híradástechnika

VOLUME XLIX.

1998/11-12

journal on
communications
computers
convergence
contents
companies

JOURNAL ON C[5]

A PUBLICATION OF THE SCIENTIFIC SOCIETY FOR TELECOMMUNICATIONS, HUNGARY

SPONSORED BY

Szerkesztőség / Editorial office
HÍRADÁSTECHNIKA
Budapest, VI. Paulay E. u. 56. II.14/A.
Telefon:(361) 341-6421, (361) 325-9058
Fax: (361) 341-6421, (361) 325-9058
Előfizetés / Orders to
HÍRADÁSTECHNIKA/TYPOTEX
H-1024 Budapest, Retek u. 33-35.
Tel./Fax: (361) 316-3759

1999-ES ELŐFIZETÉSI DíJAK
Hazai közületi előfizetők részére*
1 évre 20000 Ft +12% ÁFA = Btto 22400 Ft; Egyes számok 2000 Ft +12% ÁFA = Btto 2240 F
Hazai egyéni előfizetők részére*
1 évre 4000 Ft +12% ÁFA = Btto 4480 Ft; Egyes számok 400 Ft +12% ÁFA = Btto 448 Ft
HTE tag előfizetők részére*
1 évre 2000 Ft +12% ÁFA = Btto 2240 Ft; Egyes számok 200 Ft +12% ÁFA = Btto 224 Ft
Subscription rates for foreign subscribers
12 issues 100 USD, single copies 10 USD
Transfer should be made to the Hungarian Foreign Trade Bank
Budapest, 10300002-20321411-00003285
* 1999. február 28-ig 50% kevezmény

HÍRADÁSTECHNIKA, JOURNAL ON C[5] is published monthly, in English and in Hungarian by TypoTEX Ltd.
H-1024 Budapest, Retek u. 33-35. Phone/Fax: (361) 316-3759. Publisher: Zsuzsa Votisky.
Type-setting by TypoTEX Ltd. Printed by Dabasi Jegyzetnyomda. HU ISSN 0018-202

HÍRADÁSTECHNIKA

Vol. XLIX. No. 11-12, NOVEMBER-DECEMBER, 1998
HU ISSN 0018-2028

JOURNAL ON C5

50 years

from the Telecommunications Scientific Society

Abstract: In this issue 8 papers are presented. Section **Communications** is represented by 1 contribution on PSTN Real-Time Simulation. Section **Computers** is comprised of 2 contributions on Fractal Properties and on ISUP Conformance Testing. Section **Convergence** is formed by 2 contributions written on the Oligopol Market Analysis and on the Telecommunications Standardisation Strategy in Hungary. Section **Contents** and distribution of multimedia is containing 2 contributions on the RED Algorithm Testing and on the ATM Data Security Systems. Section **Companies** is now dealing with 1 contribution on the E-Mail Reader System from Technical University of Budapest. In this issue 7 submitted papers of the 8 ones are scientifically evaluated by 4 senior reviewers. One paper is not accepted only by the reviewers as scientific contribution. The others are marked by the sign of $\mathcal{L}$ giving evidence of their scientific nature.

THE RISING SUN

54 ÉV UTÁN

„Kettős jubileumot ünnepelhetünk; 1999. januárban indul lapunk, a Híradástechnika 50. évfolyama és 1999. januárban lesz 50. évfordulója Egyesületünk megalakulásának is. Lapunk tulajdonképpen már el is múlt 50 éves, mert első száma – még mint Magyar Híradástechnika – a Magyar Technika mellékleteként 1946. szeptemberében jelent meg. A Híradástechnika tehát e számának megjelenésekor már az 54. életévébe lép. Az első önálló szám kelte 1950. december 21. volt és ez a szám a IV. évfolyamnak nevezte magát. A lapengedélyt csak ebben az évben kértük, mert a mellékletekhez korábban lapengedély nem kellett és ezért a bürokrácia csak az I. évfolyam megjelöléshez járult hozzá. Az első három, ilyen módon illegális évfolyam még, mint a Magyar Mérnökök és Technikusok Szabad Szakszervezete Híradástechnikai Szakosztályának lapja jelent meg. Főszerkesztője Gerő István volt. A legális I. évfolyam 1. számát már a Híradástechnikai, Finommechanikai és Optikai Tudományos Egyesület adta ki, Lévai Pál főszerkesztő irányítása alatt. A lap ekkor elvileg kéthavonta jelent meg, de a cikkekkel való ellátás még így is akadozott; gyakoriak voltak a dupla számok. Híradástechnikai iparunk ebben az időben az újjáépítéssel volt elfoglalva, önálló fejlesztés alig volt, a magyar híradástechnikai tudományok pedig még gyerekcipőben jártak. A híradástechnikusokat szinte rá kellett venni egy-egy cikk megírására. A Híradástechnika cikkei időrendi sorrendben hűen tükrözik híradástechnikai iparunk és tudományunk történetét."

Dr. Izsák Miklós írta ezeket a ma is időszerű sorokat a lap 25.-ik évfordulójára, értelemszerűen 1974-ben. 50 év után pedig alig emlékszik valaki, hogy teljes három (az 1946, 47 és 48-as) évfolyam anyaga egyszerűen kimaradt a számozásból (1949-es évfolyam pedig nem is volt). Ezek az anyagok igazi hídépítő, megalapozó munkák és a szakma nagy öregjei készítették feltörekvő, ifjú korukban. Régen esedékes kárpótlásként ezek az "elfelejtett évek" – tisztelgően – 1999-ben újra megjelennek.

PLUG AND PLAY A NOÉ BÁRKÁJÁN

Mintegy fémjelezni lehetne szakmánk pillanatnyi helyzetét és meg lehetne mosolyogtatni az utókort a Noé bárkájára vihető mai értékekkel, hogy unokáink is lássák.

Mindenek előtt Nokia Communicatort és ISDN vezetékes szolgáltatást kellene a bárkára vinni, egy 300 MHz-es Pentium II notebookkal, AGP-s, Voodoo II-s gyorsítókkal. Ez lehet egy DVD-vel kiegészített, 128 Mbyte RAM-mal és 9 Gbyte HD-vel felfegyverzett Toshiba eszköz, PCMCIA kártyákkal. Egy hasonló kiépítésű Compaq desktop gép is elkelne a bárkán a Creative (AWE64 Gold) multimédia, a Yamaha CDR400t CD-író, az Adaptec SCCI támogatás és az AVM Fritz ISDN kártya integrált kezelésével. A géphez egy TI-89 kalkulátor is csatlakoztatható.

Programokat is vinni kellene; WIN98-as alatt futó Photoshop 5.0, Corel Draw 8.0 grafikus programokat és Office 97-et Norton AntiVirus 5.0 támogatással. Játszani is lehetne a Final Fantasy VII., ill. a ChessMaster 6000 használatával. A világ kultúrájának teljes anyagát az Encyclopedia Britannica 99 két CD-je biztosítaná. CD-nként mp3-ban tömörítve 12 óra zenei anyagot vihetnénk fel.

A bárkán ajánlható olvasnivaló a Serény-féle Albert Speer könyv és a Radzinszkij-féle Sztálin könyv, hogy soha el ne felejtődjön elődeink kettős csapdája, amely ellopta tőlük és egész Kelet-Európától a század felét.

Kiválasztott programozási nyelvként a Java2-t preferáljuk. Ez immáron az egyetlen Java Virtual Machine, ami egységes és kompatibilis környezetet jelent. A Noé bárkáján kivárható, amíg a „cyber-war" jelenleg folyó ütközetei eldőlnek. A túlélők majd maguk választanak egy Win2000 bázisú (kikapcsolom-bekapcsolom, hátha most majd megy típusú) világ és egy „napsütéses" Java/X-tone bázisú élet között, amely utóbbi már szolgáltató orientált és univerzális szolgáltatással biztosított mindenki számára.

AZ X-TONE VÍZIÓ

A Linux, ill. az Oracle software vonal, valamint a nem teljesen független Java irányzat, a Novell NetWare, a Windows 2000 (vagy az NT5), a 3Com Palm eszközei olyan piaci forgatagot képeznek, amelyhez képest a riói karnevál egy busójárás. Mindez belső családi viszálynak tűnhetne, ha nem minden esetben a Java2 korszakot fordító győzelme látszana kikerekedni. A Java2-vel stabil, vírus-védett, object-orientált, a smart-cardtól a szuper számítógépekig fel-le skálázható platform biztosítható minden (távközlési és Internet) fejlesztés számára. Hovatovább nincs alkalmazás és főleg távközléssel összefüggő programozási feladat a földön, ami a Java nyelv segítségével, Java applet generálásával ne volna menetből megoldható. És ami még soha nem történt meg a történelemben; a megírt programok eleve interoperábilisek bármilyen jelenlegi és új, érkező eszköz viszonylatában.

A Sun az X-tone koncepcióval gyakorlatilag minden (új és meglévő) távközlési operátort szövetségre hívott. Azt mondja, hogy ha a ház ég, akkor a különböző tárcsázási hangokat adó segélyszolgálatokat hívja mindenki és nem E-mail-t küld az NT-s számítógépén a vak világba, választ nem is remélve. A Sun szerint hamarosan minden, de minden alkalmazáshoz búgó hang és szolgáltató tartozik, amely megveszi az egyre többet tudó – bármiféle – eszközöket és szolgáltat. A rádiótelefon előfizető utáni hajigálása óta tudjuk, hogy a tökéletes ember-gép interface eszközöket akár ingyen is kaphatjuk, hogy a szolgáltató szolgáltatásai minél vonzóbbak legyenek.

Ma már minden józanul gondolkozó fejlesztő-alkalmazó számára világos, hogy a WINTEL/Internet Explorer trükkös és monopolisztikus térhódítása véget ért. Az AOL-Netscape-Sun szövetség győzött és a Java2 vonal ily módon visszakapta a Netscape Navigator browser igazi lehetőségeit. Ettől függetlenül, de közel egyidejűleg a Java2 immáron egyetlen, egységes és megújított platformot képvisel. Ezt jelenleg is közel 1 millió fejlesztő használja és az AOL 10 milliós nagyságrendben teríti – világszerte.

Mindazonáltal az alapvető támadó állítás az, hogy az 50 millió soros software és vírusvédett, 4000 üzemmódú szövegszerkesztő bázisán működő PC teljesen természetellenes, anakronisztikus. Ez majdnem olyan, mint „egy atomreaktor működtetése a pincében". A jövőt tehát a Java platform, az operátorok X-tone bázisú szolgáltatásai képezik, amelyhez a Jini software támogatás már minden plug-and-play típusú hálózati eszközhöz rendelkezésre áll.

Forrás: tele.com, February, 1999.

KÖZCÉLÚ KAPCSOLT TÁVBESZÉLŐ-HÁLÓZATOK (PSTN) VALÓS IDEJŰ SZIMULÁCIÓJA

KUMLI TAMÁS és FARKAS JÁNOS

TRAFFIC ANALYSIS AND NETWORK PERFORMANCE LABORATORY, ERICSSON KFT.
TAMAS.KUMLI@ETH.ERICSSON.SE; JANOS.FARKAS@ETH.ERICSSON.SE

Az Ericsson-nál kifejlesztésre került a PlasmaSIM rendszer, távközlő-hálózatok vizsgálatára alkalmas eszköz, amely a hálózati szimulációt analitikus módszerekkel együtt használja az adott hálózat kívánt jellemzőinek meghatározására. Az eszköz alkalmas a hálózat viselkedésének modellezésére és számos hálózati forgalommenedzsment beavatkozás vizsgálatára. Egy ilyen szimulátor birtokában felmerül az ötlet, hogy létesítsünk kapcsolatot a szimulátor és a valós hálózat között. Ha már van egy, a szimulátorban felépített modellünk, a megoldandó probléma a hálózati konfiguráció és az előfizetők által felajánlott forgalom jellemzőinek frissítése a központokból kinyert valós idejű adatok alapján. Ezt a kapcsolatot megvalósítva a menedzsmentnek hiteles információ áll rendelkezésére a hálózat működéséről. Ez azért hasznos, mert a menedzser megvizsgálhatja a lehetséges beavatkozások hatásait anélkül, hogy kárt okozna az igazi hálózatban. Ha a beavatkozások hatékonynak bizonyulnak, akkor végrehajthatók a valódi hálózatban. Megvizsgáltuk, milyen mérések állnak rendelkezésünkre és ezek közül melyik hasznos a modellépítés szempontjából. Felmértük hogyan lehet a szimulátorba leképezni az előfizetők forgalmi viselkedését a különböző mérések alapján. Ezeken felül megvizsgáltuk mit tehetünk ha a mért adatok egy része elvész.

1. BEVEZETÉS

Manapság a hálózati forgalommenedzsment egyre fontosabb szerepet játszik a távközlés világában. Ennek legfőbb oka, hogy a jól működő menedzsment a legmegfelelőbb eszköz a már létező távközlési hálózatok hatékony üzemeltetésére, szolgáltatásai színvonalának javítására. A hálózati forgalommenedzsment alkalmasan választott beavatkozásai bizonyos határokon belül például az előfizetők számának megnövekedésével járó problémákat is megoldhatja, természetesen nem végleges megoldásként. A hálózati forgalommenedzsmenttel szemben támasztott követelmények miatt egyre fontosabb a szimulációs módszereken alapuló számítógépes eszközök alkalmazása.

2. A PLASMASIM

A PlasmaSIM az Ericsson-nál kifejlesztett hálózat analizáló eszköz PSTN hálózatokra. Az eszköz a hálózati szimulácót ötvözi analitikus eljárásokkal és optimalizáló módszerekkel. Annak ellenére, hogy a PSTN hálózatok, illetve az ezek forgalmát leíró matematikai formulák régóta ismertek, egy ilyen hálózat megtervezése, illetve hatékonyságának kiértékelése nagyon bonyolult feladat, sok esetben heurisztikus lépéseket is tartalmaz. Nagy hálózatoknál a probléma egyre összetettebbé válik. A helyzetet tovább nehezíti, hogy a mai modern PSTN hálózatokban számtalan olyan hatást figyelhetünk meg, amelyeket már nem lehet az Erlang modellel leírni (dinamikus útvonalválasztás, intelligens hálózati funkciók). Ezen okok inspirálták az Ericsson Traffic Analysis and Network Performance Laboratory-ját, hogy kifejlessze a PlasmaSIM-et.

A hagyományos hálózati forgalommenedzsment rendszerek a hálózat állapotáról nagymennyiségű adatot szolgáltatnak, ezeket gyakran grafikus formában. Lehetővé teszik, hogy a szakemberek könnyen reagálhassanak a hálózatban bekövetkezett változásokra, de csak ritkán támogatják a helyes beavatkozások kiválasztását. A PlasmaSIM a hálózati szimuláció és az analitikus módszerek egy rendszerbe integrálásával egy hatékony eszköz, egy olyan döntéstámogató rendszer, amely a hagyományos feladatokon túlmenően nagymértékben megkönnyíti az optimális NTM (Network Traffic Management: hálózati forgalommenedzsment) beavatkozások megtalálását. A megoldás nem a szimuláció és az algoritmusok egyszerű kombinációját jelenti. A PlasmaSIM ezeket a módszereket egy olyan egységes rendszerbe integrálja amelyben a szimulációs, illetve algoritmikus eredmények bemeneti adatokat szolgáltatnak egymás számára.

3. MENEDZSMENT ESZKÖZÖK

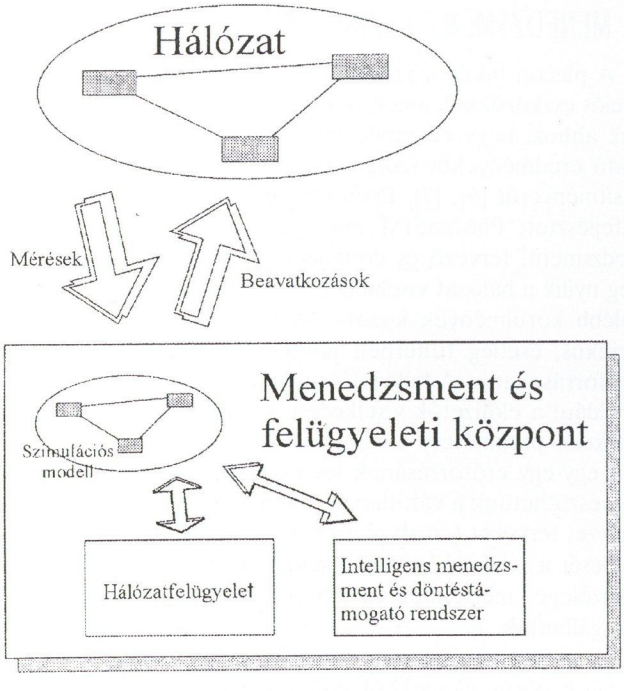
A piacon találkozhatunk olyan hálózat analizáló szimulációs eszközökkel, amelyek már elég robusztusak és fejlettek ahhoz, hogy elegendő információ birtokában megbízható eredményeket szolgáltassanak egy adott hálózat teljesítményéről [6], [7]. Ilyen eszköz például az Ericssonnál kifejlesztett PlasmaSIM intelligens hálózati forgalommenedzsment, tervező és döntéstámogató rendszer. Lehetőség nyílik a hálózat viselkedésének vizsgálatára a legkülönfélébb körülmények között. Meghatározhatjuk a hálózat kritikus, esetleg túlterhelt pontjait vagy a kihasználatlan erőforrásokat is. A hálózati modell egy-egy paraméterének (például a előfizetők viselkedésére vagy a topológiára vonatkozó paraméter) módosításával szimulálhatjuk a hálózat egy-egy erőforrásának kiesését, és ennek segítségével felkészülhetünk a váratlan eseményekre; úgynevezett vészhelyzet terveket (crash plan) készíthetünk. A hálózat viselkedését a modell részletességétől függően tulajdonképpen tetszőleges mértékben és tetszőleges körülmények között vizsgálhatjuk.

Ugyanakkor a jelenleg üzemelő korszerű távközlési hálózatok olyan elemekből épülnek fel, amelyek igen komoly lehetőségeket kínálnak a hálózati forgalommenedzserek számára. A jelenlegi PSTN (PSTN: Public Switched Telephone Network – nyilvános távbeszélő hálózat) hálózatokban főleg olyan digitális, tárolt-program-vezérlésű központok vannak, amelyek forgalommenedzsment lehetőségei nagyrészt kihasználatlanok. Ennek legfőbb oka az,

hogy ezen hálózatok nagy kiterjedésű, bonyolult, algoritmikusan nehezen számítható rendszerek. A hálózatokban rengeteg lokális érvényességű adat van, az egyes központok igen kevés információval rendelkeznek a hálózat egy távoli pontjáról, ezért igen nehéz átlátni egy ilyen hálózat viselkedését. Egy váratlan helyzetben (túlterhelés, központ vagy áramkörcsoport kiesése esetén) igen bonyolult feladat megtalálni a megfelelő beavatkozási módot. Ilyen helyzetekben előfordul, hogy a szakemberek nem avatkoznak be, félve az esetleges előre nem látható kedvezőtlen hatásoktól, pedig a megfelelő forgalommenedzsment eszközök alkalmazásával számottevő nyereséget lehetne elérni, illetve a veszteséget csökkenteni, vagy a szolgáltatás színvonalát javítani. Ezért vált szükségessé a hálózatmenedzserek számítógépes döntéstámogatása.

4. VALÓS IDEJŰ SZIMULÁCIÓ

Az off-line jellegű szimulációra épülő módszer hátránya az, hogy a valóságban előforduló események száma nagyon nagy, ezek mindegyikét szimulálni nem lehet. Off-line a szimuláció ha a hálózat modellje, vagyis a szimulációs hálózat nincs közvetlen összeköttetésben a valós hálózattal csupán annak egy leképezése egy adott állapotra nézve. Egy ilyen rendszert alkalmazva készíthetünk tervet például egy adott központ kiesésére vonatkozóan, de valószínű, hogy más- más beavatkozásra van szükség, ha a központ egy lokális túlterhelés, globális túlterhelés, vagy esetleg más műszaki hiba miatt állt le. Más beavatkozásra van szükség a forgalmas órát tekintve, másra korán reggel. A beavatkozásra nagy hatással lehet a hálózat többi, esetleg távoli pontjának állapota is.



1. ábra.

