető az LTRACK még hatékonyabbá?

- Nem fa topológián futtatjuk.
- Több követő handovert engedünk meg normal-handoverek között.
- Egy LTRACK csomópont több bázisállomást szolgál ki.

6. Összefoglalás

A mobilitás menedzsment megoldások áttekintése után bemutattuk az LTRACK-et, egy teljesen új mobilitás menedzsment protokollt.

Bemutattuk az LTRACK hálózat felépítését, és a handover típusokat. Kvalitatív és kvantitatív megfontolások után az LTRACK-et egy szimuláció segítségével hasonlítottunk össze az Mobile IP és a Hierarchical Mobile IP megoldásokkal.

Irodalom

[1] Vincent W.-S. Wong and Victor C. M. Leung: „Location Management for Next-Generation Personal Communications Networks", IEEE Network, September/October 2000, pp.18-24.

[2] Claude Castelluccia, HMIPv6: A Hierarchical Mobile IPv6 Proposal. ACM Mobile Computing and Communication Review (MC2R), April 2000 issue

[3] Hierarchical MIPv6 mobility management (HMIPv6), IETF draft, (draft-ietf-mobileip-hmipv6-04.txt)

[4] B. Gloss, C. Hauser: "The IP Micro Mobility Approach", EUNICE 2000, September 2000, Eschende pp.195-202.

[5] H. Schulzrinne, J. Rosenberg: "The Session Initiation Protocol: Internet-Centric Signaling", IEEE Communications Magazine, October 2000, pp.134-141.

[6] Z. Turányi, Cs. Szabó, E. Kail, A. G. Valkó: "Global Internet Roaming with ROAMIP", ACM SIGMOBILE Mobile Computer and Communication Review (MC2R), Vol. 4, No. 3, July 2000.

[7] 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

[8] R. Ramjee, T. La Porta, S. Thuel, K. Varadhan: "HAWAII: A Domain-based Approach for Supporting Mobility in Wide-area Wireless Networks", Seventh International Conference on Network Protocols, Toronto, Canada, 1999

[9] Yi-Bing Lin, Imrich Chlamtac: "Wireless and Mobile Network Architectures", John Wiley and Sons, 2001.

Digitális rádiózás hosszú/közép/rövid hullámú tartományokban

DR. SÁRKÁNY TAMÁS *fizikus*
sarkany.tamas@mail.datanet.hu

Kulcsszavak: DAB, DRB, terjedési perspektívák

Az áttérés az analóg technológiáról a digitális technológiára a harmadik évezred elején a rádiózásban is forradalmi változásokat idéz elő: a digitalizálás új távlatokat nyit az amplitúdómodulációs átvitel hosszú/közép/rövid hullámú tartományaiban. Miután a fading, interferencia és rossz hangminőség évtizedekig zavarta az analóg műsorszórást, az ötéves globális fejlesztéssel létrehozott DRM rádiórendszer nagytávolságú átvitel esetén is zajmentes vételt és FM minőségű hangzást eredményez a jelenlegi AM hullámsávokban. Az átmeneti időszak azonban hosszú ideig fog tartani, minthogy gazdasági okokból a globális sugárzású rövidhullámú analóg adások még sokáig megmaradnak, és a több mint kétmilliárd analóg rádióvevő lecserélése horribilis feladatnak tűnik.

A globális rövidhullámú rádiózásnak még mindig világszerte igen nagy a hallgatósága, és a többnyire csak országon belüli tökéletes lefedést nyújtó közép- és hosszúhullámú rádióadásokat is elég sokan hallgatják. Újabban azonban a hallgatók száma észlelhetően csökken, főként a gyenge hangminőség és vételi zavarok miatt, mivel a rádióhallgatók minőségi igényei a CD lemezek, a digitális hangszalagok és az MP3 lejátszók megjelenésével megnőttek.

Az URH tartományban az analóg FM adások leváltása céljából egyes országokban már a 90-es években digitális rádióadást vezettek be, ez a DAB (Digital Audio Broadcasting), amely jobb átviteli minőséget és járulékos szolgáltatásokat kínál. Azonban a DAB sikere kétségesnek látszik: bevezetése a tervezettnél sokkal lassúbb, minthogy a DAB vevőkészülékek drágák, az FM átvitelhez képest csak mérsékelt minőség javulást eredményeznek, és az URH sávban csak kis vételkörzetben használhatók.

A DAB adásoktól függetlenül már 1998-ban megkezdődött egy nagyszabású fejlesztő munka, amely az analóg AM adások minőségének drasztikus javítására irányult digitalizálás útján. A hosszú/közép/rövid hullámú 30 MHz alatti tartományban világszerte több mint kétmilliárd analóg AM rádiókészülék működik, és néhány százmillióra tehető az AM adások hallgatóinak száma.

Az AM rádiózás a legősibb átviteli technológiát alkalmazza, amely elvileg nem sokat változott a XIX. század vége óta, amikor Marconi első kísérleteit végezte elektromágneses hullámok nagy távolságú továbbításával. Az évtizedek során az AM adó és vevő technológiája persze sokat fejlődött, és a hullámterjedési ismeretek is bővültek. Azonban az utóbbi 80 év alatt, az AM rádiózás kezdete óta, mégsem lehetett kiküszöbölni az analóg átvitel alapvető hátrányait:

- Igen nagy adóteljesítmények és így magas üzemi költségek
- Rossz vételi hangminőség a 4,5 kHz-es sávszélesség korlát miatt.
- Nagyobb távolságban gyenge vétel a hullámterjedésből adódó jelingadozás és zaj miatt.
- Hullámterjedési okokból több adófrekvencia szükséges adott célterület ellátásához.
- Nagytávolságú adás esetén frekvencia-váltás szükséges a napszaktól, évszaktól és napfolt-tevékenységtől függően.
- Zsúfolt hullámsávokban a hallgató nehezen találja meg a keresett állomást.

E negatív jelenségek egy idő óta csökkentették az AM adások hallgatóinak számát, ezért egyes adásokat meg is szüntettek. Digitális rendszer használata viszont számos előnyt biztosíthat a rádióhallgatók, a gyártók és a rádiótársaságok számára:

- Olcsó, kis fogyasztású rádióvevő kiváló hangminőséggel
- Jobb vételi minőség, nagyobb műsorválaszték lehetősége
- Járulékos információk szöveges kijelzéssel (állomásnév, műsor címe)
- Régebbi nagyteljesítményű AM rádióadók megtartása
- Meglévő frekvencia kiosztás hatékonyabb kihasználása
- Vételi körzetek célszerűbb ellátása
- Lehetőség több mint két milliárd AM rádióvevő fokozatos lecserélésére

Minthogy minden új rádiós technológiának szüksége van az ITU ajánlásai szerinti frekvenciasávokra, az ITU 1994-ben felhívta a tagállamok hatóságait, nyújtsák be javaslataikat az AM rádiózás digitalizálására. Erre az érdekelt országok a fejlesztés koordinálására globális konzorciumot alakítottak, amely értékelte azokat a beérkezett javaslatokat, amelyek analizálták a 30 MHz alatti sávokban működő analóg technológia digitalizálási eljárásait. Végül egyezség született, amely szerint egyetlen javaslatot továbbítottak az ITU részére, kérve

ennek jóváhagyását a tagállamok részéről. Az illetékes ITU-R (rádió) szekció 6-os tanulmányi bizottsága ennek alapján terjedési vizsgálatokat végzett. Az így született javaslatot az ITU 189 tagállamának többsége 2001-ben jóváhagyta, és ilyen módon az ITU-R hivatalos ajánlásaként megszületett a DRM rendszer (Digital Radio Mondiale), mint az analóg AM műsorszórást felváltó utódrendszer.

Az ITU a hosszú/közép/rövid hullámú tartományban ma már ezt ajánlja az ITU tagállamok rádiótársaságai számára, minthogy – bátran mondhatjuk – csodákra képes: korszerű digitális technológia alkalmazásával a változatlan 9 kHz-es rádiócsatornában 15 kHz-es hangfrekvenciás átvitelt tesz lehetővé, és fading esetén is stabil, zajmentes vételt biztosít! És minthogy a DRM világszabvány lesz, a világon bárhol vásárolt DRM rádió az egész világon fog működni.

ITU ajánlás, DRM konzorcium

Tizenhat vezető műsorszolgáltató vett részt a világ sok részéből a WRC-03 (World Radio Conference) genfi értekezletén, amikor 2003. június 16-án, csupán öt évvel a fejlesztés megkezdése után, történelmi eseményre került sor a genfi tó partján fekvő egyik elegáns kastélyban: több nagy globális rádiótársaság egyidejűleg elkezdte az első rövidhullámú DRM programok sugárzását Európa, az Egyesült Államok, Kanada, a Közép Kelet, Ausztrália és Új Zéland területére.