A problémára jó megoldás lenne, ha a hálózat analizáló eszközt közvetlen kapcsolatba hoznánk a valós hálózattal. Egy olyan rendszert kell építeni, amely a hálózat analizáló eszköz számára a hálózat összes pontjáról a szükséges információkat valós időben összegyűjti. Egy ilyen rendszer megalkotásával tulajdonképpen átfogó képet kaphatunk a hálózat aktuális állapotáról, hiszen egy központi helyen rendelkezésünkre állnak az egész hálózatra vonatkozó szükséges információk. Ugyanakkor a valós idejű adatgyűjtés bemeneti adatot szolgáltathat a hálózat analizáló rendszer számára, így például a PlasmaSIM döntéstámogató rendszer segítségével megvan a lehetőség, hogy vészhelyzetben azonnal és a megfelelő módon avatkozzunk be. A szimulációs módszereket kihasználva, még a beavatkozások előtt megfigyelhetjük azok hatásait, így nagymértékben csökkenthetjük a kockázatot, sőt többféle beavatkozás közül könnyen és gyorsan kiválaszthatjuk a legmegfelelőbbet.

A valós idejű adatgyűjtésen alapuló hálózati forgalommenedzsmentet tehát az 1. ábra szerint képzeljük el.

Egy központi helyen megtalálható a hálózat egy on-line, interaktív modellje. Ez a modell – úgymond követő hálózat – on-line olyan értelemben, hogy a hálózatban végzett valós idejű mérések alapján mindig annak aktuális állapotát tükrözi, valamint interaktív olyan értelemben, hogy a hálózati forgalommenedzsment beavatkozásokat a modell segítségével véghezvihetjük.

5. A VALÓS IDEJŰ ADATGYŰJTÉS JELLEMZŐI

Ha megvizsgáljuk a valós idejű adatgyűjtés lehetőségét a nyilvános kapcsolt távbeszélő-hálózatokban, akkor a következő főbb jellemzőket figyelhetjük meg:

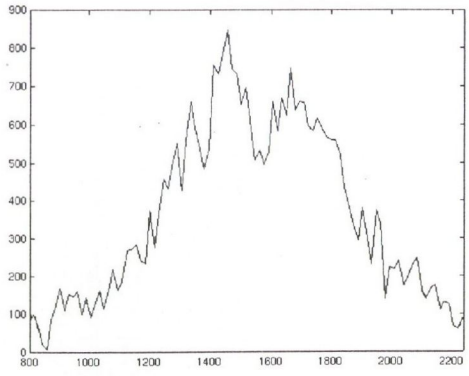
1. A hálózatban alkalmazott eszközök (kapcsolóközpontok, áramkörcsoportok) kapacitása valamint teljesítménye, a hálózat topológiája, az útvonalválasztási stratégia és más hasonló jellemzők általában nem változnak. Ezen paramétereket a modell megalkotásakor vesszük figyelembe, karbantartásuk valós idejű adatgyűjtést nem igényel. Méréseket az előfizetők által felajánlott forgalomra kell végezni. A tényleges feladatot tehát az előfizetők állapotának (a felajánlott forgalomra vonatkozó paraméterek) nyomon követése jelenti. A hálózat egy-egy erőforrásának kiesésének detektálásával nem foglalkozunk, hanem annak meghatározásával, hogy hogyan kell beavatkozni az adott körülmények között ahhoz, hogy a legkedvezőbb hatást érjük el. Ehhez az szükséges, hogy a hálózatban szereplő előfizetők pillanatnyi viselkedéséről pontos képünk legyen.

2. Az előfizetők viselkedéséről elmondható, hogy az általuk generált forgalom viszonylag lassan, egy napi profil szerint változik. A 2. ábrán egy központban egy adott cél irányába kezdeményezett hívások számának változását figyelhetjük meg az idő függvényében. A hívások száma egy egész napot véve egy jellegzetes M alakú görbét ír le.

A folyamatról számos statisztika áll rendelkezésre, a görbétől általában csak akkor tapasztalunk nagy eltérést, ha valamilyen váratlan esemény történik.

3. A központokban a méréseket viszonylag hosszú intervallummal érdemes végezni, különben a mérési eredmény nem lesz megbízható annak nagy szórása miatt.

A módszer nehézsége abban áll, hogy nehéz összegyűjteni a hálózatra vonatkozó kellő mennyiségű információt. A hálózat felügyeleti, mérési funkciói a központokban vannak implementálva, így az információgyűjtés gyakorlatilag az ott található adatbázisok lekérdezését jelenti bizonyos időközönként.



2. ábra. Egy üzleti telefonbeszélgetés hívásintenzitásának napi eloszlása

A rövid mérési periódus általában nagy fluktuációt eredményez a mérési eredményekben, hiszen a hálózatban előforduló, véletlentől függő eseményekből kevés minta áll rendelkezésre, ugyanakkor sűrűn kell az adatokat átvinni ami nagy sávszélességet igényel az adatok továbbításához. Túl hosszú mérési periódus esetén a szimulációs modell lassan reagál a valós hálózatban történő változásokra.

5.1. A mérési intervallum

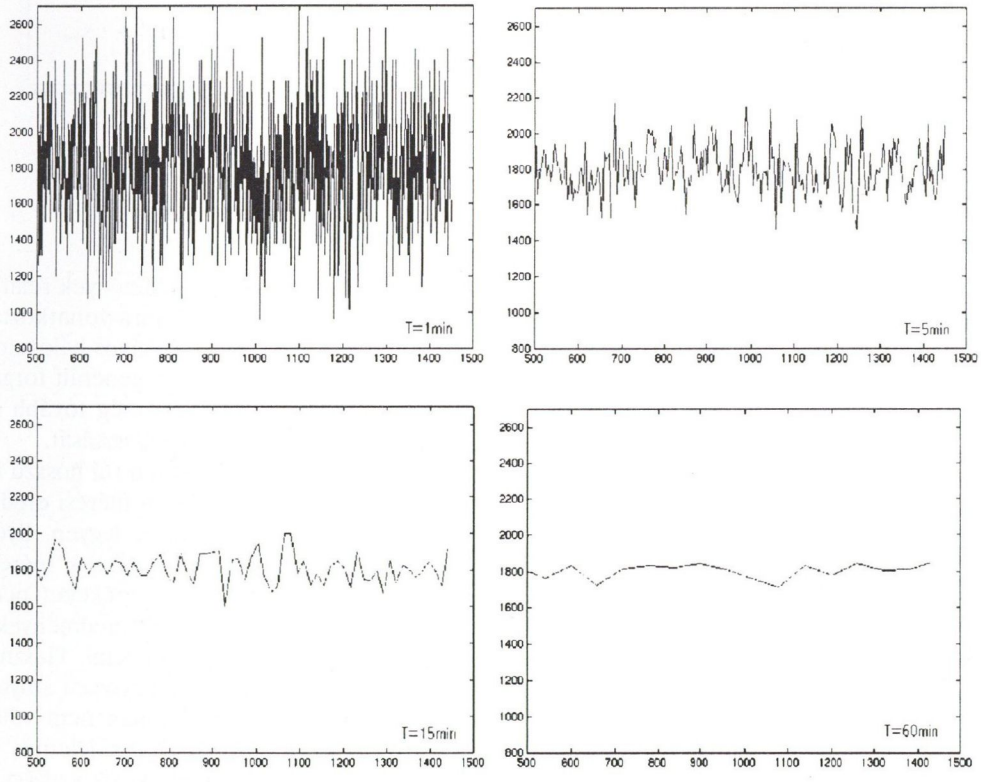
A felhasználói csoportok által generált forgalmat gyakran Poisson folyamattal modellezik. Egy λ paraméterű Poisson eloszlású valószínűségi változó várható értéke és szórásnégyzete is λ, ezért a relatív szórásra a következő összefüggést kapjuk: $\sigma_r = \frac{\sigma}{m} = \frac{1}{\sqrt{\lambda}}$.

Tehát minél nagyobb a valószínűségi változó várható értéke, annál kisebb annak relatív szórása. Ha egy forgalomforrás időegység alatt λ hívást kezdeményez, akkor t idő alatt a forrás által generált hívások száma λt paraméterű Poisson eloszlású valószínűségi változóval jellemezhető. A mérési intervallumtól és a hívásintenzitástól a relatív szórás tehát négyzetgyökösen függ.

A gyakorlatban ez azt jelenti, hogy a mérési intervallumot elég nagyra kell állítani ahhoz, hogy a mért eredmények nagy valószínűséggel a várható érték közelébe essenek. Az intervallum optimális megválasztásánál figyelembe kell venni, hogy túl hosszú mérési intervallum esetén az eredménybe beleszámítanak olyan mérési értékek is amelyek hosszú idővel ezelőtt történtek, tehát a rendszer lassan reagál a hálózatban előforduló változásokra, így a szimulációs modell egy állandó, esetleg túl nagy késéssel követi a valóságos hálózat változását. Az is előfordulhat, hogy a nagyon gyors változásokat észre sem veszi.

A 3. ábrán a grafikonok ugyanazon $\lambda = 0,5 \frac{\text{hívás}}{\text{mp}} = 1800 \frac{\text{hívás}}{\text{óra}}$ intenzitású forgalomforrásra vonatkoznak különböző mérési intervallumok esetén.

Az ábrákon jól megfigyelhető, hogyan csökken a mérési eredmények szórása a mérési intervallum növelésével.



3. ábra

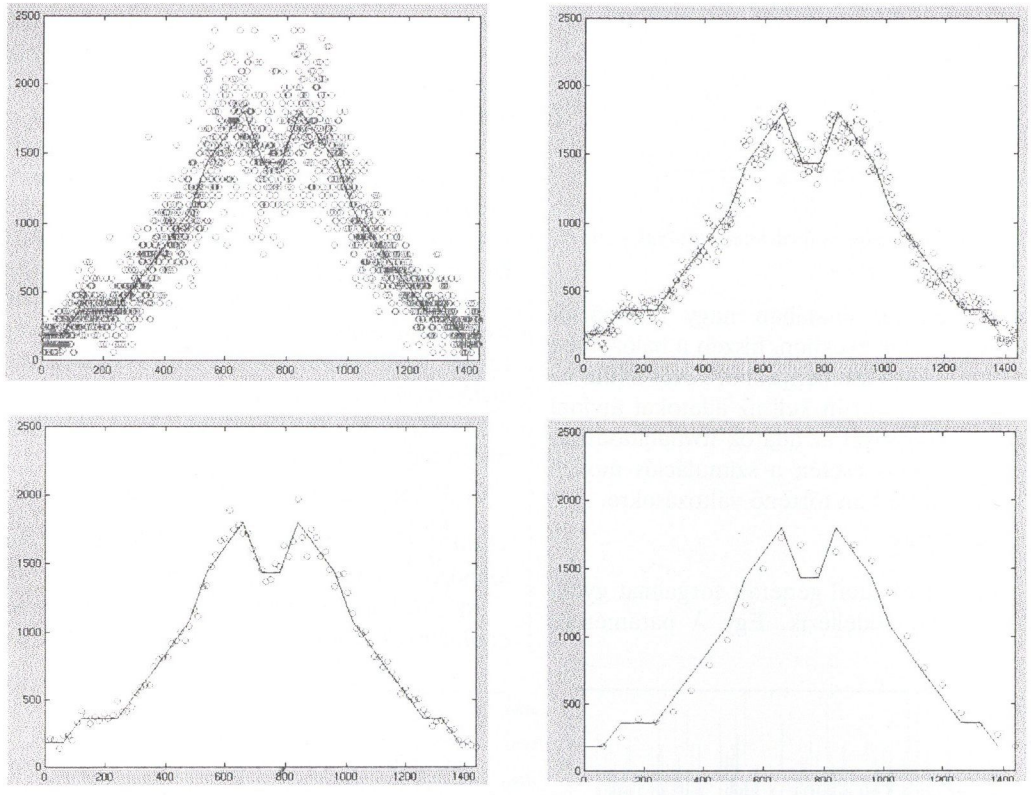
Az egyes esetekhez tartozó szórásparaméterek:

Mérési interv: T [perc]	Szórás: s
1	320
5	145
15	81
60	50

A 4. ábrán a grafikonok azt az esetet mutatják, amikor a hívásintenzitás változik a már említett M alakú görbe szerint. A hosszú távú statisztikák alapján kapott napi profilt folytonos vonal, míg a mérési eredményeket karikák jelölik.

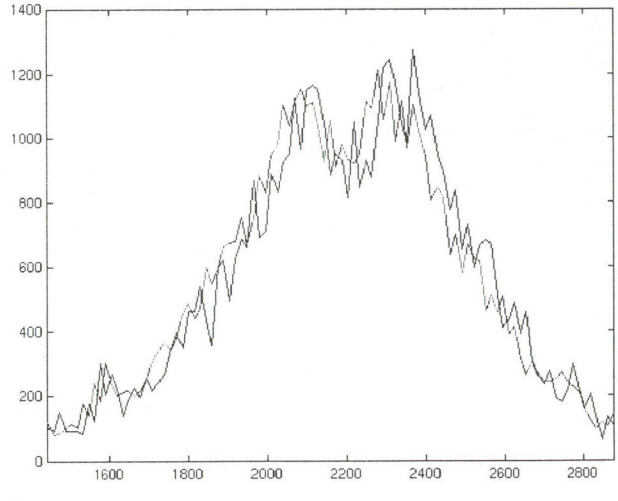
Főleg az utolsó ábrán figyelhető meg a mérési intervallum hosszának hatása. $T = 60$ perc esetén a modell hálózat egy órás késéssel követi a valós hálózat változását.

A felajánlott forgalom mértékének lassú változása lehetővé teszi, hogy PSTN hálózatokban 15 perces vagy akár órás mérési intervallumot válasszunk. Nagyon hosszú mérési intervallum esetén azonban gondoskodni kell arról, hogy a hálózatban bekövetkező hirtelen változások esetén a követő hálózat gyorsan reagáljon a változásokra. Ezt megtehetjük például extra mérések beiktatásával.



4. ábra

Az 5. ábrán a hálózat egyik áramkörcsoportjára vonatkozó mérési eredményeket láthatjuk negyedórás mérési intervallum esetén. Az óránkénti hívások számát figyelhetjük meg az idő függvényében. A világos görbe mutatja a valós hálózatból származó eredményeket, a sötét pedig a követő hálózatban szimulált értékeket.

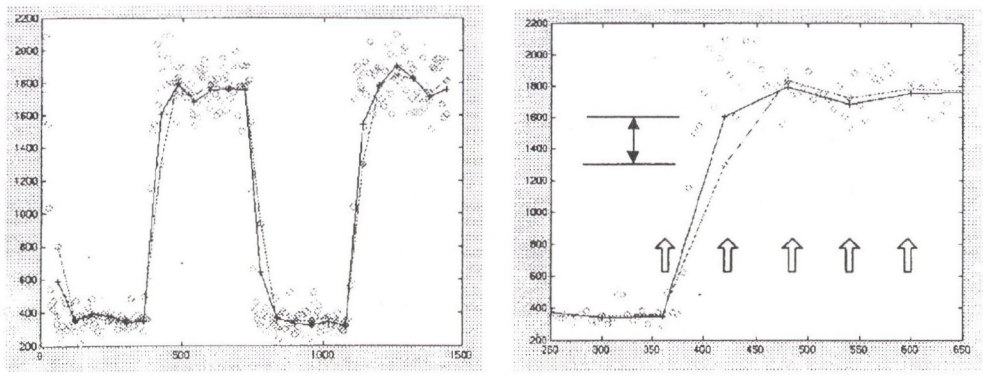


5. ábra

5.2. További lehetőségek

Azt láttuk, hogy a mérési eredmények relatív szórását az értékeknek a mérési intervallumra vonatkoztatott várható értéke határozza meg. Egy valóságos hálózatot tekintve az egyes források intenzitása, így a generált forgalom várható értéke nagyon eltérő lehet. Ez még tovább nehezítheti a helyes mérési intervallum megválasztását.

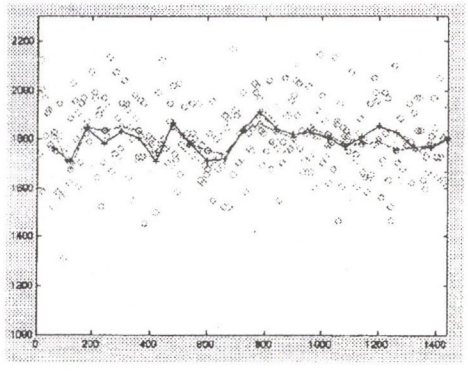
Alacsony hívásintenzitás esetén túl hosszú intervallumot kellene választani ahhoz, hogy a mérési eredmények relatív szórása megfelelően alacsony legyen. Ilyenkor megtehetjük, hogy visszamenőleg ugyan sok mérési eredményt veszünk figyelembe, viszont az értékeket nem egyformán súlyozzuk. Célszerű a legfrissebb eredményekhez a korábbiaknál nagyobb súlyfaktort rendelni. Használhatunk különböző csúszóátlagolást vagy egyszerű súlyozást is. Ha a forgalom a vizsgált intervallumban nem változik jelentősen, akkor a súlyozás nem játszik jelentős szerepet. Ha azonban hirtelen változás mutatkozik a vizsgált intervallum folyamán, és a későbbi értékeket nagyobb súllyal vesszük figyelembe, akkor a rendszer várhatóan gyorsabban reagál a változásokra. Ezt a jelenséget szemlélteti a 6. ábra. Képzeljük el, hogy a forgalom intenzitása váltakozva hol nagyon alacsony, hol nagyon magas. (A b) ábra az a) ábra egy kinagyított részletét mutatja.)



6. ábra

Az ábrákon karikák jelölik a mérési eredményeket, világos vonal jelöli az egyszerű átlagolással kapott órás eredményeket, sötét jelöli a súlyozott átlagolással kapott eredményeket. A kinagyított ábrán látható, hogy a sötét görbe a változást követő első mérési eredményben mennyivel jobban tükrözi a valós hálózatban bekövetkezett eseményt, tehát gyorsabban reagál a hirtelen forgalomnövekedésre mint a világos. (Az ábrán külön jelöltük az órás mérési periódusok végét.)

Ha megvizsgáljuk, hogy hogyan viselkedik a két módszer abban az esetben, amikor a felajánlott forgalom időben állandó, azt tapasztaljuk, hogy a sötét görbe jobban fluktuál. A mért értékek alapján a sötét görbére vonatkozó szórás az eredeti 50-ről 62-ra növekedett (7. ábra).



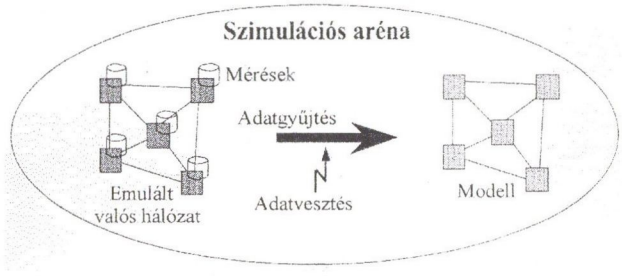
7.ábra

A jelenség azért tanulságos, mert látható, hogy megfelelő súlyozást használva elérhető, hogy az egyes forrásokra vonatkozó mérések relatív szórásai közel egyezőek legyenek.

6. A VIZSGÁLATI MÓDSZER

Célunk a valós idejű adatgyűjtés szimulációs vizsgálata. Konkrét, valódi hálózat híján a valós hálózatot emuláljuk. Az emulált hálózat teljes egészében a valós hálózat szerepét tölti be vizsgálataink során, innen származnak a szimulált mérési eredmények, az esetleges váratlan helyzeteket, túlterheléseket ebben állítjuk be stb. Ebben a hálózatban a valós hálózat egy igen részletes, pontos modelljét használjuk.

Egy másik szimulátorban megvalósítottuk a valós hálózat egy másik modelljét az úgynevezett követő hálózatot, amint az a 8. ábrán látható. Ez a modell hálózat bizonyos esetekben lehet teljesen azonos az emulált hálózatnál alkalmazott modellel, de lehet egy annál elnagyoltabbat is alkalmazni, attól függően, hogy milyen mélységű vizsgálatokat szeretnénk végezni. A követő hálózat áll a hálózati forgalommenedzsment rendelkezésére. A két szimulátor közötti kapcsolat létrehozása után lehetővé válik a felmerülő problémák, lehetőségek vizsgálata.