Az augusztusban Berlinben, szeptemberben Amszterdamban, novemberben New Delhi-ben tartott elektronikai kiállításon élő DRM vételt és prototípus DRM vevőkészülékeket is lehetett látni. A berlini kiállításon a BBC frekvencia diverziti vételt is demonstrált két szinkronizált DRM adó sugárzásával. Ma már 40 rádióállomás sugároz DRM teszt adásokat, többek között a BBC World Service, Radio France Internationale, China Radio International, Deutsche Welle, Kuwait Radio, Radio Canada, Radio Vaticana, Voice of America. (Szokásos AM vevővel ezek az adások erős zaj észlelésével azonosíthatók).

A digitális rádiózás fejlesztését, szabványosítását és a 2003. végére tervezett piaci megjelenést az említett *Digital Radio Mondiale/DRM* globális konzorcium koordinálja. A DRM konzorcium Svájcban regisztrált nonprofit szervezet, amelynek egyetlen célja az, hogy reális költséggel digitális rádiózást és a világpiacon új szolgáltatásokat hozzon létre. A konzorciumot 1998. márciusában Kínában alapította hét országból érkező húsz alapító tag (rádiótársaságok, adó- és vevőgyártók, kutatóintézetek, egyetemek), egy Memorandum of Understanding aláírásával.

Ennek alapján 1998 szeptemberében Amszterdamban konzorcium-szerződés született, amelyet 24 ország 38 küldötte írt alá, Magyarország részéről az Antenna Hungária. A konzorcium székhelye Genf, elnöke a Deutsche Welle német rádióállomás igazgatója. Ma a konzorciumnak 30 ország nagy rádióállomásai és távközlési vállalatai részéről több mint 80 tagja van, magyar tagjai: az Antenna Hungária és a Hírközlési Felügyelet. A vezetőségi tagok évi 10.000 dolláros fizetést kapnak a projektek szervezésével járó költségek fedezésére.

A DRM rendszer széleskörű globális bevezetése céljából az adó és vevő berendezések gyártásához a gyártóknak ipari szabványra van szükségük, amelynek létrehozására az IEC két Technikai Bizottságot hozott létre. Ezeket a szabványokat az IEC és az ITU-R egyelőre közösen fogja megalkotni. Ettől függetlenül már elkészültek a DRM-ETSI szabványok (European Telecommunication Standardization Institute), melyek alapján Európában már megindulhat a DRM berendezések gyártása. A későbbiekben ezt a szabványt világméretű szintre óhajtják emelni.

A tervek szerint az ITU és az IEC közös DRM szabványt fog alkotni, a WRC-2000 konferencián Isztambulban hozott határozat alapján. Az ITU ajánlása szerint a hosszú/közép/rövid hullámú frekvenciatartományokat a csatorna-raszterrel együtt változatlanul át kell venni, és a frekvencia-kiosztást újabb tervezési konferenciákon kell majd meghatározni.

DRM átvitel

A DRM rendszer, amely a 30 MHz alatti frekvenciasávokban rádióműsorok átvitelére szolgál, COFDM átvitellel működik (Coded Orthogonal Frequency Division Multiplex). Az elnevezés jel-kódolásra és OFDM modulációra utal. Utóbbi spektrum-hatékony modulációs eljárás, amely egymástól azonos távolságokban elhelyezett vivőhullámokat alkalmaz a bemeneti hangjelből digitális kódolással előállított bit-sorozat átvitelére. Egy kétszáz, egymáshoz közeli vivőhullám lehet modulálva 64QAM vagy 16QAM kvadratúra amplitúdómodulációval, esetleg QPSK kvadratúra fázismodulációval. A száma és a moduláció a rendelkezésre álló sávszélességtől és a kívánt megbízhatóságtól függően optimalizálható.

A legnagyobb elérhető bitsebesség hangátvitelhez 24 kbit/s, de az alkalmazott bitsebesség ennél kisebb lehet, a megkívánt zavarvédelemtől, a sávszélességtől és a hibajavítás módjától függően. Ugyanis DRM átvitel esetén a sugárzás lefedési területe nemcsak az adóteljesítménytől, hanem a moduláció és a bitsebesség megválasztásától is függ.

A DRM átvitel forráskódolást alkalmaz (erre utal a C betű a COFDM elnevezésben), amely a hibavédelem optimális biztosítására, továbbá a földfelszíni hullámok és a térhullámok terjedési viszonyainak figyelembe vételére szolgál.

Ezáltal extrém esetekben, mint például rossz terjedési viszonyokkal rendelkező rövidhullámul szakaszok esetén, különösen robusztus üzemmódokat és hibavédelmi módokat lehet alkalmazni. A bitsebesség és a bemeneti jel digitális kódolási módja az átvitt információtól és az átviteli útvonal terjedési viszonyaitól függően választható.

Három forráskódolási rendszer jöhet szóba, hogy a legjobb minőséget lehessen biztosítani az átvitt hangjeltől (zene, szöveg) és az ennek megfelelően választott bitsebességtől függően:

- **MPEG-4 AAC** (Advanced Audio Coding), hatásos hibavédelemmel együtt, mono és sztereo adáshoz,
- **MPEG-4 CELP** (Code Excited Linear Prediction) kizárólag mono beszéd-adásra, ha csak kis bitsebességet lehet alkalmazni, vagy hatásos hibavédelemre van szükség,
- **HVXC** (Harmonic Vector Excitation Coding) több beszéd-program átvitelére egy átviteli csatornában, vagy a fő műsorral párhuzamosan hír-csatorna átvitelére, 4 kbit/s bitsebességgel.

Az első forráskódolási rendszer esetén a 9 vagy 10 kHz-es RF csatornában 15,2 kHz-es, majdnem teljes hallható sávátvitel elérhető az SBR eljárás alkalmazásával (Sequential Bandwidth Replication – spektrális sávmásolás). A DRM rendszer várható sikerét döntően a nagytávolságú rövidhullámú vétel esetén is az elérhető úgyszólván URH-FM hangminőség fogja biztosítani, amit e fejlett kódolási rendszer és az SBR eljárás együttes alkalmazása tesz lehetővé. Két csatorna terhelésével valódi sztereo átvitel is lehetséges.

Az MPEG-4 CELP forrás-kódoló 8 kbit/s sebességgel használatos tisztán beszédátvitel céljára, ezzel két vagy akár három beszéd-műsor átvitele lehetséges egy csatornában. A HVXC kódoló a még kisebb 4 kbit/s bitsebességgel működik. Ennek alkalmazásával a főműsorral párhuzamosan például hírek is közvetíthetők, vagy szóba jöhet állókép átvitele, kijelzőn való megjelenítéshez.

A DRM adatstruktúra átviteléhez a vivőhullám-spektrum három csoportra van osztva azért, hogy a műsorjelen kívül különféle vezérlőjeleket lehessen átvinni a DRM vevő számára, a következők szerint:

- Az **MSC csatorna** (Main Service Channel) közvetíti az átviendő műsort (hang vagy kép), utóbbi a vevőkészülék kijelzője számára.
- Az **FAC csatorna** (Fast Access Channel) különféle információkat szolgáltat, például a csatorna sávszélességére és a szolgáltatás fajtájának kiválasztására vonatkozólag. (Gyors hozzáférésre lehet szükség az adó azonosító kijelzéséhez állomás keresés folyamán.)
- Az **SDC csatorna** (System Description Channel) információkat szolgáltat az MSC csatorna dekódolására, és megadja a szolgáltatások jellemzőit a DRM vevő számára (bitsebesség, QAM moduláció fajtája, hibavédelem adata).

DRM vevőkészülék

A DRM adások megkezdéséhez új vevő-típusok bevezetésére lesz szükség, amelyek a DAB rendszerhez hasonlóan alkalmasak lesznek multimédia átvitelre is. A hallgató számára a jobb hangminőségen, nagyobb zajtűrésen és járulékos információk vételi lehetőségén túl további előnyök adódnak. DRM vétel esetében ugyanis a hallgatónak nem szükséges ismernie az adó frekvenciáját, csupán azonosító jelét. Például a Deutsche Welle vételéhez a DW-D azonosítót kell beütni a DRM vevőbe. Erre a vevő megkeresi az ilyen azonosítót sugárzó adó frekvenciáját, és azonos műsort sugárzó több adó esetén a legjobb minőségűt hangolja be. Ha az adó több frekvencián érhető el, ezeket a frekvenciákat tárolja, és a mindenkori legjobban vehető adóra kapcsol át, a hallgató számára alig hallhatóan. Az ilyen „szoftver vevő" analóg adók vételére is alkalmas lehet.

A DRM vevő járulékosan egy újra írható tárolót is tartalmazhat (Flash Memory), amely kívánatra tárolhatja a vett műsort későbbi lejátszás céljára. Ezen kívül a vevő megfelelő interfészen át PC-hez is csatlakoztatható, úgyhogy a vevő által rögzített anyag egy PC-n megjeleníthető és tovább feldolgozható. A tervek szerint USB csatlakozóval rendelkező DRM vevő is fog készülni, amelyet megfelelő szoftverrel ellátott notebookhoz lehet csatlakoztatni. A vevő tehát multimédia megjelenítésre is alkalmas, és szóba jöhet mobil telefonba való integrálása is. Természetesen lesznek csupán hang műsort közvetítő olcsó készülékek is.

DRM adóberendezés

Jó linearitású adóberendezés esetében a kisszintű analóg hang-modulátor helyettesíthető a digitális üzemhez szükséges OFDM áramkörrel, és így egy meglévő adó viszonylag kis befektetéssel digitális üzemben is működhet. Az OFDM jel ahhoz a ponthoz csatlakozik, amelyhez az analóg kis-szintű jel csatlakozott, ezért a torzításmentes átvitelhez kellő sávszélesség és igen jó linearitás szükséges. A nagyteljesítményű végfokozatok, amelyek az adó költségének és áramfelvételének nagy részét teszik ki, általában DRM üzemben is változatlanul alkalmazhatók. Adott terület digitális besugárzása az analóg AM adáshoz képest tipikusan 6-10 dB-lel kisebb adóteljesítményt, és ez által kisebb hálózati teljesítmény-felvételt kíván. Ez kisebb energiaköltséget jelent, csökken a környezeti zavarósugárzás, és tehermentesíti az energiaellátást, ami fejlődő országokban lényeges szempont.

Terjedési vizsgálatok

Az eddig elvégzett terepkísérletek során sok gigabájt nagyságrendű terjedési adatot értékeltek ki. Ezek látványosan mutatják a nagy különbséget az ismert analóg AM átvitel és az új digitális DRM technológia között vételi minőség tekintetében.

A mérések szerint a nappal domináns földfelszíni középhullámú sugárzás esetén kiváló vételt eredményez, és az éjjel fellépő térhullámnak sincs zavaró hatása, eltérően az analóg AM adások jól ismert „szelektív fading" torzításától. A térhullámra vonatkozó eredmények rövidhullámú átvitel esetében azonosak a középhullá-

mon kapott eredményekkel. Közös csatornás és szomszéd csatornás interferencia, jelingadozás és zaj nem figyelhető meg a DRM vételben, amíg a bit hibaarány nem nő 10^{-4} fölé. Megjegyzendő, hogy a használható maximális bitsebesség rövidhullámú adások esetében kisebb, mint középhullámon. Ennek oka az, hogy több ezer kilométeres távolságok esetében a térhullám többszörösen reflektálódik az ionoszféra és a földfelszín között.

A DRM rendszer paraméterei és karakterisztikái

- A meglévő rövid/közép/hosszú hullámú frekvenciasávok használata 30 MHz alatt
- Az ismert spektrum változatlan használata, új frekvencia kiosztások nélkül
- Simulcast adások lehetősége, tehát AM és DRM adás egyidejűleg egyetlen adóval
- A meglévő adóberendezések és adóállomások további használata
- Változatlan besugárzott terület mellett lényegesen kisebb adó-áramfelvétel
- Azonos csatornatávolság és RF sávszélesség AM és DRM esetén
- 2,4 bit/Hz a digitális rendszerek legnagyobb spektrum hatásfokát jelenti
- MPEG 4 AAC forráskódolás + SBR esetén 15,2 kHz hangfrekvenciás sávszélesség
- Csatornák összevonásával valódi sztereo átvitel lehetséges
- Lehetőség programkísérő vagy független adatátvitelre (szöveg, grafika és kép)
- Automatikus vevő behangolás az adó azonosító beadása után
- Automatikus áthangolás a mindenkor legjobb vételt nyújtó frekvenciára
- Stabil rádióvétel kedvezőtlen térerősség, zaj vagy interferencia esetén
- Lehetőség nagytávolságú sugárzásra kiterjedt célterületek ellátásához
- Hordozható vevő egyszerű antennával is megbízható vételt biztosít, épületen belül is

Jövőkép

DRM terepvizsgálatokat 2000 óta végeznek szerte a világon. 2002-ben indultak a pilot adások, 2003-ban pedig már reguláris DRM adások vannak folyamatban. A globális rádiókommunikációs értekezlet, a WRC-03, jóváhagyta az ITU-R által a 30 MHz alatti digitális műsorszórásra vonatkozó ajánlást. Erre az alkalomra a DRM konzorcium egy piaci bevezetési tervet készített, megadva a DRM adások és a DRM vevőkészülékek megjelenési időpontját a világ egyes körzeteiben.

Az előjelzések szerint az analóg és digitális adások közötti lényeges minőségi különbség folytán várható a több mint 2 milliárd analóg vevőkészülékkel rendelkező piac fokozatos meghódítása. A piac megnyitása alkalmából stratégiai együttműködés készül a vevőkészülék gyártók, az adóállomások és az egyes országok hírközlési felügyeletei között, amelynek keretében árulják majd a digitális vevőkészülékeket. 2004. végére várhatók a tömeggyártással előállított első DRM csipek, amelyek lehetővé teszik majd az olcsó DRM vevők tömeges piacra dobását.

A Sony prototípus modulátora SCS átvitelre is alkalmas (Single Channel Multicast), amelynek során a műsor egyidejűleg DRM és hagyományos AM átvitellel lehet közvetítve oly módon, hogy a 9 kHz-es csatorna egyik fele a DRM spektrumot, másik fele pedig két oldalsávos hagyományos AM jelet visz át (kisebb felső határfrekvenciával). Ilyen módon az AM jelet a hagyományos AM vevők is vehetik. A tervek szerint a DRM vevők AM demodulátort is fognak tartalmazni, és így a hosszú ideig tartó átmeneti időszakban mindkét fajta jel vételére alkalmasak lesznek. Áruk eleinte 25-50 dollárral fogja meghaladni az AM vevők árát, de mint minden új technológia esetén, ez is idővel csökkenni fog. A végső cél az, hogy a DRM vevő ne legyen drágább, mint egy mai ekvivalens AM vevő. A DRM vevők tömeges megjelenése 2004 utánra várható.

A gondos előkészítések ellenére számolni kell hosszú, több mint tíz évig tartó átmeneti időszakra, amelynek folyamán az analóg sugárzás még párhuzamosan fog folytatódni. A rövidhullámú tartományban ez esetleg eltérő frekvenciasávokban történhet majd, de közép- és hosszú hullámon ez nem valószínű, minthogy itt az adók részére rögzített frekvenciák vannak. Ez nem jelent majd problémát, hiszen a DRM csatornák együtt létezhetnek a szomszédos AM csatornákkal. Japánban 2011-re tervezik a digitális adóhálózatnak az egész országra történő kiépítését, egyúttal az analóg hálózat végleges leállítását.

Az átmeneti időszak hosszabb ideig fog tartani, mint az analóg FM-DAB átmenet, mert a világszerte használt analóg rádióvevőket gazdasági okokból még hosszú ideig üzemben kell tartani, főként a fejlődő országokban. Végül is azonban biztosra vehető, hogy a DRM rendszer igen sok előnye folytán az analóg adások az átmeneti időszak után világszerte fokozatosan meg fognak szűnni.

Irodalom

[1] Heinz Preibisch, DRM:
Digital Radio Mondiale,
Telekom Praxis 1/2003, p.30.

[2] Dr. Gschwindt András:
Az AM műsorszórás újjászületése,
HTE hírlevél, 2003. október

[3] Dr. Gschwindt András:
Szól a DRM,
Rádiótechnika, 2003/9, p. 424

[4] www.etsi.org, www.drm.org (angol nyelven),
www.drm-national.de (német nyelven)

[5] ITU Rec. BS1514-1,
Service requirements for digital sound broadcasting below 30MHz

[6] ETSI Rec. TS 101 980 V1.1.1 (2001-09),
Digital Radio Mondiale (DRM); System Specification

Könyvet ajánlunk

A digitális földfelszíni televíziós műsorszórás

Szép kiállítású, aktuális és színvonalas könyvvel lepett meg minket az Antenna Hungária. A 146 oldalas mű a témával kapcsolatban mindenkinek kielégíti az igényeit. Magas színvonalú műszaki ismertetést, helyzetképet ad a DVB-T terjedésének helyzetéről, a szabályozásról és a jövőképről.

Az első fejezetben hat ország DVB-T bevezetéséről olvashatunk. Valamennyi fejezet foglalkozik a szabályozással, a jogi háttérrel, az infrastruktúrával, az árakkal, az előfizetés módjával és a makró szabályozási környezettel. Nagyon ügyesen van szerkesztve, így könnyű összevetni a különböző országok megoldásait, és hamar felismerni azt, ami közös és könnyű átvenni.