8. ábra

Szimuláljuk az on-line méréseken alapuló adatgyűjtéseket, az esetleges adatvesztéseket stb. Az adatok összegyűjtése és feldolgozása után a modell hálózat paramétereit állítjuk be az eredményeknek megfelelően. Az emulált, illetve a párhuzamosan működő modell hálózatra vonatkozó mérésekkel vizsgálható a módszer hatékonysága különböző körülmények között.

Modellünkben fontos szerep jut az úgynevezett forgalomforrásoknak, amelyek a hívások egy csoportját írják le, meghatározott forrásközponttal és célközponttal rendelkeznek. A felajánlott hívások a forrásközpontban jelentkeznek igényként, a hívott fél a célközpontban található.

7. A KAPCSOLAT MEGVALÓSÍTÁSA

A kapcsolatot tulajdonképpen a megfelelő mérési adatok, illetve az ebből származtatott adatok követő hálózatba való áttöltésével valósíthatjuk meg. Felmerül a kérdés, hogy milyen méréseket végezhetünk PSTN hálózatokon, ezek közül melyik használható közvetlenül vagy esetleges továbbfeldolgozás után.

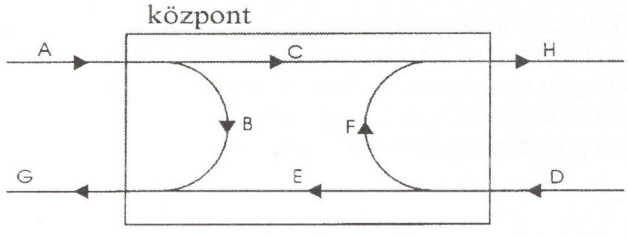
7.1. PSTN hálózatokon végezhető mérések

A központokban igen sokféle mérés áll a rendelkezésre, ezek közül kell kiválasztani egy megfelelő halmazt a következő szempontok figyelembevételével:

- Az általunk használt modell.
- A mérések során összegyűlő adathalmaz mérete. A mérési eredményeket valamilyen időközönként le kell tölteni a szimulátorba, így törekedni kell arra, hogy az adott mélységű modellhez elegendő minél kevesebb mérést végezzük csak el, így csökkentsük az időközönként átviendő adatmennyiség méretét.
- Ténylegesen milyen mérések állnak rendelkezésre a valós központban.

A digitális központokban rendelkezésre álló mérésekről szól az ITU-T Q544-es ajánlás [4]. Vizsgálataink fókuszában a forgalomra vonatkozó mérések állnak.

Egy központban a forgalmat a következő kategóriákra lehet bontani (9. ábra).



9. ábra. A központban előforduló hívások kategóriák szerint

A – helyben generálódó forgalom
B – belső forgalom
C – helyben generálódó, kimenő forgalom
D – bejövő forgalom
E – bejövő, helyben végződő forgalom
F – átmenő forgalom
G – helyben végződő forgalom
H – kimenő forgalom

Az ajánlás kitér arra, hogy milyen típusú méréseket érdemes definiálni a központban található különböző kategóriájú forgalmakat tekintve, a központok közötti áramkörcsoportokra, az előfizetői vonalakra stb.

Az ajánlás külön kitér a forgalommenedzsment számára fontos mérésekre és adatokra. A menedzsment számára rendkívül fontos, hogy a méréseket különböző célkódok szerint el lehessen végezni, hiszen így adott a lehetőség, hogy a hálózat más-más részét érintő hívásokat különböző módon kezeljük. Az egyes központokban ezért különböző célkódokat (destination code, traffic destination, TRD) lehet definiálni. A célkódok ország-, körzet- és központkódokkal, illetve ezek kombinációjával adhatók meg. Az egyes célkódok szerinti méréseket a kimenő forgalomra lehet elvégezni.

Modellünket figyelembe véve, a forgalomforrásokra vonatkozó paraméterek meghatározásához legjobb lenne, ha

- a helyben generálódó, kimenő forgalomra,
- célkód szerint lebontva

tudnánk méréseket végezni. Ekkor gyakorlatilag a forgalomforrások paramétereire közvetlen méréseket végezhetnénk.

Az ajánlás nem definiál méréseket a helyben keletkező kimenő forgalmi kategóriára. Az ilyen mérések megléte gyártó-, implementációfüggő. A tapasztalat azt mutatja, hogy általában elég körülményes dolog ilyen jellegű méréseket végezni, fel kell készülni, hogy a szükséges paramétereket több, egyszerűbben elvégezhető mérésből határozzuk meg. Fontos szempont még, hogy a mérések is azt a processzort terhelik, amelynek elsődleges feladata a hívások lebonyolítása.

A 9. ábrát tekintve könnyen beláthatjuk, hogy a helyben keletkező kimenő kategóriára vonatkozó számos mérési eredmény – például a felajánlott forgalom vagy a felajánlott hívások száma – könnyen meghatározható a többi kategóriára vonatkozó mérési eredmények ismeretében, hiszen ezen eredmények additív jellegűek. Számos más mennyiséget tekintve (átlagos tartásidő, sikeres hívások aránya stb.) azonban csak közelítő becsléseket adhatunk, hiszen a pontos eredmény kiszámításához csak azokat a hívásokat szabadna figyelembe venni amelyek ténylegesen az adott kategóriához tartoznak.

A központokban definiált mérések egy része alapadatokra, egy része az ezekből származtatott adatokra vonatkozik. A tapasztalatok szerint az alapadatokra vonatkozó mérések sokkal megbízhatóbbak, számítási célra jobban felhasználhatóak mint a többi, származtatott, számított adat. Valós idejű szimuláció esetén ezen szempontokat is figyelembe kell venni.

7.2. A modell paramétereinek számítása

A modell szempontjából leggyorsabb közvetlenül a forgalomforrások paramétereire vonatkozó méréseket végezni TRD (Traffic Destination, célkód) szerint szétválogatva. Ez a valóságban nem túl egyszerű feladat, hiszen a méréseket általában áramkörcsoportokon (kimenő linkeken, bemenő linkeken) vagy különböző kategóriájú hívásokon (átmenő, kimenő hívások stb.) végezhetjük. Egy adott célközpont felé igyekvő hívások általában több kimenő linken is megjelenhetnek, az adott kimenő linken figyelembe vett hívás lehet, hogy helyben generálódott, lehet, hogy egy bejövő linken érkezett.

Előfordulhat tehát, hogy a modell beállításához szükséges adatokat nem közvetlen mérési eredményekből kapjuk, hanem a hálózat több, esetleg távoli pontjáról származó mérési értékből számítjuk azokat.

Lehetséges a központokban több egyszerűbb mérés alapján következtetni a forgalomforrások által kezdeményezett hívások számára. Tegyük fel, hogy egy adott központban nem tudunk közvetlenül a forgalomforrások paramétereire méréseket végezni, viszont a központban a kimenő forgalomra vonatkozólag rendelkezésre áll a felajánlott hívások száma (BH: Bids per Hour – erőforrás-lefoglalás megkísérlése óránként) TRD szerint lebontva.

Azt természetesen nem tudjuk, hogy a kimenő forgalomnál számításba vett hívások helyben generálódtak vagy nem. Ámbár ha ismerjük a hívások útvonal-irányítását valamint az áramkörök blokkoltságát akkor alkalmas egyenletrendszert írhatunk fel, melynek megoldása a kívánt paramétereket adja. A következőkben ezt tárgyaljuk.

JELÖLÉSEK

Jelölje S a hálózat központjaiból alkotott forrás-cél párokból álló halmazt:

$$S = \{AB; AC; AD; ....BA; BC; BD; ...; ...\}$$

A halmaz elemei a forrás-cél párokon túl jelölhetik az adott forrásközpont és célközpont között húzódó áramkörcsoportot is (iránnyal együtt), ha van ilyen. Fontos az irány szerinti megkülönböztetés, hiszen az áramkörcsoporton végezhető mérések (pl. blokkolás) irányfüggő. Jelölje I_j $(j \in S)$ a j forrás-cél párral rendelkező forgalomforrás által kezdeményezett hívások intenzitását. Ezek az ismeretlen paraméterek amiket meg kell határozni. Ha n darab központunk van, akkor az ismeretlenek száma $n*(n-1)$.

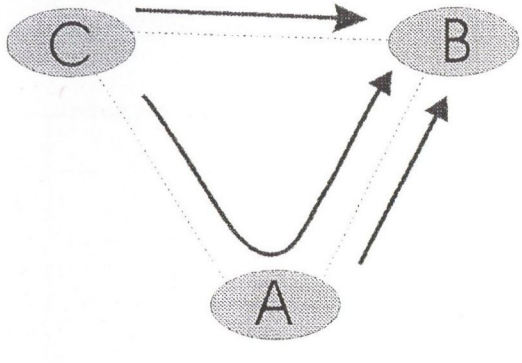
Jelölje N_j $(j \in S)$ a j-ben szereplő forrásközpontban mért, j-ben szereplő célközpont felé tartó hívások intenzitását. Ez tartalmazza az átmenő forgalmat is. Ilyen méréseket végzünk a valós hálózatban.

Jelölje B_j $(j \in S)$ a j-vel definiált forrás-cél között húzódó áramkörcsoporton az elfogadott és az összes hívás arányát (1 – blokkoltságát). Ha az áramkörcsoportnak felajánlott forgalomhoz tartozó intenzitás I, akkor a lebonyolított forgalomhoz körülbelül $B_j * I$ intenzitás fog tartani. A B_j értékeket mérjük a valós hálózatban.

Jelölje $R_{j,k}$ $(j \in S,\ k \in S)$ azt az arányt, amely az I_j forgalomból (felajánlott hívások számából) megjelenik a k linken. Ha például az AB forgalomforrás 100 hívást generál és ebből 25 jelenik meg felajánlott hívásként a CB linken akkor $R_{\mathrm{AB,CB}} = 0.25$.

Egyparaméteres forgalommodellel élve a hálózat áramkörcsoportjainak blokkoltsága valamint az alkalmazott útvonalválasztás egyértelműen meghatározza, hogy egy adott I_j forgalom hány százaléka jelenik meg felajánlott forgalomként az egyes linkeken. A felajánlott hívások számát tekintve hasonló a helyzet. Tehát az útvonalválasztást, illetve a linkeken a B_j értékeket ismerve az $R_{j,k}$ értékek meghatározhatók. Ha például a hálózat aktuális állapotában nincs blokkolás, minden hívás az első alternatíván közelíti meg a célközpontot. Ekkor minden I_j 100 %-osan megjelenik a felajánlott hívások számában minden olyan áramkörcsoportnál amelyen keresztül a I_j forgalom megközelíti a célt. Ha a blokkolás vagy az útvonalválasztás miatt (alternatív vagy terhelés megosztó útvonalválasztás) a hívások több úton közelítik meg a célt, akkor ez az érték már nem feltétlenül 100 %.

Nézzünk meg egy három központból álló esetet (10. ábra).



10. ábra. A 'B'-be menő forgalmak

Az áramkörök blokkoltságát mutatja a táblázat:

Trönk	Sikeres hívások aránya
B_{AB}	0,96
B_{CA}	0,92
B_{CB}	0,6

A 10. ábrán bejelöltük a B-ben végződő hívások útvonalát. Látható, hogy C-ből B-be két útvonalon is mennek a hívások, míg A-ból B-be csak egyen.

Az alkalmazott útvonalválasztás a következő: Minden hívás először a közvetlen linken próbálkozik. Ha ott nincs szabad áramkör, akkor a kettő hosszú kerülő úton próbál felépülni a hívás.

A fenti adatok birtokában a CB forgalomra vonatkozó $R_{j,k}$ értékek:

$$R_{\mathrm{CB,CB}} = 1,0$$
$$R_{\mathrm{CB,CA}} = 1,0 * (1 - B_{\mathrm{CB}}) = 0,4$$
$$R_{\mathrm{CB,AB}} = 0,4 * B_{\mathrm{CA}} = 0,37$$

Az $R_{j,k}$ értékek felírásakor azzal a már említett közelítéssel éltünk, hogy a különböző források által egy linknek felajánlott hívásokat Poisson folyamatnak tekintjük. Ekkor igaz az, hogy az egyes források által felajánlott hívások azonos mértékben blokkolódnak az adott linken.

Az $R_{j,k}$ értékek ismeretében felírhatunk egy olyan egyenletrendszert melynek megoldása szolgáltatja a keresett I_j értékeket. Igaz ugyanis a következő: Az N_j-be beleszámít minden olyan I_k ahol a j-ben és k-ban a célközpont megegyezik $(j \in S,\ k \in S)$ és az I_k forgalom eljut valahogyan a j-ben szereplő forrásközpontba, másképpen, az I_k forgalom megjelenik a j-ben szereplő forrásközpont kimenő linkjén.

$$N_j = \sum_{k \in S} I_k \sum_{I \in G_j} R_{k,j} \quad j \in S,\ k \in S$$

ahol G_j jelöli S azon részhalmazát ahol a forrás a j-ben szereplő forrásközpont.

Ilyen módon pontosan $n * (n-1)$ egyenletet felírva megkapjuk a kívánt I_j ismeretleneket.

8. ADATVESZTÉS

A valóságban természetesen nem biztos, hogy a kívánt mérési eredmények minden időpontban helyesen megérkeznek. Lehet, hogy egyes központokból nem kapjuk meg időben az eredményeket. Ez főleg a hálózatban bekövetkezett hibák esetén fordulhat elő, amikor az adatok fontossága jelentősen megnő. Ilyenkor célszerű a hiányzó értékeket valamilyen módon megbecsülni a korábbi adatok alapján.

Hibás, vagy nem létező mérési eredmény esetén az új értéket görbeillesztéssel számíthatjuk ki. Az előző néhány (8-20) mérési pontra egy másodfokú görbét illesztünk úgy, hogy a görbétől való eltérések négyzetösszege minimális legyen ([5] 673. o.). Az adatvesztés vizsgálata során változtatott paraméterek:

- adatvesztés valószínűsége (a központokban állítható);
- a görbeillesztésnél figyelembe vett pontok száma.

A görbeillesztésnél figyelembe vett pontok számánál két szempont játszik szerepet:

- a mérési eredmények viszonylag nagy fluktuációja miatt érdemes minél több pontra támaszkodó görbét készíteni;
- a felajánlott forgalom napi változása miatt nem szabad túl sok pontot figyelembe venni, hiszen ekkor sokkal korábbi tendenciákat is figyelembe veszünk.

A két szempont ellentmondó. Negyedórás adatgyűjtéssel számolva és tekintetbe véve, hogy a forgalmas óra környékén a felajánlott forgalom akár egy óra leforgása alatt is jelentősen változhat, láthatjuk, hogy ezen paraméter megválasztása nem egyszerű feladat. Más-más érték javasolható a forgalmas óra környékén, illetve korán reggel. Kedvezőbb esetben egy nagy forgalmú forgalomforrásról van szó, hiszen nagyobb forgalom esetén a mért értékek relatív szórása csökken, így kevesebb mérési pont figyelembevételével is kaphatunk kielégítő becsléseket a görbeillesztéssel.

A hiányzó mérési eredmény becslésekor további lehetőség, hogy figyelembe veszünk hosszú távú statisztikákat a forgalom napi változását illetően. Ilyen információk figyelembe vételével kiszűrhetünk hibás mérési eredményeket (konfidencia intervallumokat határozhatunk meg), és elérhetjük, hogy normál működés esetén pontosabb követő hálózathoz jussuk. Ilyenkor viszont a szokásostól eltérő, előfizetők viselkedésében beálló hirtelen változásra rosszabbul reagál a rendszer.

9. SZIMULÁCIÓS EREDMÉNYEK

Az itt közölt eredményeket igen egyszerű, három központból és az őket összekötő három trönkből álló, méretezési és forgalmi szempontból teljesen szimmetrikus hálózat szimulációs vizsgálata során kaptuk. Célunk a tárgyalt problémák illusztrálása volt. A 11., 12. ábrán az egyik forgalomforrás hívásintenzitásának változását láthatjuk az idő függvényében. A világos görbék a valós hálózatból, egész pontosan az emulált hálózatból származó eredményeket mutatják, a sötétek pedig a követő hálózatból nyert szimulációs értékeket. A szimuláció minden esetben 15 perces mérési intervallummal történt.

9.1. Normál működés

A következő két grafikonon a két alapvető mérési hozzáállásból származó különbségeket láthatjuk. A 11. a) ábrán azt az esetet látjuk, amikor a valós hálózatból közvetlenül a modellünknek megfelelő mérési adatokat kapunk. A b) ábrán látható esetben pedig több, egyszerűbb mérésből a 7.2-ben leírt módon származtatott adatokat használtunk a modell beállításához.

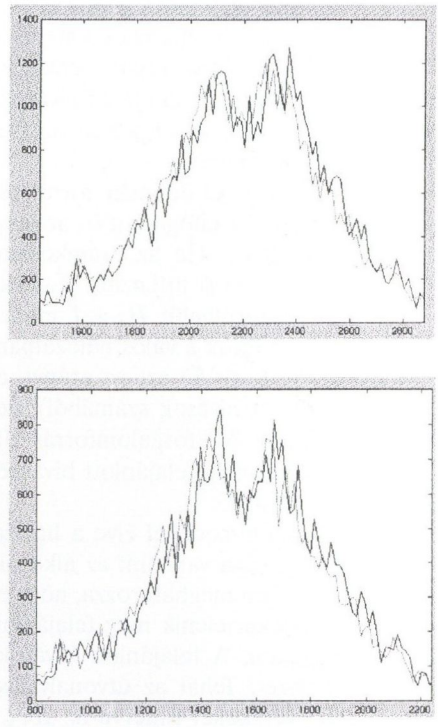
Látható, hogy az utóbbi esetben a követő hálózat jobban eltér a valós hálózattól, mint a közvetlen méréses esetnél. A hatás leginkább a forgalmas órák környékén jelentkezik

9.2. Adatvesztés esete

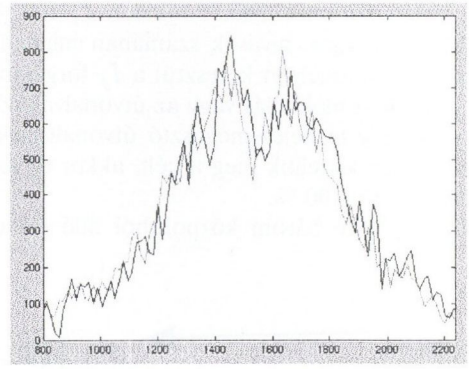
Megnéztük, hogyan viselkedik a rendszer, ha nem minden mérési adat érkezik meg. A hiányzó értékek becslésére a már említett minimális négyzetes eltérésen alapuló jóslást alkalmaztuk. Tíz pontra parabolát illesztve becsültük a hiányzó adatokat.

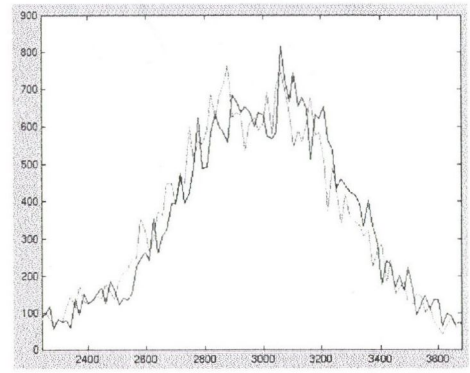
A 12. ábra a szimulációs eredményeket mutatja. Az a) ábrán az az eset látható, amikor a mért adatok egynegyede veszik el, a b) ábrát pedig úgy kaptuk, hogy a mért értékek fele nem érkezett meg.

Ötven százalékosnál jóval nagyobb hibavalószínűség esetén a követő hálózat viselkedése jelentősen eltérhet a valós hálózatétól. Viszont ha a méréseknek átlagosan legalább a fele rendelkezésre áll, akkor számíthatunk arra, hogy a követő hálózat viszonylag pontosan visszaadja a valós hálózat előfizetőinek viselkedését körülbelül egy mérési periódussal késleltetve.



11. ábra. Normál működés





12. ábra. Adatvesztés

10. ÖSSZEFOGLALÁS

A hálózati forgalommenedzsment növekvő fontossága miatt egyre nagyobb az igény valós idejű menedzsment segítő, döntéstámogató eszköz létrehozására. Ez megvalósítható már meglévő, off-line eszközök továbbfejlesztésével, átalakításával, és a valós hálózathoz kapcsolásával.