A második fejezet a rendszertechnikát írja le. Ez a szöveg bármely műszaki főiskolán vagy egyetemen a műsorszórás oktatásának színvonalas része lehetne. Blokk-diagrammokkal, a modulációs rendszerek táblázatos értékelésével, a gyakorló tervezőknek is sok segítséget nyújt.

A következő rész a szolgáltatásokat ismerteti. Rendkívül érdekes, ahogy a szinte triviális szolgáltatásoktól az interaktív szolgáltatásokon keresztül az igény szerinti programrendelésig eljut. Lehetőség van a személyre szabott alkalmazások bevezetését is megtanulni a könyvből, melynek már közvetlen következménye a távoktatás. Ennek hagyományait hasznosítja, de továbbmegy és multimédiás tananyagok szerkesztésére és szétosztására is tanácsot ad. Látszik, hogy gyakorló szolgáltatók írták a könyvet, mert nem hanyagolják el a tarifálást és az elszámolás témáját sem. Mivel a pénz is szóba kerül, tehát összekötik a DVB-T lehetőségeit az elektronikus tranzakciók felépítésével. Ez a fejezet is bármely oktatási intézményben használható lehetne.

A negyedik fejezetben összehasonlítja a különböző szabályozási rendszereket, amely remélhetőleg tanulságul szolgál majd a hatóságnak a magyar digitális műsorszórás bevezetése során. A tapasztalatok nem jelentenek kötelező átvételt, de a korábbi fejezetekkel összevetve mindenkiben kialakulhat, hogy mit érdemes és mit nem szabad átvenni.

A hazai helyzetnél bemutatja a szabályozási kereteket, az infrastrukturális hátteret és a tartalomszolgáltatói piacokat. Meglepő az a kördiagram, mely a 2001-es piaci részesedést mutatja be. Feltétlenül érdemes az olvasóknak ajánlani, hogy ezt vesse össze a 2003. évi statisztikai adatokkal, és akkor elgondolkodhat azon, hogy mi okozta a jelentős változást. Nyilvánvalóan ezt meg lehet fejteni és indokolást is lehet adni. Ebből minden tartalomszolgáltató tanulhat.

Érdekes, hogy az utolsó oldalakon olyan filozófiai kérdéseket is megérthetünk a könyvből, amelyek a magyar nyelvvel, a hazai hagyományokkal kapcsolatban felmerülhetnek a műsorszolgáltatásnál.

A fentiekből látszik, hogy igazán értékes könyv van a kezünkben. Ezek után érthetetlen, hogy senki nem vállalja a felelősséget ennek a könyvnek a megírásáért, lektorálásáért és szerkesztéséért, pedig nem félni kellene, hanem lehetőséget adni az olvasóknak, hogy gratuláljanak mindazoknak, akik ezt összeállították.

Valószínűleg sokan megkeresnék a szerzőket további kérdéseikkel, esetleg azután érdeklődnének, hogy milyen műszaki, vagy gazdasági változások történtek az elmúlt évben, így ezzel az interaktivitással valamennyien jól járnánk.

Amennyiben lehetőségünk lesz rá, a Híradástechnika januári számában szívesen közzé tennénk mindazoknak a nevét, akik a könyv megszületését elősegítették.

L.Gy.

Hírek

A **Sony** elkötelezte magát, hogy segít kiszélesíteni a digitális rádió piacát Európában megfogadva, hogy aktív támogatást nyújt a DRM és a World DAB Forum kereskedelmi szektoraiban. A DRM az egyetlen nem szabadalmaztatott, univerzálisan szabványosított digitális rendszer a világon rövid-, közép-, és hosszúhullámon, amely már a meglévő frekvenciákat és sávszélességeket hasznosítja. A DRM világszerte újraéleszti a rádiós piacot, 2004-re várhatóan DRM vevők széles választéka jelenik meg a boltokban.

Az IBC2003 konferencián a **DRM** bemutatta standján a nemrég beindított élő adásait különböző vevőkön, melyek között egy második generációs fogyasztói vevőkészülék is szerepel, ami még ebben az évben piacra is kerül. Emellett látható volt egy USB vevő bemutató modellje is, kereskedelmi ügynökök számára. Ezek a vevők a legfrissebbek a DRM fejlesztési sorozatából, amelyek két hónappal a WRC 2003 júniusában történt digitális rádiórendszerek nemzetközi debütálása után láttak napvilágot. Azóta az élő napi vagy periodikus alkalmi adásokat sugárzók száma 26-ra emelkedett, a kínai kormány megerősítette, hogy teszteli a DRM rendszert a későbbi felhasználás céljából, a DRM és a World DAB Forum bejelentették együttműködésüket, megerősítve ezzel a DRM-et és DAB-ot venni képes vevők jövőjét.

A **svédek** a széles sávot vonzóbbnak találják, mint a digitális televíziót – ez a legújabb tendencia derül ki a stockholmi székhelyű Mediavision tanácsadó cég új jelentéséből. 2003 második negyedévében rekord szintet értek el a szélessávú összeköttetés megrendelések. Az említett időszakban 250.000 új lakossági szélessávú hozzáférést regisztráltak. Svédország kilencmilliós lakosságából több, mint 1,6 millió fizet elő valamilyen szélessávú/nagysebességű Internet szolgáltatásra. Egyetlen év alatt több, mint 600.000-rel nőtt a szélessávú felhasználók száma, további 1,6 millió lakos pedig tervezi, hogy „egy éven belül" széles sávra kapcsol.

Az **SCM Microsystems** megalkotta a világ első PCMCIA-alapú digitális TV adapterét. A mobil földfelszíni vevő képes a digitális földfelszíni jelek és a kábel nélküli adatszolgáltatások vételére a laptopokon és a palmtopokon. A kicsi, igen könnyű berendezés nem igényel tápegységet. A vevők nagyobb mennyiségű szállítása várhatóan 2004 első negyedévében indul be. Az első modell a német piacot célozta meg, habár az bármelyik elérhető DTT szolgáltatással kompatibilis lenne.

Egy jelentés szerint a **brit** kormányzatnak „jelentős állami támogatást" kell nyújtania a digitális televíziót választó TV-nézők számának fellendítése érdekében, ha el akarja érni 2010 évi célját, miszerint megszűnne a meglévő analóg műsorszórás. A jelentésben állítottak szerint a Freeview, a BBC és a BSkyB vegyes vállalat sikerének ellenére – amely vállalat a nézőknek egyszeri díj ellenében biztosít hozzáférést a digitális televízióhoz – a kormányzat még mindig valamelyest elmarad azon céljától, hogy a lakosságot meggyőzze arról, hogy az évtized végéig váltson digitálisra.

A felmérést készítő Strategy Analytics cég előrejelzése szerint a digitális televíziós szolgáltatások vételéhez szükséges adapterek ára négy éven belül 27 fontra fog esni. Úgy véli azonban, hogy a kormányzatnak jelentős pénzösszegeket kell az adapterek és digitális TV-készülékek fejlesztésére áldoznia, ha a nézők többségét meg akarja győzni az átállásról. A felmérés szerint az adapterek ára a mostani 60-80 fontról 30 font alá esik, ami hozzá fog járulni azok számának növeléséhez, akik meglévő antennáikkal digitális televíziót néznek.

A Strategy Analytics felmérése szerint a digitális földi televíziózás (DTTV) iránti igény most kezd jelentkezni. Előrejelzésük szerint a DTTV-vel rendelkező európai háztartások száma 2003 végére a kétszeresére, azaz 3,7 millióra nő. Az olcsóbb set-top boxok – amelyek ára már most 100 euró alatt van – felelősek részben a keresletért. A set-top boksz gyártók közötti éles verseny az elkövetkezendő néhány év során gyorsan csökkenő árakat fog eredményezni.

A világ első 100%-ban **pandzsábi rádióállomása** arra vállalkozott, hogy két digitális multiplexen keresztül közvetít adást, amelyek közül az egyik a The Digital Radio Group által november 8-tól üzemeltetett London Three, a másik pedig a TWG-EMAP Digital által 2004. január 5-től működtetett Bradford &Huddersfield. A Panjab Radio, amely három éve gondoskodik a pandzsábi közösség igényeinek ellátásáról, egyidejűleg közvetíti majd műholdas szolgátatását is, amely jelenleg a 880-as Sky Digital csatornán érhető el. 2001. szeptembere óta az interneten is közvetít műsort. Az állomás 70%-ban zenét, 30%-ban szöveges műsorokat sugároz, ezen belül hagyományos és modern progresszív pandzsábi zenét közvetít minden korosztály számára. A programban emellett magazinműsorok, hírműsorok valamint pandzsábi vallásos és irodalmi művek felolvasásai szerepelnek. A Panjab Radio bekapcsolása a multiplexek közé újra aláhúzza a digitális rádiónak azt az elkötelezettségét, hogy szélesíteni kívánja a rádióhallgatás választékát az általa kiszolgált közösségek számára.