Vizsgálataink középpontjában a hagyományos telefonhálózatok szerepeltek, azonban a vizsgált jellemzők többsége más hálózatokban is megtalálható, például az ISDN, GSM hálózatokban. Ezekben a hálózatokban a valós idejű szimuláció hasonló problémákat vet fel, az eredmények egy része ott is kamatoztatható.

További megfontolások tárgyát képezi, hogy a valós idejű adatgyűjtés eredményeképpen, a menedzsment központban rendelkezésre álló adatok alapján milyen módon lehetséges a hálózat erőforrásainak kiesését, vagy más rendellenes helyzetet észlelni.

Felmerül még, hogy a hálózatban bekövetkező nem várt esemény hatására érdemes rendkívüli mérési eredményeket letölteni, ill. hiányzó mérési eredmények esetén a napi forgalomra nézve hosszú távú statisztikákat is figyelembe venni.

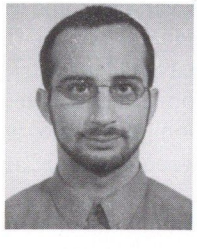
A tárgyalt szimulációs módszerek segítségével csökken a hálózati forgalommenedzsment beavatkozás kockázata. Érdemes tehát összevetni egy ilyen rendszer megépítésének a költségeit azzal az összeggel amit egy ilyen eszköz megtakaríthat a sokkal hatékonyabb forgalommenedzsment segítségével.

IRODALOM

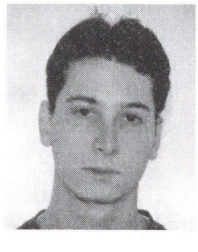
[1] Recommendation E.410, International Network Management – General Information, ITU, 1992.
[2] Recommendation E.411, International Network Management – Operational Guidance, ITU, 1992.
[3] Recommendation E.412, Network Management Controls, ITU, 1992.
[4] Recommendation Q.544, Digital Exchange Measurements, ITU, 1992.
[5] G. A. Korn, T. M. Korn: Matematikai Kézikönyv Műszakiaknak, Műszaki Könyvkiadó, Budapest, 1975.
[6] OPNET: www.mil3.com
[7] COMNET III: www.casias1.com/comnet.html

REAL TIME SIMULATION OF PSTN NETWORKS

At Ericsson there is a performance evaluation tool called PlasmaSIM, which uses simulation and analytical methods to obtain the required performance metrics of a given network in certain situations. The tool is suitable for modelling the behaviour of the network and the impacts of several traffic management actions as well. Having this kind of simulator the idea occurs to create connection between the simulator and a real network. Having a model in the simulator the problem to be solved is refreshing the parameters of the traffic offered by the subscribers according to real time data collected in the exchanges. Having such a connection the management has up-to-date information of the operation of the real network. This is useful because the manager can examine the effects of possible interventions without causing damage to the real network. If the actions are prove to be efficient they can be applied to the real network. We examined what kinds of measurements are available from a real network and which of them are useful from model building viewpoint. We also investigated the possibilities of setting the traffic behaviour of the subscribers in the simulator on the basis of different types of measurements. Furthermore we examined what can be done if some of the measured data are lost.



Farkas János a BME Villamosmérnöki és Informatikai Karának ötödéves villamosmérnök hallgatója a távközlés és telematika szakirányon. Egyetemi tanulmányai mellett 1997 ősze óta az Ericsson Kutatólaboratóriumában dolgozik, PSTN hálózatok forglommenedzsmentjével és teljesítmény analízisével foglalkozik. Jelenleg diplomamunkáját készíti, melynek témája: Az áramkörtartalékolás (circuit reservation) alkalmazásának lehetőségei távközlési hálózatok forgalommendzsmentjében.



Kumli Tamás a BME Villamosmérnöki és Informatikai Karának ötödéves villamosmérnök hallgatója a távközlés és telematika szakirányon. Egyetemi tanulmányai mellett 1997 ősze óta az Ericsson Kutatólaboratóriumában dolgozik, PSTN hálózatok forgalommenedzsmentjével és teljesítmény analízisével foglalkozik. Jelenleg diplomamunkáját készíti, melynek témája: Hangátvitel ATM hálózatokon.

INVESTIGATION OF FRACTAL PROPERTIES IN DATA TRAFFIC

TRANG DINH DANG, SÁNDOR MOLNÁR, ATTILA VIDÁCS

HIGH SPEED NETWORKS LABORATORY
DEPT. OF TELECOMMUNICATIONS AND TELEMATICS
TECHNICAL UNIVERSITY OF BUDAPEST
H-1117, PÁZMÁNY PÉTER SÉTÁNY 1/D, BUDAPEST, HUNGARY
TEL: (361) 463 3889
FAX: (361) 463 3107
E-MAIL: {TRANG,MOLNAR,VIDACS}@TTT-ATM.TTT.BME.HU

The goal of this study is to introduce some important topics in today's traffic modeling in high-speed networks. In recent years, a number of studies demonstrated that in wide variety of networking environments the traffic appears to exhibit many unusual characteristics such as heavy-tailed distributions, long-range dependence (LRD) and self-similarity. Since understanding traffic characteristics is very important in network dimensioning and performance prediction, the identification and quantification of these phenomena are in the focus of this paper. Together with the description of the statistical methods used, the analysis results are presented for two data sets taken from real networks.

1. INTRODUCTION

The classical models in queuing and network theory based on, for example, the Erlang formulas contain simple assumptions that guarantee the Markovian properties and ensure their analytical tractability. In the early stages of traffic modeling – when the typical case was the telephone traffic – the Poisson process was known as a simple and adequate model of real traffic. Nowadays, with a surprisingly rapid rate of the evolution of communication technology, we know much more about traffic flows of different kinds. Let's take a look at some of them which we are using in our everyday's life: the wide area TCP traffic which provides the Internet connection, the possibility for e-mail; the FTP traffic for file transfers; the TELNET traffic for external accessing; the video conferencing data; etc. Statistical analysis of number of data sets selected from this traffic mix show that some properties cannot be explained by Poisson-like models. Analysis of these data is challenging since there is strong evidence that the classical modeling assumptions (such as independence or the lack of long memory) do not hold any longer.

In recent years, a number of studies, [1], [2], [5], [7], [14], and [19], demonstrated that in certain environments, the traffic appears to exhibit many unusual characteristics such as *heavy-tailed distributions*, *long-range dependence* and *self-similarity*. In some of these publications useful analytical methods – which were used to identify and quantify these properties – can be found with detailed (or less detailed) descriptions.

Since understanding traffic behavior and characteristics is very important to network designers and system analysts in network dimensioning and performance prediction, there are needs to study and understand the heavy-tailed and self-similar properties of today's network traffic. In this paper the mathematical side of these phenomena is addressed. First, approaches and results which researchers had reached in their studies of this area is summarized. Second, our analysis to test the fractal behavior of measured data including heavy tail and long-range dependence tests are presented.

2. BACKGROUND

Before turning to the main point of this study, this chapter introduces the basic concepts of fractal traffic characteristics.

2.1. Heavy-tailed distributions

The concept heavy-tail can be found in many environments. Heavy-tailed distribution arises in the set of cities have all the people, the set of words have all the use, the set of earthquakes do all the damage, etc. Let's look at an example: consider a variable that represents a waiting time. For waiting time with a light-tailed distribution, the longer we have waited, the sooner we are likely to be done. In contrast, for waiting time with a heavy-tailed distribution, the longer we have waited, the longer is our expected future waiting time [2].

To be more specific, let X be a random variable with distribution function F concentrating on $[0, \infty)$.

Definition 1 *[16] F is said to be heavy-tailed with index α, if*

$$1 - F(x) = x^{-\alpha} L(x), \quad \text{as} \quad x \to \infty, \quad \alpha > 0 \quad (1)$$

where L is slowly varying at ∞, i.e., $\lim_{x\to\infty} L(tx)/L(x) = 1, t > 0$.

If $\alpha < 2$, the distribution has infinite variance, and if $\alpha < 1$, it has infinite mean.

For example, the simplest case of heavy-tailed distributions is the so-called Pareto distribution. In this case, $L(x) \equiv 1$, so the distribution function of Pareto is $F(x) = 1 - x^{-\alpha}$. The difference between exponential tails and heavy tails can be seen on Fig. 1.

In communications, heavy-tailed distributions have been used to model number of traffic flows like sizes of Unix files or frame sizes of variable bit rate video.

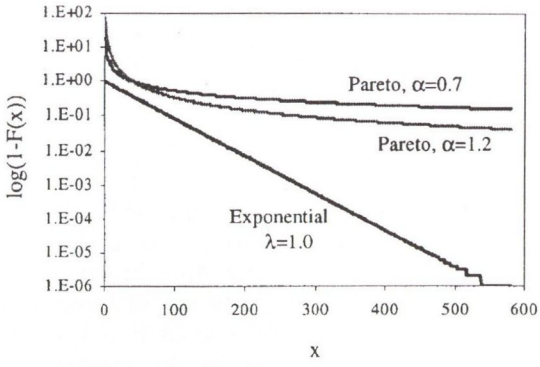


Fig. 1. The distribution tails of exponential and Pareto distributions

2.2. Long-range dependence

The autocorrelation function $r(k)$:

$$r(k) = \frac{E\{(X_n - E(X))(X_{n+k} - E(X))\}}{E\left\{(X_n - E(X))^2\right\}}$$

of a long-range dependent stochastic process decays hyperbolically as the lag increases. As a result, $\sum_{k=1}^{n} r(k) \to \infty$ when n grows in infinity. This non-summability of the correlations captures the intuition behind long-range dependence, namely that while high-lag correlations are all individually small, the cumulative effect is of importance and gives rise to features which are drastically different from those of the more conventional, i.e., short-range dependent processes. The latter are characterized by a geometric decay of the autocorrelations, i.e., $r(k) \sim a^k, 0 < a < 1$ as $k \to \infty$, resulting in the summable autocorrelation function $0 < \sum_k r(k) < \infty$. By definition,

Definition 2 *[9] X_t is called a stationary process with long range dependence (LRD or long memory) if there exists a real number $H \in (0.5, 1)$ and a constant $c_r > 0$ such that*

$$\lim_{k \to \infty} \frac{r(k)}{c_r k^{2H-2}} = 1, \qquad (2)$$

where H is called the Hurst parameter and measures the degree of LRD.

2.3. Self-similarity

The unifying concept underlying fractals, chaos, and power laws is self-similarity. Self-similarity, or invariance against changes in scale or size, is an attribute of many laws of nature and innumerable phenomena in the world around us [17]. A phenomenon that is self-similar looks the same or behaves the same way when being viewed at different scales on a dimension. The dimension can be considered in space or time. In our study of the traffic data, we concentrate on the time series and stochastic processes that exhibit self-similarity with respect to time.

Fig. 2 is a comparison of time series plots of a self-similar and a non-self-similar stochastic process.

Note that self-similarity does not mean that the time function is exactly reproduced at different time scales. Instead we can observe similar burstiness of traffic at different time scales in case of self-similar traffic. This difference is noticeable between the self-similar process (left side) and the non self-similar process (right side).

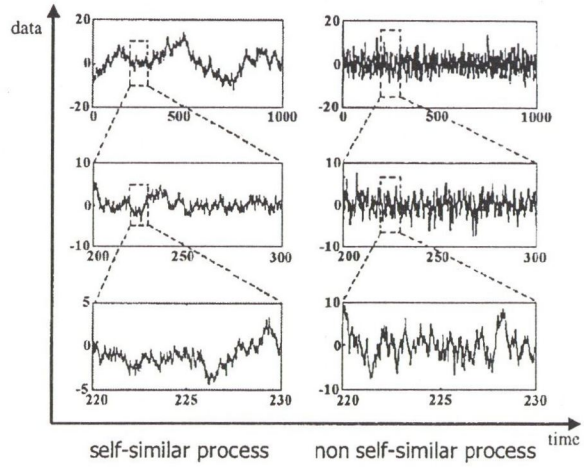


Fig. 2. Comparison of self-similar and non self-similar process

Definition 3 *[14] Consider the process X, and define the m-aggregated time series $(m = 1, 2, \ldots)$*

$$X^{(m)} = \{X_k^{(m)} : X_k^{(m)} = \frac{1}{m}(X_{mk-m+1} + \ldots + X_{mk}), \quad k = 1, 2, \ldots\} \qquad (3)$$

Let $r^{(m)}(k)$ be the autocorrelation function of the aggregated process. The process X is said to be

(a) exactly self-similar, if $X \stackrel{d}{=} m^{1-H} X^{(m)}$, i.e., if X is identical to $X^{(m)}$ within a scale factor in a finite dimensional distribution sense.

(b) exactly second-order self-similar, if $r^{(m)}(k) = r(k)$, $k \geq 0$.

(c) asymptotically second-order self-similar, if $r^{(m)}(k) \approx r(k)$, $k, m \to 0$.

3. PERFORMANCE IMPLICATIONS

The first study of fractal behavior of traffic was published in [5] by researchers at Bellcore. Based on extensive measurements made on a local area Ethernet network they concluded that the traffic possesses self-similar properties and discovered that the higher the load on the Ethernet, the higher the estimated Hurst parameter H of the traffic or, equivalently, the higher the degree of self-similarity. This result is vital because it is precisely at high loads that performance issues become most relevant.

An equally important result of the Ethernet analysis was the inadequacy of traditional queuing models to predict performance. For example, a common assumption concerning data traffic is that multiplexing a large number of independent traffic streams results in a Poisson process. It would be the right assumption, if we disregard some limits in the environment. Study in [6] points out that this assumption and the resulting queuing analysis led Asynchronous Transfer Mode (ATM) switch vendors to produce first generation switches with small buffers (10 – 100 cells). When these switches were deployed in the field and exposed to real traffic, cell losses far beyond those expected were experienced and resulted in a redesign of the switches.

For a queuing system, such as ATM, Frame Relay, 100BASE T, Wide Area Network (WAN) routers, and generally for statistical multiplexers, if the input data of the queue is self-similar, then increased delays and increased buffer size requirements will be experienced [5]. The queuing performance of actual ATM traffic exhibiting self-similar characteristics was investigated in [13?]. It has been found that the upper time scale which determines the range of correlations of interest from cell loss point of view is approximately ten times the buffer size. However, this time scale also depends on the load.

For better traffic control, the traffic profile can be changed, for example by traffic shaping. However, the fractal characteristics seem to be rather robust with respect to shaping and can difficultly be removed [11].

The nature of traffic self-similarity may be inherent in the data traffic source, for example the Variable Bite Rate (VBR) video traffic [8], or may be the result of numerous interactions with the network, for example the Transmission Control Protocol-based (TCP) traffic [7]. In the first case, the traffic behavior remains dependent of the network conditions under which it is sent, it can be effectively managed in the context of admission control and resource allocation subject to Quality of Service (QoS) guarantees. In the other case, the traffic self-similarity changes its behavior depending on the congestion status, re-transmission scheme (different TCP version), number of concurrent users, request file size (for Web), File Transfer Protocol (FTP) file size, and so on. Some cases, non-stationarity can be detected in measured traffic which can also provide alternative modeling approaches to fractal traffic modeling [12]. In both cases the traffic is difficult to be characterized and modeled. From traffic engineering point of view, it yields to a difficult traffic control.

This summary took part in a wide area and dealt with different kinds of network traffic and based on the results, self-similarity and heavy-tailedness seem to be good structures in high-speed network modeling. Although their application can explain and address many problems in the traffic behavior, it does not mean that these models are the best and the only solution for the modern traffic modeling. The studies on self-similarity and heavy-tailedness is complicated and still the subject of the ongoing research all over the world.

4. MEASUREMENTS

These measurements are freely available from the Internet Traffic Archive [18].

4.1. IP traffic traces

This trace is the result of an hour long Ethernet measurement ran from 14:00 to 15:00 on Friday, January 21, 1994. The tracing was done on the Ethernet DMZ network over which flow all traffic into or out of the Lawrence Berkeley Laboratory, located in Berkeley, California. The raw traces were made using tcpdump on a Sun SparcStation using the BPF kernel packet filter.

The measurement captured arrival timestamps in microsecond precision of TCP, UDP, TCP SYN/FIN/RST, encapsulated IP and other IP packets in five files, respectively. After processing these files, a set of around $300,000$ IP packet arrivals in consecutive time-windows, equally $0.021sec$, was selected for analysis.

4.2. WWW traffic traces

These measurements were done at Boston University's Computer Science Department. In order to capture all of the Web activity on a Local Area Network (LAN), researchers modified the Web browser NCSA Mosaic and installed it for general use. After that Mosaic browsers could write down all working activities of browsers in a *log* file. Each line in a *log* corresponds to a single URL requested by the user; it contains the machine name, the timestamp when the request was made, the user id number, the URL, the size of the document (including the overhead of the protocol) and the object retrieval time in seconds (reflecting only actual communication time, and not including the intermediate processing performed by Mosaic in a multi-connection transfer). These traces contain records of the HTTP requests and user behavior of a set of Mosaic clients running in a general computing environment at the department. This environment consists principally of 37 SparcStations 2 workstations connected in a local network, which is divided in two sub-nets. Each workstation has its own local disk; *log*s were written to the local disk and subsequently transferred to a central repository. The data collection then took place in about 5 months from 17 January 1995 until 8 May 1995.

In this study we consider only the characteristics of the file sizes transmitted over the Internet. So a small C routine was implemented to subtract this information from over 6000 *log* files. Around $230,000$ unique file sizes were recorded. As the suggestion of some previous studies, this data set – called the Web file sizes data set or the WFS set – may contain heavy-tailed properties.

5. ANALYSIS AND RESULTS

5.1. Testing for heavy tails

A heavy-tailed process has its own feature that the tail of the distribution decays much more slowly than exponential. This is the main point of methods used to detect the heavy tail. Moreover, to estimate the scale parameter α (see Definition 1) various exploratory plotting techniques are available. They are based on the Hill estimator and the modified QQ-plot. Another considerable method is the DeHaan's moment estimator. These statistics are shortly described in the followings.

Hill estimator Suppose $X_1, X_2, \ldots, X_n$ are independent, identically distributed (iid.) random samples from a distribution F and $X_{1,n} \geq X_{2,n} \geq \ldots \geq X_{n,n}$ are the order statistics. If F is a heavy-tailed distribution (see Definition 1), The Hill estimation of index α takes the following form [16]:

$$\hat{\alpha} = \hat{\alpha}_{k,n} = \left(\frac{1}{k} \sum_{j=1}^{n} \log X_{j,n} - \log X_{k,n} \right)^{-1} . \quad (4)$$

The Hill estimation of WFS data set can be seen on Fig 3. The plot goes fast to its stable value 0.67. It is the estimate of index α of the WFS distribution tail.

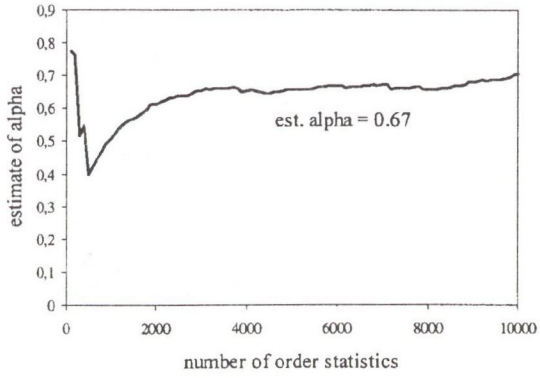


Fig. 3. The Hill plot estimation of WFS data set

Modified QQ-plot The main idea of using modified QQ-plot follows the assumption: if $X_1 \geq X_2 \geq \ldots \geq X_k$ are samples from a distribution F and k is large enough, the distribution function F at $x = X_j$ can be estimated by

$$P(x < X_j) = F(X_j) \approx 1 - \frac{j}{k+1}. \tag{5}$$

From this, the modified QQ-plot is defined as follows [10]: Let $X_1 \geq X_2 \geq \ldots \geq X_k = u$ be the order statistics of a distribution, which is approximately Pareto. Then the plot of

$$\left\{ \left(\log X_j - \log u, \quad -\log\left(\frac{j}{k+1}\right)\right), \quad 1 \leq j \leq k \right\} \tag{6}$$

should roughly look like a straight line with slope α.