A hazai antennavizsgáló telephely története

DÓSA GYÖRGY
okl. villamosmérnök

Kulcsszavak: antennatörténet, mérési módszerek

A háború utáni években a rádió-műsorszórás fontossága, jelentősége megnőtt, ami az üzembelépő új adóberendezések és antennarendszerek számában és a teljesítmény növekedésében jelentkezett. Európa, Közel-Kelet és részben Észak-Afrika területein nagyteljesítményű hosszú,- közép,- és rövidhullámú adóberendezéseket és különféle kialakítású antennarendszereket telepítettek. Ugyancsak megindult – különösen az európai területen – az URH-FM adóberendezések és antennarendszerek használata. Az élvonalbeli híradástechnikai cégek, kutatóintézetek és egyes országok postai szervei, az antennarendszerek hatékonyabb fejlesztése, tervezése és gazdaságosabb gyártása érdekében antennamérő és vizsgáló telephelyeket létesítettek az ötvenes évek elején.

1. Nemzetközi és hazai előzmények

Az antennamérő- és vizsgáló telephelyek alkalmazásának célja a tervezés alapján a számított értékek helyességének ellenőrzése kicsinyített vagy valóságos modellekkel. Az elektromos és mechanikai jellemzők vizsgálatával továbbá a szerkezeti konstrukciós és mérési módszerekkkel segítették a fejlesztőket.

A telephelyek kiépítése jelentős költségkihatással járt és csak akkor gazdaságos, ha sokoldalúan – különféle antennák (hosszúhullámtól mikrohullámig) tervezésénél, fejlesztésénél egyaránt – használhatóak. A mérő telephely felszerelését a végrehajtó mérések, vizsgálatok szabják meg.

Bár egy antenna vagy antennarendszer tulajdonságai közül az irányítényező a bemeneti impedancia legfontosabb, azonban a mérések folyamán előforduló minden részlet adat jelentős, mert ezeket összegezve a vizsgált antenna tulajdonságairól teljes képet adnak.

Egy antenna minőségét a következők jellemzik:
- az antenna bemenő impedanciája, sugárzási ellenállás, állóhullámarány,
- az antennagerjesztés elosztása (áram, közeltér, mikrohullámú tartományban az appertura tér, fáziscentrum stb.),
- az antenna távolterének mérése (irányítényező, nyereség, polarizáció, hatásos reflektáló felület),
- földhálózattal kapcsolatos mérések (földáram, vezetőképesség, reflexió).

Az ötvenes évek második felében Európában két korszerű antennamérő, vizsgáló telephely épült ki. Az egyik a Rohde&Schwarcz cég müncheni, a másik az NDK területén a Brück-i telephely. Az ötvenes évek végén kezdte meg működését az USA-ban a Bedford-i MIT Lincoln laboratóriumának vizsgáló állomása.

A Brückben kiépült antennamérő telephelyet a német postán kívül híradástechnikai gyártó cégek és kutatóintézetek is használták. Itt épült ki az első, 54 méter magas, teljesen fémmentes, öntartó fa mérőtorony. Később kiépült még egy egyes és egy kettős 54 méter magas fa mérőtorony is. A villámvédelme automatikus tekercselő szerkezettel volt ellátva, így a mérések alatt a villámhárító rendszert fel lehetett gombolyítani.

A tornyok alatt nagyfrekvenciás földhálózat is kiépült, melyet rövid-, közép-, és hosszúhullámú vizsgálatoknál használtak.A vizsgálandó antennákat egy forgó szerkezetre lehetett erősíteni. A forgó szerkezetet akkumulátor táplálta és távvezérelhető volt. A Brück-i antennamérő telephely univerzális kialakítású volt. Akár antennák, akár modellek mérésére alkalmas volt.

A Rohde&Schwarcz cég müncheni telephelye főleg URH, TV és mikrohullámú antennák, antennarendszerek és modellek vizsgálatára készült. A vízszintes és függőleges iránykarakterisztikák felvételét automatizálták.

A MIT Lincoln laboratóriumának Bedford-i mérő telephelye főleg 300-16000 MHz-ig terjedő sáv részére használatos antennatípusok, tehát URH-TV és mikrohullámú antennák mérésére, vizsgálatára készült. Ezen kívül antennamodell kísérleteket is végeztek a telephelyen.

Hazánkban az antennamérő- és vizsgáló telephely megvalósításának gondolata először 1948-ban a PKI-ban, egy szakmai értekezleten merült fel, miután tervezték a hazai közép- és rövidhullámú műsorszóró adóhálózatunk fejlesztését és az URH-FM műsoradások távlati megindítását. Várható volt ezért antennafejlesztések megkezdése, és ehhez vizsgálatokra volt szükség. (A javaslattevők Bognár Géza, Sárközy Géza, Czeglédy György, Kodolányi Gyula, Szikszay Lajos, Susánszky László és Garai László voltak.)

A hazai telephely létrehozásában az első konkrét lépések 1957-ben történtek, miután a BHG megkezdte az URH-FM adók és antennák fejlesztését. Több híradástechnikai cég részéről (EMV-BRG-HTV), akik különféle antennarendszerek tervezésével kezdtek foglalkozni, valamint a Magyar Posta és egy-két kutatóinté-

zet részéről is igényként merült fel, hogy kiépüljön egy antennamérő- és vizsgáló telephely. A BHG 1957-ben Budapest környékén, Bugyi-Telekpusztán egy ideiglenes telephelyet hozott létre, ahol 1958-ban URH-TV antennák mérését és vizsgálatát kezdte meg. A területen ebben az időszakban sem épület, sem felszerelés (torony stb.) nem volt kiépítve.

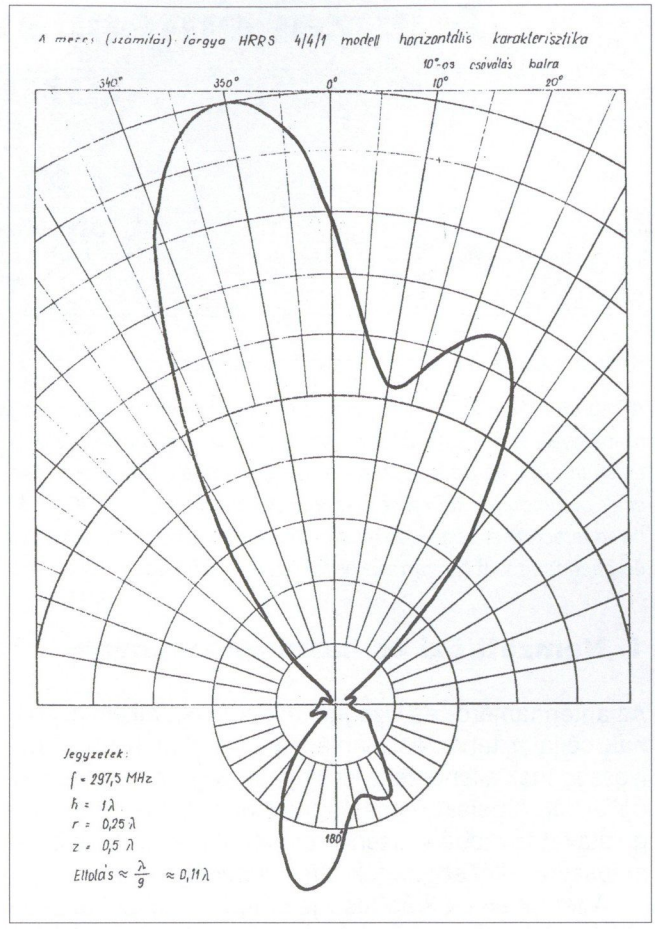
A növekvő hazai mérési és vizsgálati igények miatt a telephely kiépítése (mérőtorony, épületek) felszerelése feltétlenül aktuálissá vált. Ennek érdekében a PKI több változatban készített tanulmánytervet antennamérő telephelyre (1962-ben Kiss Lajos). 1958-ban az Elektromechanikai Vállalatnak (ÉMV) új fejlődési szakasza kezdődött, ezért szükség volt fejlesztési laboratóriumok bővítésére, valamint az URH és TV antennarendszerek fejlesztéséhez korszerű antennamérő telephely kialakítására. Ennek érdekében az ÉMV 1960-ban megvette a Bugyi-Telekpusztai területet, és megkezdte a telephely kiépítését, aminek fő szorgalmazója és irányítója Tófalvi Gyula volt. Műszaki és gazdasági okok miatt a telephely nem minden antennatípus, hanem főleg URH-TV antennarendszerek és modellek vizsgálatára készült. A mikrohullámú antennák vizsgálatára pedig a TÁKI épített ki egy kis telephelyet.