Fig. 4 is the modified QQ-plot of WFS data set. It can be seen on the figure that the plot is not exactly a straight line but a regression line can be fitted over points with small deviations. The slope provides the estimate of α to be 0.73.

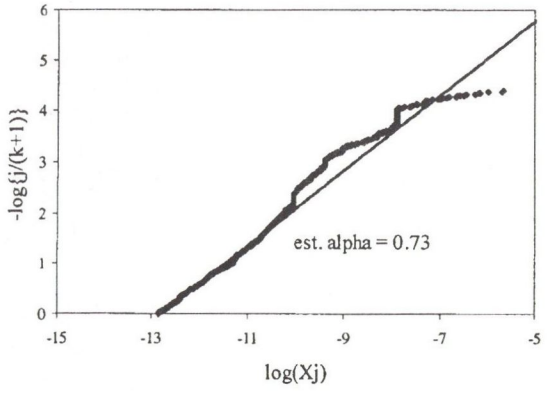


Fig. 4. The modified QQ-plot estimation of WFS data set

DeHaan's moment estimator According to [16], DeHaan's moment estimator is defined as follows: Let $X_1 \geq X_2 \geq \ldots \geq X_n$ be the order statistics from a random sample of size n. Define for $r = 1, 2$ and for k upper-order statistics

$$H_{k,n}^r = \frac{1}{k} \sum_{i=1}^{k} \left(\log \frac{X_i}{X_{k+1}} \right)^r. \tag{7}$$

DeHaan's estimate of index α can be calculated by the form

$$\hat{\alpha} = \hat{\gamma}^{-1} = \left(H_{k,n}^1 + 1 - \frac{1}{2\left(1 - \frac{(H_{k,n}^1)^2}{H_{k,n}^2}\right)} \right)^{-1}. \tag{8}$$

Fig. 5 shows the plot result generated by DeHaan's testing methods. The estimate of α in this case, 0.65, is a bit smaller than in the Hill's case. It may be the effect of smoothing technique used in DeHaan's algorithm.

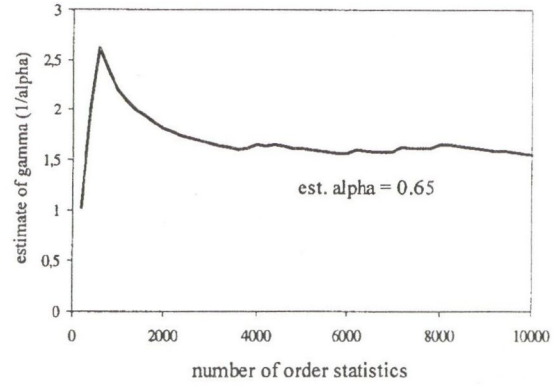


Fig. 5. DeHaan's estimate of index α of WFS data set

We can conclude that the set of file sizes transferred over the Internet seems to fit well the Pareto distribution with index α about 0.7. Similar results were also explored by other researchers in [1]. As discussed in this paper, it may be an evidence of self-similar WWW traffic.

5.2. Testing for LRD and self-similarity

For estimating the Hurst parameter, a number of algorithms has been worked out. Algorithms were described, for example, in [3], [4], [16]. In this section four widely used methods: variance-time plot, R/S plot, periodogram, and Whittle estimator are summarized. However, by using LRD tests and other statistical tests, it is difficult to make reliable conclusions about the self-similarity of traffic. Note that in most cases statistical methods can not prove an empirical data set to be produced by an exactly self-similar process. Instead, as shown in Definition 3, a data set may only have the property of second-order or asymptotically second-order self-similarity.

Variance-time plot For a stationary process with LRD, the following property can be proven:

$$\mathrm{var}(X^{(m)}) = \frac{1}{m^{2-2H}} \mathrm{var}(X), \tag{9}$$

so

$$\log \mathrm{var}(X^{(m)}) = \log \mathrm{var}(X) + (2H - 2) \log m. \tag{10}$$

Because $\log \mathrm{var}(X)$ is a constant independent of m, if we plot $\mathrm{var}(X^{(m)})$ versus m on a log-log graph, the result should be a straight line with a slope of $(2H - 2)$. The plot can be easily generated from the data series X by generating the aggregated processes of X at different levels of m and then computing the empirical variance. Plot with slope values between -1 and 0 suggests LRD.

The variance-time plot of IP data set is drawn on Fig 6. It is surprising that there is a breaking point on the plot. From a certain large value of time unit, the slope takes up a bigger value. Anyway, by the Definition 2 of LRD it is an asymptotic characteristics, so the Hurst parameter should be estimated by the slope of the higher aggregation levels. The estimate of H was 0.83.

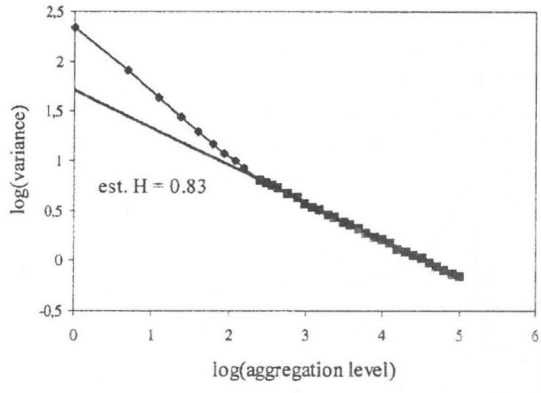


Fig. 6. Variance-time plot of IP data set

R/S plot For a stochastic process X defined in discrete time $\{X_j : j = 1, 2, \ldots, n\}$, the rescaled adjusted range or R/S-statistics of X over a time interval n is defined as the ratio R/S with:

$$\begin{aligned} R &= \max\{W_i : i = 1, 2, \ldots, n\} \\ &\quad - \min\{W_i : i = 1, 2, \ldots, n\}, \\ S &= \sqrt{\mathrm{var}(X)} \end{aligned} \tag{11}$$

where $W_i = \sum_{k=1}^{i}(X_k - \overline{X}), i = 1, 2, \ldots, n$ and $\overline{X} = (1/n)\sum_{i=1}^{n} X_i$. It can be proven for any stationary process with LRD that the ratio R/S has the following characteristics for large n:

$$\frac{R}{S} \approx \left(\frac{n}{2}\right)^{H} \tag{12}$$

which is known under the name *Hurst effect*. Thus if we plot R/S versus n on a log-log graph $\log(R/S) \approx H \log n - H \log 2$, the plot should fit a straight line with slope H.

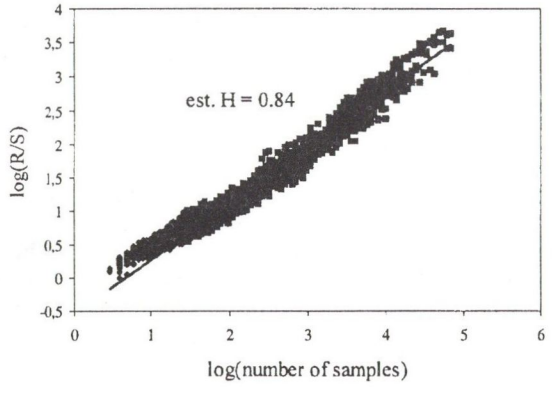


Fig. 7. R/S analysis of IP data set

Using this algorithm, the R/S analysis of IP data set was provided and can be seen on Fig. 7. Data points are scattered around a straight line, which means that IP packet arrivals seem to be LRD with Hurst parameter $H = 0.84$, which is the estimate from the slope of regression line.

Periodogram Another alternative way to estimate the Hurst parameter of LRD is the periodogram plot. The power spectral density of a LRD process obeys a power law near the origin

$$\lim_{\nu \to 0} \frac{f(\nu)}{c_f |\nu|^{1-2H}} = 1. \tag{13}$$

where c_f is a constant, ν is the frequency, and $f(\nu)$ is the power spectral density function, that is the Fourier transform of the autocorrelation function $r(k)$. Periodogram provides a fast estimate of $f(\nu)$:

$$I(\nu) = \frac{1}{2\pi n}\left|\sum_{k=1}^{n}(X_k - \overline{X})e^{ik\nu}\right|^2. \tag{14}$$

So if the periodogram is plotted against small values of frequency on a log-log graph, the plot should be a straight line with slope $(1 - 2H)$.

The periodogram plot of IP data set is shown on Fig. 8. The estimate of H in this case is 0.82.

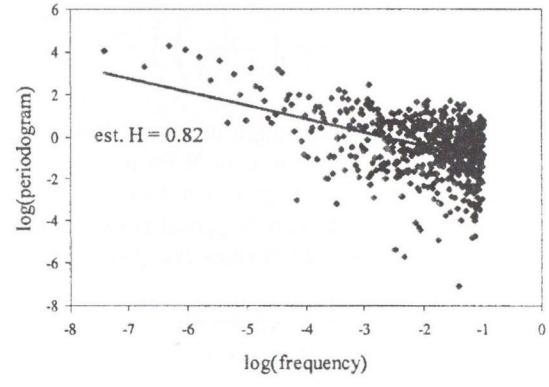


Fig. 8. Periodogram plot of IP data set

Whittle estimator Whittle estimator is a concrete application of maximum likelihood method (MLE). On the other hand, the Whittle estimation is based on the periodogram. So in most cases these methods provided the same estimates of the Hurst parameter.

The Whittle estimator was suggested to estimate the Hurst parameter of Fractional Gaussian Noise (FGN), which is an exactly self-similar process. If data is from a FGN process, the estimate of H is the value that minimizes the function $Q(H)$:

$$Q(H) = \int_{-\pi}^{\pi} \frac{I(\nu)}{f(\nu, H)}\,\mathrm{d}x + \int_{-\pi}^{\pi} \log f(\nu, H)\,\mathrm{d}\nu. \tag{15}$$

To calculate the value of $Q(H)$, we should consider the exact behavior of the spectral density $f(\nu)$ of the process close to the origin. The Whittle estimator is more robust testing method than the others, and it also provides the confidence interval (95%) of the calculated Hurst value.

Fig. 9 shows the Whittle estimation of IP data set. The result is 0.83 with confidence interval (0.81, 0.85).

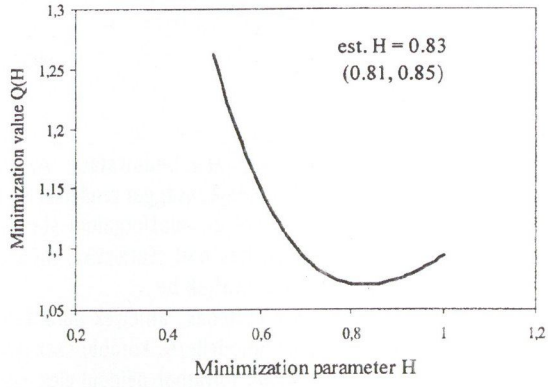


Fig. 9. The Whittle estimate of H of IP data set

So, by going through four testing methods, variance-time plot, R/S plot, periodogram, and Whittle estimator, the IP packet arrival process seems to exhibit LRD with $H \approx 0.83$. (Although Whittle estimator provides the good estimate of Hurst parameter, it is a bit soon to make a conclusion about self-similarity of this process.)

Note that IP packet arrivals and WWW file sizes are not the only samples of traffic flows which are analyzed to provide fractal properties in recent several years. This topic is still an open area of traffic modeling for more studies and researches.

6. CONCLUSION

In this paper, after summarizing the results and observations of researchers about self-similar and heavy-tailed properties of some high speed network traffic types in recent years, the brief mathematical background of them was discussed. These properties of high-speed networks have a strong impact on the performance of the networks. Then the analytical methods testing for self-similarity and heavy-tailedness were described. It included the algorithms of useful statistical methods: variance-time plot, R/S plot, periodogram, and Whittle estimator for LRD and modified QQ-plot, DeHaan's moment method and Hill estimator for heavy-tailedness. Using these methods, two data sets from real traffic measurements were analyzed.

Testing with the IP packet arrivals data set provided LRD property with asymptotic characteristics. The estimate of H in various estimating methods was about the same, 0.83. The confidence interval (95%) given by the Whittle estimator was $(0.81, 0.85)$. The distribution of file sizes transferred on the Internet from a given threshold may be well modeled by heavy-tailed (Pareto) distributions. The estimates of scale parameter α are about the same and equals 0.7. Heavy-tailed file sizes may be a cause of self-similar WWW traffic which was discussed in [1].

More recent researches indicate that complex traffic (ATM or Internet) is consistent to an even more complex structure compound to self-similarity. This research [14] suggests that traffic has multifractal nature. The application of multifractals for traffic modeling is a hot research topic.

REFERENCES

[1] M.E. Crovella and A. Bestavros. Explaining World Wide Web Traffic Self-similarity. Technical Report TR-95-015, Boston University Computer Science Department, Revised, October 12, 1995.

[2] V. Paxson and S. Floyd. Wide-Area Traffic: The Failure of Poisson Modeling. In Proceedings of SIGCOMM '94, 1994.

[3] M.S. Taqqu, V. Teverovsky, and W. Willinger. Estimators for long-range dependence: an empirical study. Preprint, 1995.

[4] M.S. Taqqu. Statistical methods for detecting long-range dependence. Available at http://math.bu.edu/people/murad/methods/index.html

[5] W.E. Leland, M.S. Taqqu, W. Willinger, and D. Wilson. On the Self-similar Nature of Ethernet traffic (Extended version). IEEE/ACM Transactions on Networking,1994.

[6] W. Willinger, D. Wilson, and M.S. Taqqu. Self-similar Traffic Modeling for High-speed Networks. ConneXions, November 1994.

[7] B. Ryu and M. Nandikesan. Real-time Generation of Fractal ATM Traffic: Model, Algorithm, and Implementation. Submitted to Globecom '96, 1996.

[8] B. Ryu and A. Elwalid. The importance of long-range dependence of VBR video traffic in ATM traffic engineering: Myths and realities. ACM/SIGCOMM'96, San Francisco, CA, USA, August, 1996.

[9] J. Beran. *Statistics for Long-Memory Processes*. Chapman & Hall, One Penn Plaza, New York, NY 10119, 1994.

[10] P. Embrechts, C. Klüppelberg, and T. Mikosh. *Modeling Extremal Events for Insurance and Finance*. Springer-Verlag, Berlin Heidelberg, 1997.

[11] S. Molnár and A. Vidács. On Modeling and Shaping Self-Similar ATM Traffic. 15th International Teletraffic Congress, Washington, DC, USA, June 23-27, 1997.

[12] S. Molnár, A. Vidács, and A. A. Nilsson. Bottlenecks on the Way Towards Fractal Characterization of Network Traffic: Estimation and Interpretation of the Hurst Parameter. International Conference of the Performance and Management of Complex Communication Networks (PMCCN'97), 17-21 November, 1997, Tsukuba, Japan.

[13] A. Vidács, S. Molnár, G. Gordos and I. Cselényi. The Impact of Long Range Dependence on Cell Loss in an ATM Wide Area Network. GLOBECOM'98, Sydney, Australia, 8-12 November, 1998.

[14] S. Molnár and I. Maricza. Source Characterization in Broadband Networks. COST 257 Interim Report, Januar, 1999.

[15] S. Molnár, T. D. Dang, and A. Vidács. Heavy-tailedness, Long-range dependence and Self-similarity in Data Traffic. *Accepted for publication to ATSMA'99*, Nashville, Tennessee, USA, 18-21 Maricus, 1999.

[16] S. I. Resnick. Heavy tail modeling and teletraffic data. *The Annals of Statistics*, 25(5):1805 – 1869, 1997.

[17] G. Samorodnitsky and M.S. Taqqu. *Stable Non-Gaussian Random Processes*. Chapman & Hall, One Penn Plaza, New York, NY 10119, 1994.

[18] The Internet Traffic Archive. http://ita.ee.lbl.gov/index.html.

[19] W. Willinger, M. S. Taqqu, and A. Erramilli. A bibliographical guide to self-similar traffic and performance modeling for high speed networks: Stochastics Networks, Theory and Applications. 339-366, Oxford University Press, 1996

FRAKTÁLIS TULAJDONSÁGOK VIZSGÁLATA AZ ADATFORGALOMBAN

TRANG DINH DANG, MOLNÁR SÁNDOR, VIDÁCS ATTILA

BUDAPESTI MŰSZAKI EGYETEM
TÁVKÖZLÉS ÉS TELEMATIKA TANSZÉK
NAGYSEBESSÉGŰ HÁLÓZATOK LABORATÓRIUM (HSNLAB)
1111 BUDAPEST, PÁZMÁNY PÉTER SÉTÁNY 1/D

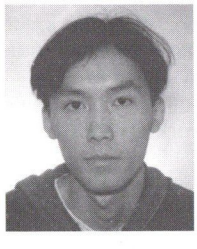
Jelen tanulmány célja néhány újszerű, napjaink nagysebességű hálózatainál alkalmazott forgalommodellezési eljárás bemutatása. Az elmúlt néhány év során spektrumában a forgalom számos szokatlan – a hagyományos technikák által nem leírt – tulajdonsággal rendelkezik, mint például „lassan lecsengő eloszlások", „hosszúidejű összefüggőség", vagy például az „önhasonlóság". Mivel az adatforgalom statisztikai jellemzőinek megértése a hálózattervezés és teljesítménybecslés szempontjából cikkünk középpontjában. A használt statisztikai módszerek leírása mellett azok alkalmazhatóságát két, valós hálózatból nyert forgalommérési eredmény analízise során mutatjuk be.

A ma már hagyományosnak nevezhető sorbanállás- és hálózatelméleti modellek olyan alapfeltevésekre építenek, amelyek garantálják a Markovi tulajdonságot és így jelentősen leegyszerűsítik a szükséges matematikai formalizmust. A forgalommodellezés korábbi szakaszában – amikor a tipikus hálózat és forgalom a vezetékes telefonhálózat és telefonbeszélgetések voltak – a Poisson folyamat például elégséges és egyben egyszerű modell volt a valós forgalom leírására.

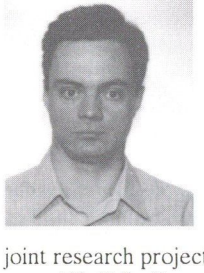
Manapság a távközlés technológiájának rohamos fejlődése következtében a forgalom minőségi és mennyiségi jellemzői is drasztikusan megváltoztak. A beszédátvitel mellett egyéb szolgáltatások széles skálájáról beszélhetünk, és minden szolgáltatástípushoz más-más forgalomtís rendelhető.

Csak néhány jellemző példát kiragadva: a globális hálózatok TCP forgalma, amely az alapját képezi az Internetes adatátvitel döntő hányadának, az elektronikus levelezés, az FTP forgalom, amely file-ok továbbítását teszi lehetővé, a Telnet kapcsolatok távoli elérés biztosítására, képátvitel az egyre inkább terjedő videokonferenciák esetében stb., mind mind alapvetően eltérő forgalmi kategóriákat jelentenek. Ezen forgalomtípusok analízise kimutatta, hogy az esetek többségében a hagyományos modellezési feltevések (mint például függetlenség vagy a hosszútávú memória hiánya) már nem állják meg a helyüket.

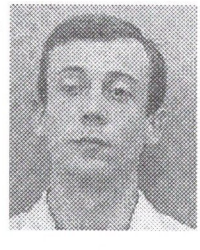
Mivel a hálózati forgalom statisztikai jellemzőinek megértése a hálózattervezés és teljesítménybecslés szempontjából kiemelkedő jelentőségű, ezen tulajdonságok kimutatása és számszerűsítése áll cikkünk középpontjában. A használt statisztikai módszerek leírása mellett azok alkalmazhatóságát két, valós hálózatból nyert forgalommrési eredmény analízise során mutatjuk be.



Trang Dinh Dang was accepted to the Technical University of Budapest on the Faculty of Electrical Engineering and Informatics in 1994. In the autumn semester of 1998 he won the first prize on the Students' Scientific Conference with the topic "On the Analysis of Heavy-tailedness and Self-similarity in Data Traffic" in the Modeling and Simulation Section. Now, as a fifth year student, he is working on his diploma on the topic of Fractal Traffic Modeling in High Speed Networks.