A Bugyi-Telekpusztai telephely az alábbi kívánalmak figyelembevételével épült:

a) megfelelő, nagy kiterjedésű, nyílt, egyenletes planírozott földterület (kb. 2-3 hold), reflexiómentes méréshez szükséges védett terület (kb. 10-15 hold);
b) legalább két nagyobb és egy kisebb – megfelelő teherbírású – mérő fatorony, melyeket fa vagy műanyag csapokkal és kötőelemekkel kell építeni fémmentes kivitelben, kivételt képez az antennákat tartó és forgatható toronyszerkezet;
c) a telephely nem építhető repülőtér közelségébe, nem lehet a közelben műút a gépkocsik gyújtásának zavara miatt;
d) be kell tartani a közép- és nagyteljesítményű rádióállomásoktól, lokátor állomásoktól a számított védőtávolságot a zavartatások elkerülése miatt;
e) a fatornyok villámvédelmét olyan villámhárító rendszerrel kell ellátni, amelyek huzalanyagát mérések előtt automatikusan felgombolyítják;
f) a mérőtornyok alatti fa mérőházakba a villamoshálózatot földkábelen kell bevezetni, a légvezeték-földkábel csatlakozásnál megfelelő zavarszűrő egységeket kell beépíteni.

2. Telekpusztai antennamérő telephely létesítése és használata

A telekpusztai kísérleti antennamérő telephely első szakasza 1961 végére, a második szakasza pedig a hetvenes évek elejére épült ki. Itt egy 40 méter magas, öntartó fa mérőtorony, továbbá egy 45 méter magas forgatható antennatartó vastorony épült. A két torony közötti távolság 100 méter. Kiépült még a fa mérőtoronytól



1. ábra

60 méter távolságra egy 32 méter magas szintén forgatható vastartótorony. A mérések lebonyolítására egy mérőbunker, valamint egy fa épület készült.

Először 1960-ban a kékesi TV III-as sávú antennarendszert, majd 1962-ben a kabhegyi antennarendszert, a következő 3 évben a miskolci, az ózdi, a salgótarjáni és a tokaji TV sugárzó rendszert vizsgálták. 1971-ben pedig az újabb TV III. sávú antennarendszert mérték be, mely Sopronba került. Jelentős volt az 1968-ban induló jászberényi rövidhullámú adóállomás építése, melynek teljes kivitelezését a Magyar Postával kötött szerződése alapján fővállalkozásban az Elektromechanikai Vállalat (EMV) végezte. Az állomáson 2 db 250 kW-os automata hangolású, elgőzölögtetéses hűtésű rövidhullámú adóberendezést 28 db nagy- és középhatótávolságú irányított és 2 db közelsugárzó antenna és tápvonalrendszerek kiépítését és üzembe állítását kellett megvalósítani 3,9–26,1 MHz frekvenciatartományban.

A Magyar Posta a szerződésben megadta a besugározandó célterületeket (sugárzási irányokat), továbbá az előzetes hullámterjedési számítások alapján a sugárzási frekvenciasávokat és az alkalmazandó antennarendszerek típusát, melyek:

– HRRS 4/4/1 típusú nagytávolságú irányított antennarendszer,
– HRR 2/2/0,25 típusú középható távolságú irányított antennarendszer,

– TRO 4/1/0,25 típusú
közelsugárzó, körsugárzó antennarendszer.

A Postai szerződés előírta, hogy az alkalmazandó antennarendszereket modell mérésekkel is ellenőrizni kell (kicsinyített és 1:1 arányú modell vizsgálatok). A tervezési munka tényezői közé tartozott a modellezés útján szerzett mérés és vizsgálat, mely vizsgálatokat 1970-1971 években végezték el.

A mérés az alábbiakra terjedt ki:
– horizontális karakterisztika mérése az elevációs szög síkjában,
– horizontális karakterisztika mérése a HRRS 4/4/1 antennáknál +/- 10°-os billentés esetére is,
– vertikális karakterisztikák felvétele 20° illetve 28° elevációs szögig,
– bemeneti impedancia mérése.

A modell méréseknél külön speciális feladatot jelentett a szigetelők kicsinyített méretben való kialakítása, valamint a tizedmilliméteres vastagságú dipolok megfelelő mértékű feszítése, megfogása.

A vízszintes sugárzási karakterisztikák felvételéhez modelleket a vízszintes síkban forgatták. A modellek vertikális karakterisztikájának felvételéhez a mérőtornyon a mérővevő-antennát függőleges irányúan mozgatták.

Egy-egy jellegzetes horizontális és vertikális sugárzási karakterisztikát az *1. és 2. ábrák* mutatják.

A modell mérésekkel a horizontális és a vertikális sugárzási karakterisztika a fősugárzási irányban, valamint a +/- 10°-os billentéses irányokban nagy pontossággal volt mérhető.

A modell mérések is alátámasztották, hogy a kicsinyített modellek mérése után bizonyos esetekben szükséges az 1:1 arányú modell vizsgálata is.

A végleges szerkezeti konstrukció ellenőrzésére a telephelyen kiépült egy 154 méter hosszú 1:1 arányú huzalokból kialakított kísérleti tápvonal szakasz is. Ezen a szakaszon mérések alapján vizsgálni lehetett a reflexió forrásokat és a kompenzálási lehetőségüket.

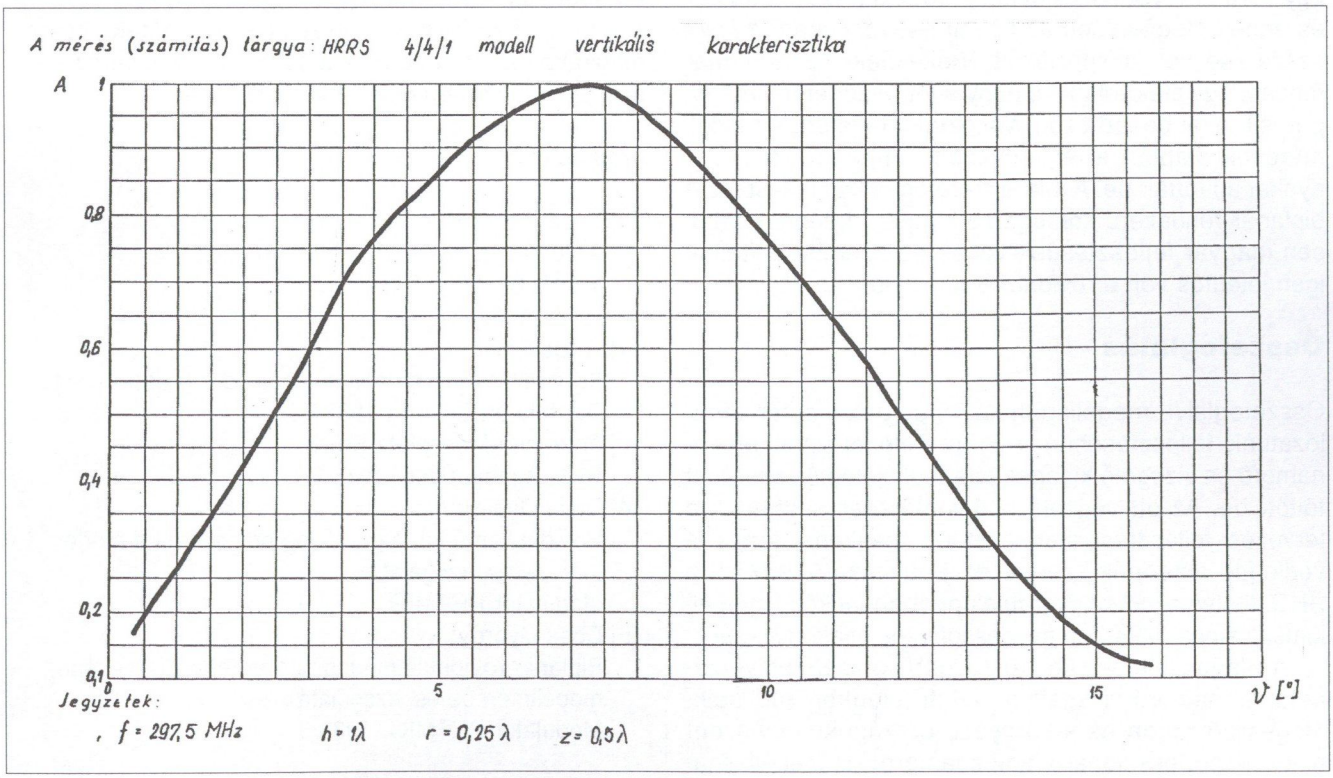
Ugyancsak a Bugyi-Telekpuszta-i telephelyen modellezték és vizsgálták a PRTMIG és a Híradótechnikai Vállalat (HTV) közötti fejlesztési szerződés alapján a postai rövidhullámú rádiókommunikációs és a rövidhullámú rádióműsorszóró szolgálat fejlesztése érdekében a csúcsával földre merőleges kialakítású log.per. síkú körsugárzó (KLP-71) és a biplanar kialakítású (TBLA-4/16) szintén körsugárzó log.per. antennarendszert, melyeket Székesfehérvár Rádióállomáson helyeztek üzembe 1979, illetve 1987-ben.

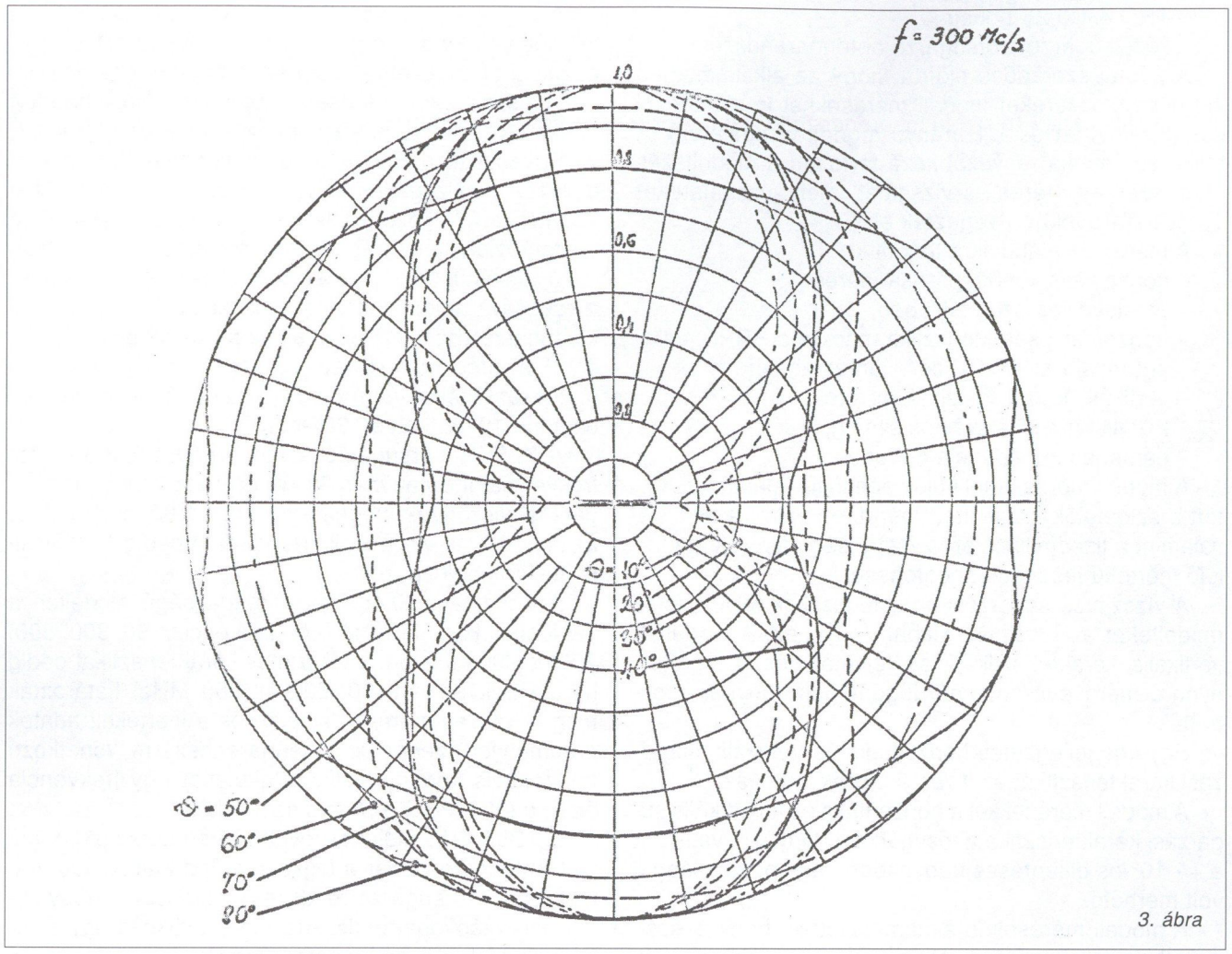
A KLP-71 körsugárzó antennarendszer 3-30 MHz frekvenciatartományban 30 kW teljesítményre adott sugárzási viszonyok meghatározására 1:30 kicsinyítésű, az impedancia viszonyok vizsgálatára pedig 1:10 kicsinyítésű modell készült.

A vizsgálatok 0,45 l max. magasságú modellen a két fősíkú karakterisztikát öt frekvencián 90, 300, 500, 700 és 900 MHz-en, a vízszintes karakterisztikát pedig három frekvencián (90, 300 és 900 MHz) határozták meg. A modell-mérések alapján és a kiértékelt adatok eredményei szerint az antennarendszerre vonatkozó horizontális karakterisztika alakulását egy frekvencia értékre (300 MHz) a *3.ábra* szemlélteti.

A TBLA 4/16 biplanar rövidhullámú körsugárzó log. per. antennarendszer a legkorszerűbb kialakítású, trapéz fogazású sugárzó rendszer sajátossága, hogy külön belső tápvonalrendszerre nincs szükség, így szerkezetileg jelentősen leegyszerűsödik.

2. ábra





3. ábra

Az impedancia viszonyok vizsgálatára ez esetben is egy 1:10 arányban kicsinyített modellt készített a HTV és ennek megfelelően az üzemi frekvenciatartománya tízszerese volt a specifikált értékeknek. Az antennamodellt úgy alakították ki, hogy a létraszöget (a két log. per. sík által bezárt szög) változtatni lehetett. A modell mérések alapján a legkedvezőbb impedancia viszonyokat állították be. A földre merőleges kialakítású és a biplanar rendszerű körsugárzó log.per. antennák teljesen magyar fejlesztésűek voltak és üzembe állításuk igen jelentős volt a rövidhullámú területen.

Összefoglalás

Összefoglalva megállapítható, hogy hazai antennahálózatunk fejlesztésében a Bugyi-Telekpuszta-i antennamérő és vizsgáló kísérleti telephely jelentős szerepet töltött be. Az ott végzett modell-mérések segítették a tervezési-fejlesztési munkákat és megkönnyítették a végleges antennák szerelését, beállítását. 1958-tól a BHG, illetve az EMV gyár tulajdonában működő mérőállomás sajnos 1994-ben gazdasági okok miatt megszűnt.

A világon jelenleg kb. 10-15 igen korszerű univerzális antennamérő-vizsgáló kísérleti telephely működik. Magyarországon és a környező országokban viszont nincsen professzionális antennamérő kísérleti-vizsgálati telephely. Hazai vonatkozásban pedig a lehetőség és adottság ma is meglenne egy ilyen alkalmazására, és így nemzetközi kooperációba, kutatás-fejlesztési munkákba is be lehetne kapcsolódni, és mint szellemi terméket, eredményeket értékesíteni lehetne.

Irodalom

[1] F. Landstorfer:
Antennen Messraum in Berech von
1 MHz bis 5000 MHz.
NTZ 1968/4.

[2] R. Becker:
Kurzwellen Richtantennen für Sender grosser Leistung
Telefunken Zeitung 1967.40.

[3] Antennen Messplatz Brück.
BRF Mitteilungen, 1958/9.

[4] Dósa György:
Rövidhullámú körsugárzó log.per. antenna modellmérése és vizsgálata.
Modulátor PRTMIG, 1977/9.

[5] Dósa György:
Biplanar rövidhullámú log.per. antenna tervezése, modellmérése és vizsgálata.
Modulátor PRTMIG, 1983/8.

Hírek

Az Oracle a Párizsban megrendezett **OracleWorld konferencián** ismertette azokat a felmérési eredményeket, amelyek első alkalommal nyújtanak részletes betekintést a szerverhardverek és a grid computing alkalmazását övező problémákba az európai vállalatok körében. A felmérés legmeghökkentőbb eredménye az volt, hogy a vállalatok több mint 50 százaléka egyáltalán nem lát bele abba, hogy milyen terhelés nehezedik technológiai infrastruktúrájukra. Azoknak, amelyek rendelkeznek némi betekintéssel, a szerverek összességében mintegy 60 százalékban vannak kihasználva. Ha a jelenlegi 60 százalékról a vállalati számítóhálózatoknak köszönhetően 90 százalékra növekedne a kihasználtság, az európai cégek évente 4,5 milliárd dollárt takaríthatnának meg szervervásárlásaiknál.

A felmérést 2003 augusztusa és szeptembere során a QNB Intelligence független elemző cég készítette. A válaszadók olyan európai vállalatok munkatársai voltak, akik a stratégiai fontosságú informatikai technológiák és megoldások tervezését, kiválasztását és bevezetését irányítják.