Sándor Molnár received his M.Sc. and Ph.D. in electrical engineering from the Technical University of Budapest, Budapest, Hungary, in 1991 and 1996, respectively. He is an Assistant Professor at the Department of Telecommunications and Telematics, Technical University of Budapest and the research leader of the teletraffic research program of the High Speed Networks Laboratory. He participates in the joint research project on ATM networking between Ericsson Telecom AB, Telia Research AB and HSN Lab, Technical University of Budapest from 1992. Dr. Molnár has been participated in the European project COST 242 and now he is engaged in project COST 257 on "Impacts of New Services on the Architecture and Performance of Broadband Networks" and in IFIP TC6 WG6.3 on "Performance on Communication Systems". His main interests include teletraffic analysis and performance evaluation of modern communication networks with special interest in B-ISDN and Internet.



Attila Vidács was born in Budapest, Hungary, in 1973. He received the M.Sc. degree from the Technical University of Budapest at the Faculty of Electrical Engineering and Informatics, in 1996. He is currently working toward the Ph.D. degree at the High Speed Networks Laboratories, Department of Telecommunications and Telematics of Technical University of Budapest. During 1997, he worked as a visiting researcher at the research and development center of the Nippon Telegraph and Telephone Corp., Tokyo, Japan. He is currently a guest researcher at the Laboratory of Telecommunications Technology of Helsinki University of Technology, Espoo, Finland. His research interests are in the field of teletraffic modeling in high speed networks.

SZABVÁNYOS TESZTSOROZAT ISUP KONFORMACIA TESZTELÉSÉHEZ

DIBUZ SAROLTA

ERICSSON TÁVKÖZLÉSI KFT.
KONFORMANCIA & SZOFTVER TESZT LABORATÓRIUM
1037 BUDAPEST, LABORC U. 1.
SAROLTA.DIBUZ@ETH.ERICSSON.SE

HORVÁTH ENDRE

BUDAPESTI MŰSZAKI EGYETEM
VILLAMOSMÉRNÖKI ÉS INFORMATIKAI KAR
ERICSSON TÁVKÖZLÉSI KFT.
KONFORMANCIA & SZOFTVER TESZT LABORATÓRIUM
HORVATHE@TTT-ATM.TTTBME.HU

Az utóbbi időben a távközlési berendezésekkel szemben támasztott követelmények egyre nagyobbak lettek, és ezek között fontos helyet kap a szabványosság. Mivel a távközlési szolgáltatók különböző cégek különféle termékeit vásárolják, szükségszerű, hogy a különböző protokoll implementációk együttműködjenek. Ez csak akkor lehetséges, ha ezek az implementációk megfelelnek az rájuk vonatkozó kommunikációs protokoll szabványoknak. A konformancia tesztelés célja az, hogy igazolja ezt a feltételt tesztsorozatok futtatása, illetve a válaszsorozatok értékelése által. Mindehhez olyan tesztsorozatra van szükség, amely szabványos és implementáció független, így a kapott eredmények bármikor reprodukálhatóak és összehasonlíthatóak. A tesztsorozat (ATS, Abstract Test Suite – absztrakt tesztsorozat) szabványos leíró nyelve a TTCN (Tree and Tabular Description Language). Az Ericsson Kft. Konformancia és Szoftver Teszt Laborja részt vett egy az ITU számára készülő ATS elkészítésében. Feladatunk TTCN tesztsorozat írása volt ISUP kiegészítő szolgáltatásaihoz (ISUP supplementary services – Q.785.2). A cikk célja az, hogy bemutassa a munka egészét, és az ehhez szükséges elméleti alapokat.

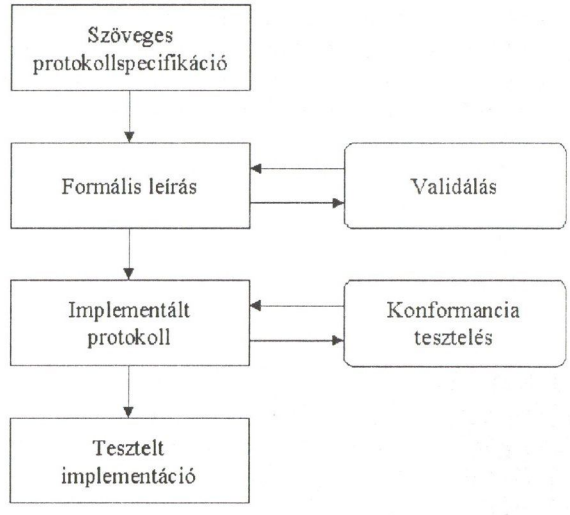
1. BEVEZETÉS

A nemzetközi szabványügyi szervek (ITU-T, ISO) szövegesen specifikálják az egyes protokollokat. Ezek a szöveges leírások részletesek ugyan, mégsem egyértelműek, nem teljesek. Ezért van szükség a protokoll formális specifikálására. A formális leíró technika (Formal Description Technique, FDT) segítségével készíthető el a protokoll egyértelmű, matematikailag egzakt, algoritmizálható modellje.

A protokollmodell logikai helyességét (pl. holtpont mentességét) ellenőrizni kell: a formális specifikálást a validálás (pl. elérhetőségi analízis) követi. A validált protokollspecifikáció már lefordítható valamilyen futtatható nyelvre: ez a fázis az implementáció (megvalósítás). Ezután az implementált protokoll tesztelhető, azaz összehasonlítható a formális specifikációval. Ezt végzi a konformancia tesztelés (alkalmasságvizsgálat), melynek az a feladata, hogy a megvalósított protokoll és az ide vonatkozó szabvány azonosságát egyértelműen igazolja. Ez tesztsorozatok generálása valamint a válaszsorozatok értékelése által történik. Így olyan teszt eredményeket kapunk, melyek összehasonlíthatóak és bármikor megismételhetőek (reprodukálhatóak) [7].

A fentiekben ismertetett életciklus egyes lépéseit az 1. ábra szemlélteti.

A cikk bemutatja az ISUP protokoll kiegészítő szolgáltatásainak konformancia tesztelésére alkalmas absztrakt tesztsorozat (Abstract Test Suite – ATS) készítésének folyamatát, valamint az ATS szimulált környezetben való futtatását (validálását). A cikk 6 fejezetből áll. A bevezetést követő második fejezet ismerteti a munka megértéséhez szükséges legfontosabb alapfogalmakat. Ezt követően a harmadik fejezet rövid áttekintést nyújt magáról a protokollról, és a következő fejezet tárgyalja a munka során alkalmazott eszközöket, környezeteket. Az ötödik fejezet szól a konkrét munkáról, majd a hatodik fejezet tartalmaz egy rövid értékelést az eredményekről, és a munka során szerzett tapasztalatokról.



1. ábra. Protokollok életciklusa

2. KONFORMANCIA TESZTELÉS

Egy adott protokoll szabványt a különböző cégek többféleképpen is megvalósíthatnak. A távközlési szolgáltatók viszont nem csak egy vállalat termékeit vásárolják, így szükségszerű, hogy ezek a különböző implementációk együttműködjenek. Ennek az a feltétele, hogy az implementációk megfeleljenek az ide vonatkozó szabványoknak.

A konformancia tesztelés célja e feltétel egyértelmű igazolása. Ehhez olyan szabványos tesztsorozatra van szükség, amely implementációtól független, és széles körben elfogadott, összehasonlítható eredményre vezet. Ez a tesztsorozat az ATS (Abstract Test Suite), melynek szabványos leíró nyelve a TTCN (Tree and Tabular Combined Notation) [1], [2], [3].

Az ATS a protokoll specifikációjából, illetve az ebből származó tesztcélból (Test purpose) készíthető el. A tesztcél nem más, mint a protokoll működésének szöveges megfogalmazása, lebontva azt a működéskor előforduló kü-

• DPC (Destination Point Code – az üzenet céljának jelzéspont azonosítója).

A Circuit identification code (CIC – áramkör azonosító kód) kijelölése az egyes áramkörökhöz kétoldali megegyezés, és/vagy az alkalmazható, előre meghatározott szabályok alapján történik.

A Message Type Code (üzenettípus kód) egy octet mezőből áll, és minden üzenetben kötelezően jelen van, hogy meghatározza az ISUP üzenet típusát és formáját.

A Mandatory Fixed Part (kötelező, fix hosszúságú rész) olyan paramétereket tartalmaz, melyek mindig jelen vannak az adott üzenetben, és hosszuk állandó. Ezek a paraméterek meghatározott helyen vannak, ezért nincs szükség nevük vagy hosszuk átvitelére.

A Mandatory Variable Part (kötelező, változó hosszúságú rész) változó hosszúságú, kötelező paramétereket tartalmaz. A paraméterek száma és sorrendje meghatározott, és ahogyan az az 4. ábráról is leolvasható, pointerek mutatnak a paraméterek helyére, ahol először a paraméter hossza található, majd ezt követi maga a paraméter.

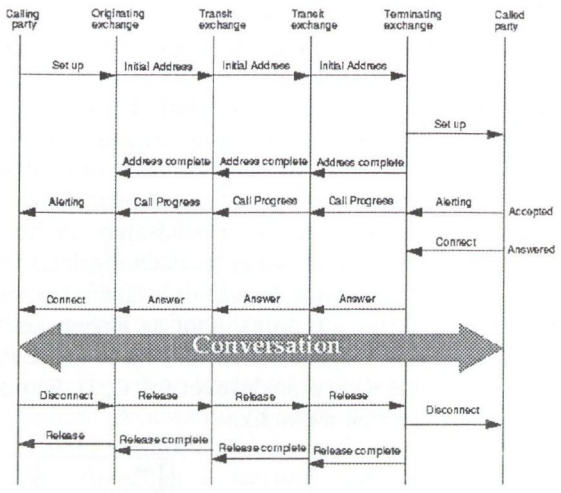
Az Optional Part (opcionális rész) opcionális paramétereket tartalmaz, melyek bizonyos esetekben feltűnnek az üzenetekben, bizonyosakban pedig nem. Az opcionális paraméterek sorrendje nem meghatározott, így minden paraméterinformációt át kell vinni (név, hossz). Az opcionális rész elejére egy pointer mutat, míg a végét egy end of optionals parameters octet jelzi, de csak akkor, ha van az üzenetben opcionális paraméter.

Példaként az 1. táblázat mutatja a Release (REL – lebontás) üzenet paramétereit, ahol F = Fix hosszúságú, kötelező paraméter; V = Változó hosszúságú, kötelező paraméter; O = Opcionális paraméter; @ = nemzeti használatra.

1. táblázat. A Release (REL) üzenet paraméterei

Parameter	Type	Length (octets)
Message type	F	1
Cause indicators	V	3-?
Redirection information @	O	3-4
Redirection number @	O	5-12
Access transport	O	3-?
Signalling point code @	O	4
User-to-user information	O	3-131
Automatic congestion level	O	4
Network specific facility @	O	4-?
Access delivery information	O	3
Parameter compatibility information	O	4-?
Redirect number restrict	O	3
User-to-user indicators	O	3
End of optional parameters	O	1

Ahhoz, hogy a felhasználó számára biztosítani lehessen a távközlési szolgáltatásokat, bizonyos jelzési folyamatokra van szükség, hogy a kapcsolat felépüljön, a szolgáltatás alatt fennmaradjon, és azután lebontódjon. Különböző szolgáltatásokhoz különböző, jól meghatározott jelzési szekvenciákra van szükség, de az érvénytelen jelzési szekvenciák kezeléséről is gondoskodni kell. Az 5. ábrán látható egy példa a jelzési folyamatra, amely egy egyszerű ISDN hívást épít fel, majd bont le.

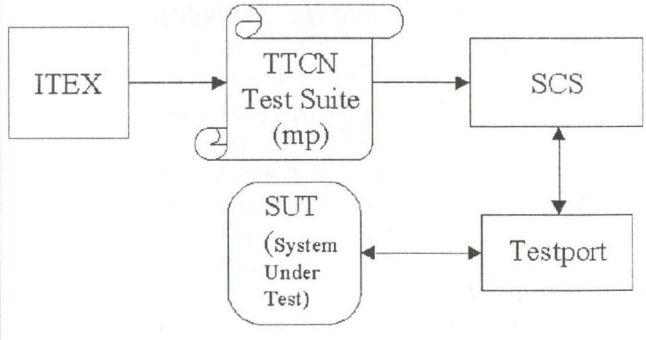


5. ábra. Egy sikeres hívás felépítése és lebontása

4. A TESZTSOROZAT KÉSZÍTÉS ÉS FUTTATÁS ESZKÖZEI - A TTCN PLATFORM

A TTCN platform (TTCN alapcsomag) azoknak az eszközöknek az együttese, melyeket az ATS írásához és végrehajtásához használtunk (6. ábra). Egy részét az Ericssonnál fejlesztették, míg a másik része vásárolt, kereskedelmi termék.

A tesztelés folyamata a tesztsorozat írásával kezdődik, melynek eszköze az ITEX (Interactive TTCN Editor and Executor). A folyamat végeredménye egy mp file (az ITEX generálja), amely a tesztsorozat ASCII formátumú leírása. Ezt kell ezután betölteni a tesztkörnyezetbe, melynek neve SCS (System Certification System). Az SCS és a SUT (System Under Test) közötti adaptáció un. Test Portok meghívásával történik, mivel ezek tartalmaznak minden protokoll specifikus információt.



6. ábra. A TTCN platform

4.1. ITEX: a TTCN editor

Az ITEX (Interactive TTCN Editor and Executor) egy eszközcsalád TTCN tesztsorozatok készítéséhez, szintaktikai vizsgálatához. Az ITEX egy modern, grafikus, X-Window alapú felhasználói interfészt jelenít meg, amely menük, dialógus ablakok és editorok együtteséből áll [10].

AZ ITEX Browser eszközével lehet a teljes tesztsorozatot, illetve annak csak egyes részeit áttekinteni. A Browser

minden olyan statikus elemét megjelenít a tesztsorozatnak, amely a TTCN szabványban definiálva van, sőt ezeket a statikus elemeket egy új tesztsorozat létrehozásakor automatikusan generálja. Ilyen statikus elem például az áttekintő rész, deklarációs rész, constaints rész, dinamikus rész, melyeket a felhasználó nem változtathat. Ezzel ellentétben a dinamikus elemeket (lényegében a táblákat, csoportokat), a felhasználó adja a tesztsorozathoz, illetve editálhatja, törölheti azokat.

Az ITEX lehetővé teszi a tesztsorozat teljes szintaktikai analízisét az Analizáló eszköz segítségével, amely ezenfelül számos statikus szemantikai vizsgálatot is végrehajt (ezzel főleg azonosítók létezését és egyediségét vizsgálja).

A tesztsorozat áttekintését, nyomon követését számos további eszköz támogatja. Lehetőség van például az egymásra hivatkozó táblák közötti egyszerű átjárásra a hivatkozási szövegrészek kijelölése által.

A ITEX editor a tesztsorozatot grafikusan jeleníti meg (TTCN.GR formátum). Ez könnyű áttekintést és editálást biztosít ugyan, de a grafikus formátum nem futtatható, ezért az ITEX megengedi a tesztsorozatok exportálását futtatható, TTCN.MP formátumú file-ba, mely a konformancia teszterek bemenete. Ez a folyamat minden megkötés nélkül történik, függetlenül a tesztsorozat vizsgálati státuszától, teljességétől, hibamentességétől.

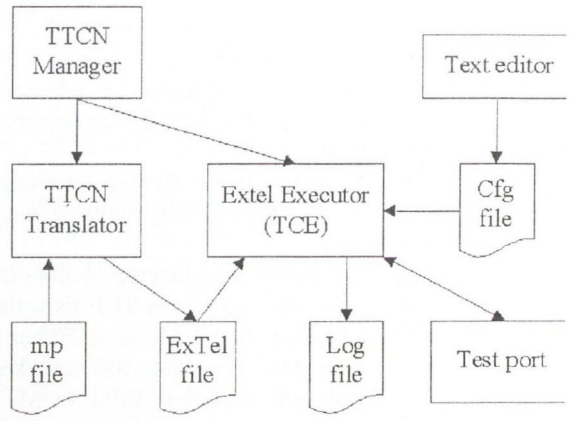
Az ITEX több eszközzel támogatja nagy tesztsorozatok elosztott fejlesztését. Így lehetőség nyílik tesztsorozatok összehasonlítására, illetve egy teljes tesztsorozat, vagy csak egy részének egy másik tesztsorozattal való egyesítésére.

Az editor egy további fontos eszköze a TTCN Link. Ez egy olyan környezet, mely TTCN tesztsorozatok hatékony, SDL specifikáción alapuló készítését támogatja. A Link összeköttetést biztosít az SDL specifikáció, és a TTCN tesztsorozat között. Összehasonlítva a manuális tesztsorozat készítéssel, növeli a termelékenységet a tesztsorozat statikus részeinek automatikus generálásával, valamint a specifikáció alapú test case tervezés támogatásával.

4.2. SCS: a tesztelés eszköze

Az SCS (System Certification System) a tesztsorozat végrehajtó platformja (7. ábra). Bemenete az ITEX editor által generált mp file, melyet a Translator (fordító) ExTeL (Executable Test Language) file-lá konvertál. Ez az ExTeL file a TCE (Test Component Executor) által már közvetlenül futtatható. Ez a módszer lényegesen leegyszerűsíti a TTCN tesztsorozat futtathatását, hiszen, ellentétben más fordító módszerekkel, csak egy fázisra van szükség a tesztsorozat futtathatóvá alakításához.

Egy másik nagyon fontos jellegzetesség az SCS-ben a tesztport koncepció. A tesztport a TCE-t illeszti az IUT-hez, biztosítva ezzel a TCE protokollfüggetlenségét. Ezzel a megoldással lehetőség nyílik az alapfunkciók elkülönített fejlesztésére anélkül, hogy a már meglevő tesztportokat ez érintené. A Test Port Interface (TPI), amely a tesztportok és a TCE közötti interfészt jelenti, lehetővé teszi új tesztportok hozzáadását a rendszerhez. Az új tesztportok szerkesztését egy olyan eszköz teszi könnyebbé, amely egy tesztport vázat generál, és ez a váz szolgál alapul a tesztport végső megvalósításához. Így aztán néhány apró konfigurációs beállítás után az új tesztport máris alkalmazhatóvá válik az SCS-ben [11].



7. ábra. Az SCS eszközök struktúrája

A TTCN Manager az SCS, Sun OpenLock környezetben kifejlesztett, grafikus felhasználói interfésze. Feladata, hogy egyszerű hozzáférést biztosítson a különböző funkciókhoz, melyek a TTCN tesztsorozat előkészítéséhez, szintaktikai vizsgálatához és futtatásához szükségesek, valamint naplózza a szintaktikai vizsgálatok eredményét és a futtatási eseményeket is. E célból a TTCN Manger interfésszel rendelkezik a TTCN Editor, a TTCN Translator (fordító), a Test Component Executor (TCE), a Konfiguráció Editor és a Log (napló) Monitor felé.

A TTCN Manager segítségével interaktív futtatás is megvalósítható: lehetőség van a tesztsorozatban az események szekvenciájának megválasztására, paramétereik megváltoztatására, és a tesztsorozat ilyen módon való futtatására. Az interaktív futtatás alatt futó teszt szekvenciákból aztán lehetséges új tesztsorozat létrehozására is.

A translator (fordító) egy olyan UNIX program, amely a gép által feldolgozható, mp formátumú file-t kap a bemenetére, és ebből a TCE által futtatható, ExTeL formátumú file-t készít.

A TCE is egy UNIX program. Bemenetére egy ExTel file-t kap, ezt futtatja, és a folyamatról log (napló) file-t készít. A futtatáshoz, a teszt rendszer konfigurálásához több konfigurációs file-ra is szüksége van: teszt konfigurációs file, tesztport konfigurációs file(ok), PDU kódoló/dekódoló file(ok).

A PDU kódoló/dekódoló kódolja a TCE által az IUT-nek küldött üzeneteket (PDU-k), valamint dekódolja az IUT-tól kapottakat.

A TCE-t teszt port illeszti a tesztelendő rendszerhez (SUT). A TCE ugyanakkor rendelkezik számos beépített tesztporttal is, melyeket a különböző applikációk használhatnak.

Az SCS eszközök használatának fő célja az, hogy TTCN tesztsorozatokat futtatni lehessen bizonyos külső vagy belső interfészek felé. Ez a cél az SCS eszközökkel úgy valósítható meg, hogy lehetőség adódik a platformhoz új interfészillesztők hozzáadására anélkül, hogy szükséges lenne a TTCN tesztsorozatot futtató TCE központi részének megváltoztatása. Ezeket az interfészillesztőket tesztportoknak hívják, és a működés megkezdésekor dinamikusan kapcsolódnak a TCE-hez. Minden interfész típushoz, ahol igény van a TTCN használatára, tesztportot kell készíteni. A tesztport feladata az, hogy biztosítsa az TCE és az IUT interfésze közötti kommunikációt.