A szerverinfrastruktúra helyzetét tekintve figyelemre méltó, hogy ha egy rendszernél kapacitásgondok merülnek fel, a vállalatok 30 százaléka – vagyis közel egyharmada – egyszerűen azt a megoldást választja, hogy még több hardvert vásárol – pedig a kiszolgálók átlagos leterheltsége csupán 60 százalék. Ez azt jelenti, hogy a meglévő kihasználatlan kapacitással is feloldhatnák szűk keresztmetszeteiket. Pontosan ezt a problémát célozza meg az Oracle Grid Computing. A Gartner szerint az EMEA kiszolgálópiacán 2002 során 1,37 millió egységet adtak el 15 milliárd USA-dollár értékben. A 60 százalékos átlagos kihasználtság azt jelenti, hogy ezekből a kiszolgálókból több mint félmillió gyakorlatilag fölösleges többletkapacitást képvisel.

A tanulmány szerint a grid computing a „korai bevezetési" stádiumnál tart. A válaszadók közel fele gondolt már bevezetésére és nyilatkozott úgy, hogy a két fő terület, ahol a számítóhálózatok bevezetését megfontolná, a vállalati alkalmazások (integrált vállalatirányítási rendszerek és ügyfélkapcsolat-kezelés), valamint az adatbázis-kezelés. Azonban a vállalatok 45 százaléka úgy érzi, hogy a grid computing még legalább három évig nem válik fővonalbeli kereskedelmi alkamazássá.

A rendezvény ehhez kapcsolódó egyik fő témája az Oracle „Enterprise Grid Computing" elnevezésű számítóhálózatos technológia és az azt képviselő új 10g termékcsalád, amelynek tagjai az Oracle Database 10g adatbázis-kezelő, az Application Server 10g alkalmazáskiszolgáló és az Enterprise Manager 10g felügyeleti eszköz. Az Oracle a konferencián bemutatta az új konstrukciót is, amely megkönnyíti az egységek beágyazását a független szoftverszállítók (ISV-k) középvállalatok számára kifejlesztett megoldásaiba.

A **Siemens** bemutatta első, nagyközönségnek szánt harmadik generációs (3G) mobiltelefonját, az U15 névre keresztelt modellt. A néhány európai országban már működő UMTS-rendszerű hálózathoz kifejlesztett készülék videotelefonként működik, s nagy sebességgel képes filmek továbbítására is. Emellett a telefon rendelkezik valamennyi multimédiás funkcióval, így videofelvételt készíthetünk vele, kép- és videoüzeneteket küldhetünk és fogadhatunk, s a zenebarátoknak MP3 lejátszót is beépítettek.

A két beépített digitális VGA kamera segítségével a telefon fényképek és videofelvételek készítésére is alkalmas, s multimédiás funkciói segítségével filmeket és zenéket tölthetünk le. A videókat a 65 ezer szín visszaadására képes, 176x220 pixeles kijelzőn nézhetjük meg, s 64 Mb tárhely gondoskodik a fontos felvételek megőrzéséről.

WHERE IS THE DIVIDE?

The digital divide between those who have computer literacy and access to the Internet and those who haven't is a hot topic all over the world. This problem was highlighted at this year's World Telecom Exhibition and Forum.

A NEW COMMUNICATIONS ERA

This article outlines the development process of communications based on formal models typical of human communication, on elementary communication as well as on information system model. The calculated world cannot replace reality, it can just provide a limited model but may be useful for the understanding and forecast of the future. The second part of the article allows insight into the mathematical background.

THE ZIGBEE TECHNOLOGY

Wireless networks enabling network based connection between mobile devices are becoming more and more popular. Current wireless technologies focus on the highest available bandwidth and on the support of ad hoc networking. Minimizing energy consumption is a question of secondary importance. Networking technology trends suggest, however, that future network communications will use devices for which power supply is a critical factor. This article introduces the Zigbee technology developed for radio communications between such devices.

ON "FUZZY" IN GENERAL

Fuzzy is present in several aspects of our life. In the everyday life the word 'fuzzy' is used when one cannot decide if a device functions correctly or not, or, in connection with persons, one is uncertain in the definition of a feature. Though the fuzzy method is used in many areas, the majority of engineers disregards it as a way of calculation of a particular problem. It simply does not come on. The purpose of this article is to change this approach.

UNIFORM MOBILE TELECOMMUNICATIONS SERVICES FOR EUROPEAN RAILWAYS

In 1993 the International Railway Union made a resolution on the development of a public GSM-based unified railway communications standard which is ready for international co-operation. Since the introduction of the standard-based GSM-R system 32 European railway companies joined the project. The new technology establishes a joint, integrated platform for a high-quality deployment of different railway applications such as for the unified European train manipulation system.

THERE IS NO ROYAL WAY

ITU organizes quadrennial world fairs in Geneva hosting also Telecom Forum where outstanding persons of the industry hold lectures on current professional issues for six days. This year's event differed from the tradition in several aspects and the 9th World Telecom surprised attendants with many thought-provoking changes.
The International Telecommunication Union held its Exhibition and Forum between 12-18 October, 2003. For the first time in its history a Youth Forum was organized as well. Each ITU member state was allowed to delegate two young participants attending a university falling in the scope of activity of ITU. The author was one of the two who represented Hungary at the event.

XYSCOM

The integrated broadband telecommunications system described in this article is a network infrastructure providing advanced broadband telecommunications services for small regions. It offers residential and business access, the establishment of the community network and thereby the elimination of the telecommunications isolation of the given small region. In terms of services it can be used for the establishment of an independents telephone network. In addition to broadband internet-based services it is able to carry nationwide narrow band telephone and other value-added services as well.

HOW LONG TESTING SHOULD LAST?

With the use of modeling temporal changes of testing and expenditures with dynamic systems our authors try to find a solution for a typical problem of software projects: how long the testing should last so that a high-quality product can reach the market. The solution is preceded by an analysis to study the estimation probabilities of the stability and the parameters of the system. The viability of the method is then tested on realistic data.

ENCRYPTING HOMOMORPHISMS

The concept of encrypting homomorphisms was introduced in 1978 by Rivest, Adleman and Dertouzos, originally for the solution of problems in computing delegation. Typically this is the case when the owner of data has a limited computing capacity, i.e. the calculations to be performed are too complex or the high amount of data cannot be managed. In such cases data have to be transferred to a computer center which is able to perform the necessary calculations. If these are mission-critical data, it is obviously a question of concern.

LTRACK – A NEW WAY FOR MOBILITY MANAGEMENT

LTRACK stands for "location tracking" and designates a new mobility management method in which major mobility protocols solutions are specific ones but generally are more efficient in that its signaling traffic requirement is lower.

DRB IN LONG/MEDIUM/SHORT WAVE REGIONS

The shift from analog to digital technology is going to bring about revolutionary changes in radio broadcasting: the digital technology opens new horizon in the long/medium/short wave regions of amplitude-modulated transmission. Fading, interference and low sound quality have been disturbing factors in analog broadcasting for several decades, however, the DRM radio system, result of a five-year global development, is going to produce noise-free reception and FM quality sound even in long distance transmission and, what's more, in the current AM wave bands.

ON THE HISTORY OF THE ANTENNA TESTING SITE

After World War II the role and importance of radio broadcasting was increasing which was reflected in the growing number of emerging transmission equipment and antenna systems as well as in their power. In the early 50s leading communications companies, research firms and postal organs of certain countries set up antenna measuring and testing sites to promote a more efficient development and planning of antenna systems as well as their production in a more economic way.

Summaries • of the papers published in this issue

Contents

WHERE IS THE DIVIDE? (NOVEMBER) 1

IMPACT OF INFORMATION TECHNOLOGY ON OTHER FIELDS

András Benczúr
Computers and communications technology: a new communications era (Part II) 2

Balázs Kovács, Roland Vida
The Zigbee technology 9

Etelka Mészáros
On „fuzzy" in general 15

Dr. Géza Tarnai, Dr. Izabela Krbilová, Dr. Jiří Zahradník
Uniform mobile telecommunications services for European railways 18

ITU WORLD TELECOM 2003

Dr. György Lajtha
There is no royal way 23

Kornélia Kontor
World Telecom Youth Forum 28

Book review 30

Eisler Péter
Xyscom 31

QUALITY AND RELIABILITY OF CONNECTIONS

Gábor Stikkel, Gábor Szederkényi
How long testing should last? 36

Réka Limbek, Péter Sziklai
Encrypting homomorphisms 42

Sándor Imre, Máté Szalay
LTRACK – A new way for mobility management 49

PAST AND FUTURE OF RADIO BROADCASTING

Dr. Tamás Sárkány
Digital radio broadcasting in long/medium/short wave regions 53

Book review 57

György Dósa
On the history of the Hungarian antenna testing site 59

Cover: World seen from ITU tower

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

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

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

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

2004-es előfizetési díjak
Hazai közületi előfizetők részére:
1 évre bruttó 31.200 Ft
Hazai egyéni előfizetők részére:
1 évre bruttó 7.000 Ft

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

www.hte.hu
Felelős kiadó: MÁTÉ MÁRIA
Lapmenedzser: Dankó András

HU ISSN 0018-2028

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