A tesztport működéséhez szükség van az aktuális konfigurációt leíró adatokra, melyek a tesztport konfigurációs file-ban találhatók. Ez a file egy konfigurációs eszköz segítségével hozható létre, ami az esetek túlnyomó részében egy egyszerű szöveg editor.

Lehetőség van a tesztporton belül történő események naplózására is: a tesztport létrehoz egy napló file-t, a nyomon követés céljából.

Az ISUP protokoll teszteléséhez szükséges további eszköz az ISUP tesztport. Ez a tesztport is a TCE és a tesztelendő rendszer (SUT) közötti adaptációt végzi. Ebben az esetben a SUT például az APZ Emulátor SS7 applikációja, amely magába foglalja SS7 protokoll ISUP és MTP3 rétegét egyaránt. Ezért a teszthez szükség van egy MTP3 tesztportra is.

Az MTP3 tesztport a TCE és az SUT közötti kapcsolatot biztosítja az MTP3 szerver segítségével. A szerver egy olyan UNIX program, amelyik a MTP3 tesztportot köti össze az SUT-vel, biztosítva ezzel a tesztsorozat futtatását az IUT felé. Az SUT lehet például az APZ emulátor SS7 applikációja vagy egy valós implementáció (AXE), melyek magukba foglalják az SS7 MTP3 rétegét, és a tesztelendő protokollréteget.

A tesztport MTP3 felső réteghatári primtíveket kínál a tesztsorozat felé, míg az SUT-val MTP3 alsó réteghatári primtívekkel kommunikál.

5. A TESZTSOROZAT KÉSZÍTÉSE ÉS VALIDÁLÁSA

5.1. Az ATS készítése

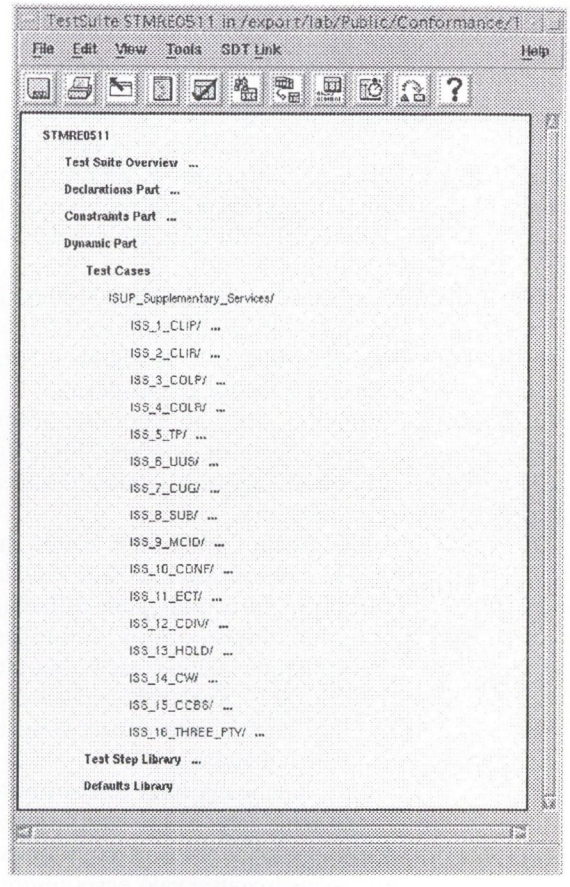
Mint azt már a bevezetőben is említettük, a magyarországi Ericsson Kft. Konformancia és Szoftver Teszt Laborjának feladata egy ATS írása volt ISUP Supplementary Services (kiegészítő szolgáltatások) konformancia teszteléséhez [8].

Egy ATS írásánál a protokoll formális leírásából származtatott test purpose-ből (tesztcélból) kell kiindulni, és az egyes test case-eket (teszteseteket) úgy kell megírni, hogy azok az ide vonatkozó tesztcélt valósítsák meg. Mi az ETSI által kiadott test purpose-t vettük alapul, és így a 8. ábrán látható test case csoportokat implementáltuk az ITEX editor segítségével. Ezek a test case csoportok az egyes ISUP kiegészítő szolgáltatásoknak felel meg, és minden egyes csoport számos test case-t tartalmaz, összesen kb. 400-at.

A test case-ek készítését egy egyszerű példán, a CLIP/CLIR szolgáltatásokon keresztül szeretnénk bemutatni. A CLIP (Calling Line Identification Presentation) a hívó fél azonosításának lehetőségét biztosítja a hívott fél számára, és ez alkalmazható az összes telekommunikációs szolgáltatásban. Ez az átvitt információ tartalmazza a hívó fél ISDN számát. A CLIR (Calling Line Identification Restriction) pedig a CLIP szolgáltatás letiltása, amely jelenthet állandó, vagy csak az egyes hívásokhoz kapcsolódó azonosítás megtagadást [5].

5.1.1. A Test Purpose (tesztcél)

Egy példa a tesztcél megvalósítására:
a CLIP ISS_V_1_7-es sorszámú test purpose-t a 2. táblázat mutatja [4].



8. ábra. Az ATS test case csoportjai

2. táblázat. Egy test purpose formátuma

TSS	TP	ISUP'97 reference	Selection expression	Q.788 reference
CLIP/	ISS_V_1_7	3.4, 3.5.2.2.1 /Q.731	Transit	None

Test purpose

Passing on the calling party number and the generic number

To verify that a calling party number and additional calling party number in the generic number can be successfully transferred to the succeeding exchange.

Pre-test conditions

SPC SPA SPB
-------IAM------> -------IAM------>

1 The PTC will initiate a call set up with the expected parameters

A táblázat alapján a tesztcél ennél a példánál az, hogy megvizsgáljuk egy tranzit központ esetében azt, hogy a hívó fél száma az általános számban sikeresen átvihető-e. Mint az a 2. táblázatból is kiolvasható, a tesztcél nem specifikálja egzakt módon a PDU-kat és azok pontos szekvenciáját, ezért szükség van a szabvány ismeretére is a tesztcél megvalósításához.

5.1.2. Az adott tesztcélt megvalósító Test Case (teszteset)

Az 1_7-es tesztcélt a 9. ábrán látható test case valósítja meg.

Test Case Dynamic Behaviour

Test Case Name: ISS_V_1_7_IUT_passes_generic_number_in_IAM
Group : ISUP_Supplementary_Services/ISS_1_CLIP/
Purpose : To verify that the calling party number and additional calling party number in the generic number can be successfully transferred to the succeeding exchange
Configuration : MTC_and_two_ISUP_PTCs
Default :
Comments : REFERENCE: 3.4;3.5.2.2.1/ Q.731
Selection Ref : Transit
Description : IUT passing additional calling number

Nr	Label	Behaviour Description	Constraints Ref	Verdict	Comments
1		+preamble			
2		CREATE (A_ISUP_PTC:A_call_setup, B_ISUP_PTC:B_call_setup)			
3		?DONE (A_ISUP_PTC, B_ISUP_PTC)			
4		+check_communication			
5		CREATE (A_ISUP_PTC:A_call_release, B_ISUP_PTC:B_call_release)			
6		?DONE (A_ISUP_PTC, B_ISUP_PTC)			
7		+check_idle			
8		+postamble			Sets final verdict
		A_call_setup			
9		+A_SEND (IAM_s_AB_Generic_number (TCV_A_cic))			
10		+A_RECEIVE (ACM_m(TCV_A_cic))			
11		+A_RECEIVE (ANM_m (TCV_A_cic))			
		A_call_release			
12		+A_RECEIVE_CALL_REL			
		B_call_setup			
13		+B_RECEIVE_cic (IAM_r_AB_Generic_number (*,*,B))			
14		+B_SEND (ACM_m(TCV_B_cic))			
15		+B_SEND (ANM_m (TCV_B_cic))			
		B_call_release			
16		+B_SEND_CALL_REL			

9. ábra. Az ISS_V_1_7-es tesztcélt megvalósító test case

A 3. fejezetben már szó volt a dinamikus viselkedés táblázatos leírásáról. Az időbeliséget, amint az a 9. ábrán látható, az egyes sorok helyzete reprezentálja: annál később hajtódik végre egy sor, minél beljebb kezdődik (balról jobbra haladva), így a párhuzamos események azonos bekezdéssel szerepelnek.

A test case tesztlépéseket (test step) hív meg (a + jel jelöli a tesztlépéseket). A test case keretét két tesztlépés adja: a preamble, amely a teszthez szükséges állapotba állítja az IUT-t, és a postamble, amely visszaállítja az IUT kezdeti állapotát, valamint meghozza a végső döntést a teszt sikerességéről (Pass, Fail, Inconclusive).

A TTCN lehetővé teszi tesztsorozat elemek párhuzamos végrehajtását tesztkomponenseken keresztül. A 9. ábrán látható test case, két párhuzamos ISUP tesztkomponenst tartalmaz, hiszen ebben az esetben tranziens központot vizsgálunk. Az ATS-ben természetesen több tesztkomponenst (ISUP, Access) is definiáltunk. Ezek típusa a tesztelendő objektumtól függ (Lokális központ, Tranzit központ...), és ezt az információt a PICS tesztdokumentum tartalmazza. Arról pedig, hogy ez a test case valóban csak tranziens központ esetén fusson, a Selection Ref mező tartalma (Transit) gondoskodik (hivatkozva a PICS-re).

A 9. ábrán látató test case működését tekintve két részből áll: az első fázisban az A oldal kezdeményezése nyomán a kapcsolat-felépítés (Call Setup) megy végbe, majd a második fázisban a B oldal kezdeményezésére megtörténik a kapcsolatlebontás (Call Release).

A kapcsolat-felépítés egy IAM üzenet küldésével kezdődik (az A oldalon), amely jelen esetben az A_SEND tesztlépés meghívását jelenti az IAM_s_AB_Generic_number paraméterrel. Az A_SEND tesztlépés az 10. ábrán látható.

Test Step Dynamic Behaviour

Test Step Name: A_SEND (sendmsg:PDU)
Group : Common_steps/
Objective :
Default :
Comments :
Description : General message sequence send MSG. Message constraint delivered as parameters

Nr	Label	Behaviour Description	Constraints Ref	Verdict	Comments
1		A_PCO ! M_TRANSFERreq	A_send (sendmsg)	(P)	

Detailed Comments:

10. ábra. Az A_SEND tesztlépés

Az A_SEND tesztlépés működése igen egyszerű: az A_PCO-n küld egy ASP-t (a küldés jele:!), melynek adatmezőjébe (11. ábra) kerül a test case által meghívott IAM üzenet. A többi adatmező értékét pedig az A_send constraint deklarációs táblája írja le, melyre a Constraints Ref mezőben hivatkozik a tesztlépés.

ASP Type Definition

ASP Name: M_TRANSFERreq(MTP_TRANSFER_Request)
PCO Type : ISUP_PCO
Comments: MTP ASP for sending ISUP messages
FS : 2.1 / 61/155.17-CRT 212 31 Uen Rev. A

Parameter Name	Parameter Type	Comments
sio	SIO	Service information octet
opc	INTEGER	Originating point code (Field of routing label)
dpc	INTEGER	Destination point code (Field of routing label)
sls	INTEGER	Signalling link selection (Field of routing label)
data	PDU	ISUP signalling message

Detailed Comments:

11. ábra. Az üzenethordozó ASP típus definíciós táblája

Az A oldal által küldött IAM-et ezután a B oldal fogadja (9. ábra, B_RECEIVE_cic tesztlépés), majd a B_SEND tesztlépéssel (a B_PCO-n) egy ACM-et, majd egy ANM-et küld az A oldalnak. Ezt a két üzenetet az A oldal a 12. ábrán látható A_RECEIVE tesztlépés meghívásával fogadja.

Test Step Dynamic Behaviour

Test Step Name: A_RECEIVE (receivemsg:PDU)
Group : Common_steps/
Objective :
Default :
Comments :
Description : General message sequence send MSG, receive MSG. Message constraints delivered as parameters

Nr	Label	Behaviour Description	Constraints Ref	Verdict	Comments
1		START T_A_STEP			
2		A_PCO ? M_TRANSFERind CANCEL T_A_STEP	A_receive (receivemsg)	(P)	
3		? TIMEOUT T_A_STEP		(F)	
4		A_PCO ? OTHERWISE CANCEL T_A_STEP		(F)	

Detailed Comments:

12. ábra. Az A_RECEIVE tesztlépés

A tesztlépés elindít egy időzítőt (T_A_STEP), és az A_receive constraints definíciós táblában leírt paraméterekkel vár (a fogadás jele: ?) egy ASP-t (11. ábra) az A_PCO-n. Amennyiben az időzítő lejárta előtt megérkezik az ASP, benne a test case-ben várt PDU-val, az ítélet: Pass (az időzítő leáll), ha viszont nem jön semmi (az időzítő lejár), illetve nem a várt üzenet jön, az ítélet: Fail.

Az ANM vételével (ha sikeresen eljutott a teszt idáig) a hívás most felépült, így következhet a második fázis: a hívás lebontása. A bontási folyamatban is ugyanaz a két tesztkomponens vesz részt, de ebben az esetben a B oldal kezdeményezi a bontást a B_SEND_CALL_REL tesztlépéssel (13. ábra).

Test Step Dynamic Behaviour

Test Step Name: B_SEND_CALL_REL
Group : Common_steps/
Objective :
Default :
Comments :
Description : General send REL receive RLC from B side of the call.

Nr	Label	Behaviour Description	Constraints Ref	Verdict	Comments
1		B_PCO ! M_TRANSFERreq START T_B_STEP	B_send (REL_m (TCV_B_cic))		
2		B_PCO ? M_TRANSFERind CANCEL T_B_STEP	B_receive (RLC_m (TCV_B_cic))	(P)	
3		?TIMEOUT T_B_STEP		(F)	
4		B_PCO ? OTHERWISE CANCEL T_B_STEP		(F)	

Detailed Comments:

13. ábra. A B_SEND_CALL_REL tesztlépés

Ez a tesztlépés két feladatot is ellát. Először egy Release (bontás – REL_m) üzenetet küld az A oldalnak (a B_send constraints definíciós táblában leírt paraméterekkel), majd egy időzítő elindítása után (T_B_STEP) az A oldal felől vár egy Release Complete (RLC_m) üzenetet (a B_PCO-n). Ha az időzítő lejárta előtt megérkezik a B_receive constraints definíciós táblában leírt ASP, benne az RLC_m PDU-val, akkor a hívás lebontása sikeresen befejeződött (Pass), ellenkező esetben pedig az ítélet: Fail.

Természetesen az A oldalon az A_RECEIVE_CALL_REL tesztlépés első lépésként a B oldal felől vár egy Release-t (az A_PCO-n), majd erre egy Release Complete üzenettel válaszol (14. ábra).

Test Step Dynamic Behaviour

Test Step Name: A_RECEIVE_CALL_REL
Group : Common_steps/
Objective :
Default :
Comments :
Description : General receive REL send RLC from B side of the call

Nr	Label	Behaviour Description	Constraints Ref	Verdict	Comments
1		START T_A_STEP			
2		A_PCO ? M_TRANSFERInd CANCEL T_A_STEP	A_receive (REL_m (TCV_A_cic))		
3		A_PCO ! M_TRANSFERreq	A_send (RLC_m (TCV_A_cic))	(P)	
4		? TIMEOUT T_A_STEP		(F)	
5		A_PCO ? OTHERWISE CANCEL T_A_STEP		(F)	

Detailed Comments:

14. ábra. Az A_RECEIVE_CALL_REL tesztlépés

A 3. fejezetben említetünk egy példát az ISUP PDU-k felépítésére: az ott található 1. táblázat mutatja a Release (bontás) üzenet paramétereit. Ennek megfelelően az ATS-ben megvalósított Release (REL) PDU definíciós táblája a 15. ábrán látható.

ASN.1 PDU Type Definition

PDU Name : REL
PCO Type : ISUP_PCO
Encoding Rule Name:
Encoding Variation :
Comments : Release (TABLE 33 / Q.763)
ES 201 233 / 61/TSS 17 CRT 212 31 Uen Rev A

Type Definition

```
SEQUENCE {
cic                 Circuit_identification_code ,
messageType         Message_type ,
var_part_ptr        OCT_1,
opt_part_ptr        OCT_1,
causeInd            Cause_indicators ,

relOptionals SET {

redirectingInfo     Redirection_information          OPTIONAL ,
redirectionNum      Redirection_number               OPTIONAL ,
accessTransport     Access_transport                 OPTIONAL ,
sigPointCode        Signalling_point_code            OPTIONAL ,
userToUserInfo      User_to_user_information         OPTIONAL ,
autCongLevel        Automatic_congestion_level       OPTIONAL ,
networkFacility     Network_specific_facility        OPTIONAL ,
accessDeliveryInfo  Access_delivery_information      OPTIONAL ,
paramCompatibilityInfo Parameter_compatibility_information OPTIONAL ,
redirectionNumRest  Redirection_number_restriction   OPTIONAL ,
userToUserInd       User_to_user_indicators          OPTIONAL
} OPTIONAL ,

endOfOp             OCT_1  OPTIONAL
}
```

Detailed Comments: relOptional is not a real ISUP parameter, but a "virtual parameter" for testing of optional parameters and for negative testing.

15. ábra. A release PDU definiálása TTCN táblával

Az előzőleg bemutatott tesztlépések a REL_m PDU constraint-et használják, amely az 15. ábrán látható PDU típus által definiált paramétereknek ad konkrét értéket (esetünkben csak a kötelező paramétereknek, erre utal az „_m" végződés).

Jóllehet, az általunk bemutatott test case csak két PCO-t használt (A_PCO, B_PCO), természetesen az ATS-ben más PCO-k is előfordulnak (16. ábra) attól függően, hogy milyen központot tesztelünk.

PCO Declarations

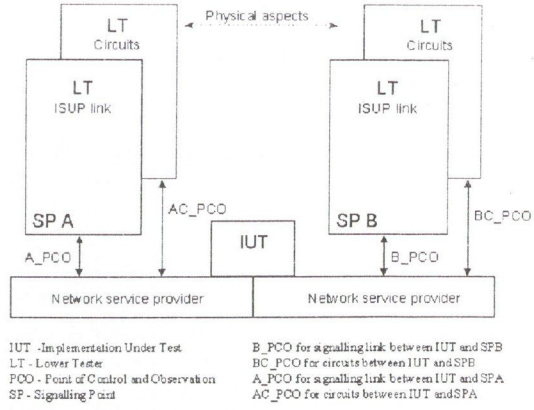
PCO Name	PCO Type	Role	Comments
A_PCO	ISUP_PCO	LT	Signalling link A subscriber
B_PCO	ISUP_PCO	LT	Signalling link B subscriber
A_ACCESS_PCO	ACCESS_PCO	LT	Access link A subscriber
M_PCO	MAINT_PCO	UT	PCO for main test component
A_PSTN_PCO	PSTN_PCO	LT	PSTN link
A_SCCP_PCO	TCAP_PCO	LT	SCCP link for TCAP messages
A_NON_ISUP_PCO	NON_ISUP_PCO	LT	Non ISUP PCO

Detailed Comments:

16. ábra. Az ATS-ben használt PCO-k

5.1.3. A tesztkonfiguráció

Már említettük, hogy a bemutatott test case Transit központot tesztel, ezért van szükség két ISUP PCO-ra. Ennek a tesztkonfigurációját a 17. ábra mutatja.



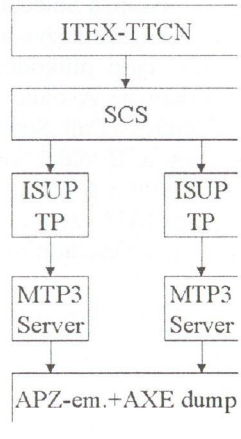
17. ábra. A tesztkonfiguráció tranzit központ esetén

Két párhuzamos tesztkomponens (alsó teszter – LT ISUP link) teszteli az ISUP jelzésüzeneteket, valamint a másik két tesztkomponens (LT circuits) a felépült beszédkapcsolat tesztelésére alkalmas.

Helyi központ esetében viszont a központ egyik oldalán access protokollt kell alkalmazni, melyet mi DSS1 L3 protokollal implementáltunk [6], és ehhez értelemszerűen ACCECC PCO-ra van szükség.

5.2. Az ATS validálása

Az ATS validálása és a konformancia tesztelés két ellentétes célú folyamat. Míg a konformancia tesztelés során az ATS futtatásával az adott implemenációt (terméket) szeretnénk vizsgálni, az ATS validálásakor magának a tesztsorozatnak a megfelelő működését ellenőrizzük (feltételezve, hogy a környezet, ahol a tesztsorozat fut, hibátlanul működik). Így az ATS-t, miután elkészült, szimulált környezetben (18. ábra) futtattuk az APZ emulátor segítségével, ahol az IUT az AXE dump volt, melyet hibamentesnek tételeztünk fel. Ebből következően, ha bármilyen Fail ítéletet kaptunk, akkor a hibát az adott test case-ben kellet keresni. Az esetleges hiba behatárolásához a szimulációs eredményeket tároló log-file-okat elemeztük [8].



18. ábra. A szimulált környezet felépítése

A validálás megkezdése előtt az ATS-ből futtatható, mp file-t készítettünk, az ITEX editor segítségével. Ezek után kezdődhetett a validálás folyamata, melynél a 4. fejezetben ismertetett SCS Test Manager-e biztosította számunkra a kezelő felületet.

Az mp file-t betöltöttük a Test Manager-be, így lehetőség nyílott az egyes test case-ek kiválasztására, futtatására. A Test Manager lehetővé teszi az összes test case, vagy csak a felhasználó által kijelölt test case-ek futtatását is.

A validálás folyamata valós időben log-ablakokon követhető nyomon, melyek a futtatás után naplófile-ok formájában is rendelkezésre állnak. Minden egyes, a test case-ben használt tesztkomponenshez tartozik egy napló-ablak (ill. file). A log-file-ok az események időpontját, valamint az egyes részekhez tartozó ítéleteket is tartalmazzák, így a fellépő hibák okai könnyen megtalálhatók, és a rögzített időpontok alapján jól nyomon követhető az események sorrendje. A file tartalmazza továbbá az üzenetek pontos tartalmát is. Ez sok segítséget nyújt a test case-ek javításában. Ha például egy üzenet vételekor Fail ítéletet kapunk, a vett üzenet tartalmát összevetve az általunk várt üzenettel kiderülhet, hogy az adott test case-ben rossz paraméterérték szerepel. Így aztán az ilyen, és ehhez hasonló hibák könnyen kijavíthatók.

6. ÖSSZEGZÉS

A Konformancia és Szoftver Teszt Labor által végzett munka része volt az ITU (International Telecommunication Union) számára az ISUP protokoll konformancia teszteléséhez alkalmas szabványos tesztsorozat készítésének, így a project végeredménye egy szabványos formátumú absztrakt tesztsorozat lett. A Labor maga is végez konformancia tesztelést az elkészült ATS segítségével, de mint szabványos tesztkészletet más gyártók is használják termékeik konformancia tesztelésére. Így a tesztkészlet olyan implementáció független konformancia tesztelést tesz lehetővé, amely bármikor rekonstruálható és összehasonlítható eredményre vezet. Mindez azért nagyon lényeges, mert a távközlési piac deregularizációjában a különböző szolgáltatók eszközeinek összekapcsolásakor végzett Interconnect eljárásoknak fontos eleme a konformancia tesztelés, mely nagy mértékben növeli a hálózati elemek együttműködésének valószínűségét.

IRODALOM

[1] Bernd Baumgarten, Alfred Giessler: OSI Conformance Testing Methodology and TTCN, 1994

[2] ITU-T Recommendation X.290-296 Data Networks and Open System Communications
Open System Interconnection – Conformance Testing

[3] ISO/IEC 9646 Information technology – Open Systetems Inteconnection – Conformance testing methodology and framework

[4] ITU-T Recommendation Q.785.2 ISUP protocol test specification for supplementary services

[5] ITU-T Recommendation Q.731 Stage 3 Description for number identification supplementay services using Signalling System No.7

[6] ITU-T Recommendation Q.931 Digital Subscriber Signalling System No. 1 (DSS 1) – ISDN User-Network Interface Layer 3 Specification for Basic Call Controll

[7] Tarnay Katalin: Protokollok Specifikálása és Tesztelése. *Híradástechnika*, 1992. agusztus

[8] Horváth Endre: TTCN tesztsorozat készítése ISUP konformancia teszteléséhez, BME Villamosmérnöki és Informaikai kar TDK Konferencia 1998

[9] Travis Russel: Signaling System #7, 1995

[10] Anders Ek: Testing and Test Generation: State of the Art and Future Expectations 11th Intenational Workshop on Testing of Communicating Systems (IWTCS '98)

[11] SCS User's Guide, Technical Report Ericsson, 1997

STANDARDISED TEST SUITE FOR ISUP CONFORMANCE TESTING

S. DIBUZ

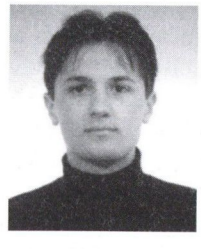
ERICSSON TELECOMMUNICATIONS LTD.
CONFORMANCE & SOFTWARE TEST LAB
H-1037 BUDAPEST, LABORC U. 1.
SAROLTA.DIBUZ@ETH.ERICSSON.SE

E. HORVÁTH

TECHNICAL UNIVERSITY OF BUDAPEST
ERICSSON TELECOMMUNICATIONS LTD.
CONFORMANCE & SOFTWARE TEST LAB
HORVATHE@TTT-ATM.TTT.BME.HU

The main aim of conformance testing is to provide comparable and repeatable test results for the products produced by different vendors. These test results show the conformity of the product to the relevant communication standards, and are the basis of the interconnection with other products. More customers require the test results especially as interconnection of different service providers is more important in the deregularised market. Ericsson is handling into ITU-T an ATS (Abstract Test Suite) for Q.785.2 (ISUP supplementary services) which is written in the standardised TTCN (Tree and Tabular Combined Notation) format. Conformance & Software Test Lab took part in the preparation of the ATS and here we describe the most important steps of this work and the theoretical basis of Conformance Testing.

Dibuz Sarolta a Budapesti Műszaki Egyetem Villamosmérnöki karának Híradástechnika szakán szerzett diplomát 1986-ban. 0986-1991 között doktori ösztöndíjasként dolgozott a KFKI-MSZKI-ban. 1991-ben egyetemi doktori fokozatot, majd 1994-ben kandidátusi fokozatot szerzett, szakterülete kommunikációs protokollok specifikálása és tesztelése. 1992-ben Köztársasági aranygyűrűvel tüntették ki. 1994-től az LNX Kft-ben elektronikus adatcserével foglalkozott. 1997-től az Ericsson Távközlési Kft. Kutatólaboratóriumában a Konformancia Központ vezetője. Részt vesz a konformancia és szoftver tesztelés területén folyó kutató munkában, több Ph.D. és diplomaterv témát irányít.



Horváth Endre a Budapesti Műszaki Egyetem Villamosmérnöki és Informatikai karának ötödéves, távközlés és telematika szakos hallgaótja. 1998-tól az Ericsson Kft. Konformancia & Szoftver Teszt Laboratóriumában dolgozik részmunkaidőben. A BME Villamosmérnöki és Informatikai karának 1998-as TDK konferenciáján első díjat nyert a „TTCN tesztsorozat készítése ISUP konformancia teszteléséhez" c. dolgozatával. Jelenleg diplomamunkáját készíti, melynek témája tesztsorozat készítése QSIG protokollhoz.

OLIGOPOL PIACI STRUKTÚRÁK ELEMZÉSE JÁTÉKELMÉLETI ESZKÖZÖKKEL

FUTÓ PÉTER és TŐKEY ZOLTÁN

BUDAPESTI MŰSZAKI EGYETEM
BUDAPESTI MŰSZAKI EGYETEM
VILLAMOSMÉRNÖKI ÉS INFORMATIKAI KAR, TÁVKÖZLÉS ÉS TELEMATIKA TANSZÉK
1111 BUDAPEST, EGRY J. U. 18.

A cikk az oligopol elmélet és különböző modelljeinek tárgyalását mutatja be. A duopol együttműködés fogolydilemmája és az individuális–kollektív racionalitás diergenciájának bemutatása is részletes kibontásra kerül. Végül a belépés, alkalmazkodás és kilépés témaköreinek rövid feldolgozása következik.

1. A TÁVKÖZLÉSI SZEKTOR

A távközlési szektor napjainkra annyira összetetté vált, hogy vizsgálata során célszerű azt egymással csak kevéssé összefüggő részeire bontani. Ez azonban kompromisszumokra kényszerít bennünket, a szektor felosztásánál – a vizsgált piacok kijelölésénél – célszerű az egyszerűségre törekednünk. Az általunk használt két nagy kategória az adat- és beszédátvitel piaca. Az adatátvitel esetében szélessávú, nem valósidejű, nagy megbízhatóságú; a beszéd esetén keskenysávú, valósidejű, nagyobb hibatűrésű átvitelt értünk. Ezt az első pillanatra merevnek tűnő elhatárolást az indokolja, hogy a két piac közt a szükségletek helyettesíthetősége igen alacsony, azonban az egyes piacokon (beszéd, adat) belül az egyes szegmensek (pl. beszéd esetében a fix, ill. mobil telefon) egymásra való hatása igen erőteljes, a szolgáltatások nagyban helyettesíthetik egymást. Így a két piac egymástól függetlenül tárgyalható, a piacokon belüli további felosztás ugyanakkor erőltetetté válna, és téves következtetésekre vezetne.

Most már rátérhetünk a piaci szerkezetek vizsgálatára, ez két dolgot takar: a piaci szereplők számát és azok egymáshoz való viszonyát.

2. OLIGOPÓLIUMOK ÉS MODELLEZÉSÜK JÁTÉKELMÉLETI ESZKÖZÖKKEL

Tisztán kompetitív, illetve monopol piac a valóságban igen ritka, a megfigyelhető piaci szerkezetek általában a két szélsőséges eset közt helyezkednek el: amikor a piacon csak néhány (kevés) vállalat biztosítja az összpiaci keresletet, akkor beszélünk oligopol piaci struktúráról. A távközlési piacok ez utóbbi kategóriába tartoznak a fent kialakított elhatárolás alapján.

Az oligopol piaci szerkezetet a kevés résztvevőn túl a kölcsönös függőség jellemzi: az egyes vállalatok kínálati árai és mennyiségei befolyásolják az összpiaci kínálat és ár alakulását és ezen keresztül egymás viselkedését. A távközlési szektorban a vállalatok kölcsönös függőségét erősíti a rá jellemző hálózatos struktúra. Minden vállalatnak figyelemmel kell kísérnie, saját döntéseiben számításba kell vennie a versenytársak aktuális és várható döntéseit.

A kölcsönös függőség ilyen meghatározó mértéke felveti a résztvevők együttműködésének lehetőségét, ill. kérdését:

A nem kooperatív esetben az iparági szereplők önállóan hozzák meg döntéseiket, lépéseiket nem egyeztetik másokkal, ennek nem mond ellent, hogy a riválisaikról rendelkezésre álló információikat (múltbéli viselkedés, várakozások) felhasználják döntéseik során.

A kooperatív esetben a résztvevők tájékoztatják egymást döntéseikről, sőt akár össze is hangolhatják azokat: olyan megegyezés születhet a vállalatok közt az árra és/vagy a termelt-eladott mennyiségre vonatkozóan, amely a kooperációban (kollúzióban) résztvevők együttes profitját növeli. Ez a fajta összejátszás lényegében a verseny intenzitását, a piaci folyamatokat kísérő bizonytalanságot csökkenti, a profitot növeli, és piacra újonnan belépni szándékozókat hatékonyabban távol tarthatja.

A piaci versenyt korlátozó összejátszást a fejlett piacgazdasággal rendelkező országokban általában törvények tiltják, ennek ellenére, mivel erős az együttműködés kialakítását célzó érdek, a vállalatok a kilátásba helyezet szankciók fenyegetése mellett is megegyezhetnek egymással nyílt vagy burkolt formában.

A következő kérdés, ami felvetődhet bennünk, hogy mennyire stabil egy-egy létrejött oligopol piaci szerkezet: ha ugyanis egy iparágban hosszabb időszakon belül pozitív gazdasági profitot realizálnak a szereplők, akkor a belépés szándéka erősödik a kívül állókban, miközben a bent levők a kialakult állapot fenntartásában érdekeltek. Egy az átlagosnál jobban jövedelmező iparág oligopol szerkezete csak belépési korlátok mellett maradhat fenn. A belépési korlátok lehetnek mesterségesek vagy természetesek, amelyeknek megfelelően mesterséges vagy természetes oligopóliumokról beszélünk. Természetes oligopóliumok akkor alakulnak ki, ha néhány vállalat alacsonyabb költséggel képes előállítani a teljes piaci kínálatot, mintha ennél több vállalat bármilyen más kombinációja működne az iparágban. Ezzel szemben mesterséges oligopóliumot eredményezhet pl. az állami szabályozás. Kezdetben a távközlési vállalatok egyedül uralták az egyes országok piacait, természetes monopóliumok voltak; majd a technológia fejlődésének hatására a gazdaságos üzemméret csökkenésével, a meglevő állami szabályozás mellett már mesterséges monopóliumokról kell beszélnünk. A '80-as évektől a szabályozáspolitika fordulatváltásának következtében, a liberalizáció térhódításával a távközlési piacokon újabb és újabb vállalatok jelentek meg, oligopol szerkezetet alakítva ki.

E rövid bevezető után térjünk át arra a kérdésre, hogy miképpen lehet modellezni bizonyos konkrét oligopol piaci szituációkat.

2. 1. Klasszikus oligopólium modellek (nem kooperatív eset)

Sokféle oligopol modell ismeretes, amelyek elsősorban abban térnek el, hogy miképpen gondolkodnak a versenytársak egymás piaci magatartásáról, illetve mennyire képesek kiismerni, megjósolni a többiek magatartását és várható döntéseit. A legegyszerűbb klasszikus modellek sok egyszerűsítő feltevéssel élve (pl. nem foglalkoznak a piacra való belépés, ill. a kilépés problémájával) vezetnek egyértelmű eredményhez, míg a döntési problémákat életszerűbben bemutató modellek ezeknél jóval bonyolultabb módon adnak nem feltétlenül határozott megoldást.

A következőkben a klasszikus modelleket tekintjük át játékelméleti eszközöket segítségül hívva. Ezekben az esetekben a játékelmélet statikus megközelítése alkalmazható, amelyekben feltételezhető a szereplők (játékosok) egyszeri szimultán döntése. A játékosok stratégiaválasztásán a konkrét modellektől függően vagy a piacra viendő mennyiség (Cournot, Stackelberg) vagy az ár meghatározását (Bertrand) kell érteni. A modell feltételrendszerének megfelelő megoldást mindig Nash-egyensúlyi stratégiák[1] formájában keressük, ez jelenti tulajdonképpen a feladat játékelméleti eszközökkel való megközelítését (eredetileg a következő klasszikus modellek megoldását a piaci szereplők ún. reakciófüggvényeinek meghatározása és megoldása jelentette).

Cournot-oligopólium

Tegyük fel, hogy a piacon $n(n > 1)$ vállalat homogén terméket termel, az i. vállalat termeljen q_i mennyiséget, és a vállalat költségeit jelölje $C_i(q_i)$. A kereslet-ár összefüggést az inverz piaci keresletfüggvénnyel $F(Q)$ adjuk meg, ahol is Q jelölje az összpiaci keresletet. Valamint q jelentse a $(q_1, \ldots, q_n)$ és q_{-i} a $(q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_n)$ vektort. Ezekből az i. vállalat nyeresége $(\Pi_i(q))$ már meghatározható:

$$\Pi_i(q) = F(Q)q_i - C_i(q_i) \qquad (1)$$

A vállalatokat tekintsük tökéletesen racionálisaknak döntéseik meghozatalakor, helyzetük legyen szimmetrikus, és ilyen körülmények közt hozzák meg egyszerre azon döntésüket, hogy mennyit kívánnak termelni. A döntés (stratégia) megválasztása után a piaci ár az $F(Q)$ függvényen keresztül már meghatározottnak tekinthető; az ilyen típusú mennyiséggel kapcsolatos döntéseket output-vezérlésnek nevezzük. Tehát a vállalatok stratégiáikat a piacra vinni kívánt mennyiség (q_i) megválasztásával realizálják, és kölcsönös függőségüket az együttesen piacra vitt mennyiség ármeghatározó szerepe fejezi ki.

A feladat Nash-egyensúlyi megoldását, amelytől egyik vállalatnak sem érdemes egyoldalúan eltérnie, a következő feltételt kielégítő $\hat{q} = (\hat{q}_i, \ldots \hat{q}_2)$ vektor adja:

$$\forall i, \forall q_i \ \Pi_i(\hat{q}) \geq \Pi_i(\hat{q}_1, \ldots, \hat{q}_{i-1}, q_i, \hat{q}_{i+1}, \ldots, \hat{q}_n), \qquad (2)$$

A következőekben vizsgáljuk meg, hogy milyen eredményre vezet ez a gondolatmenet, ha további egyszerűsítő feltételeket szabunk:

- minden vállalat rendelkezzen azonos $C_i(q_i) = cq_i$ költségfüggvénnyel;
- az inverz keresleti függvény legyen a következő alakú: $F(Q) = a - bQ$, ahol $a, b > 0$, ill. $a > c$.

Így tehát a vállalati nyereségek (1) alapján:

$$\Pi_i(q) = (a - bQ)q_i - cq_i \qquad (3)$$

A fenti feltételek mellett és az egyensúlyi kritérium (2) alapján a megoldásra fennáll:

$$\frac{\partial \Pi_i(\hat{q})}{\partial q_i} = 0, \quad \forall i \qquad (4)$$

Tehát, mivel a megoldás szimmetrikus (a vállalatokat jellemző költségfüggvények azonosak):

$$a - b\sum_i \hat{q}_i - b\hat{q}_i - c = 0 \ \forall i \qquad (5)$$

azaz:

$$\hat{q}_i = \frac{a - c}{b(n + 1)}, \ \forall i \qquad (6)$$

Így az aggregált kibocsátás (nq_i) kisebb lesz, mint kompetitív piac esetén lenne $(q_{komp} = (a - c)/b)$, és ugyanakkor nagyobb, mint tiszta monopólium esetén $(q_{mon} = (a - c)/2b)$. Az összprofit az iparágban viszont nagyobb lesz, mint a kompetitív esetben, de kisebb, mint monopólium esetén.

Két szereplő esetén az eredmények (a következő modellel (Stackelberg-duopólium) való összehasonlíthatóság érdekében):

$$(\hat{q}_1, \hat{q}_2) = \left(\frac{a - c}{3b}, \frac{a - c}{3b}\right) \text{ és } \hat{p} = \frac{a + 2c}{3}$$

ill.

$$\Pi_1 = \Pi_2 = \frac{(a - c)^2}{9b} \qquad (7)$$

Stackelberg-duopólium

A Stackelberg-modell a Cournot-modell egy alternatív megközelítését kínálja kétszereplős esetben: mindössze annyiban tér el az előző megközelítéstől (a szigorúan két szereplőn kívül), hogy nem követeli meg a vállalatok szimmetrikus helyzetét: elemzése szerint az oligopol piacokon egy-egy cég nagy piaci részesedése folytán olyan hatalomra tesz szert, hogy outputdöntéseivel befolyásolni, vezérelni tudja a többi vállalatot. Az ilyen vállalatot vezetőnek, a többit (a másikat) követőnek hívjuk.

A továbbiakban legyen az 1. vállalat a vezető, a 2. vállalat pedig a követő. Az 1. vállalat vezető szerepe a modellben oly módon jelenik meg, hogy ismeri a 2. vállalat reakciófüggvényét (tudja, hogy a 2. vállalat outputdöntései hogyan függnek össze saját döntéseivel):

$$q_2 = H_2(q_1) \ , \quad \text{ha} \quad \forall \tilde{q}_2 \quad \Pi_2(q_1, q_2) \geq \Pi_2(q_1, \tilde{q}_2) \qquad (8)$$

[1] A játékelméletben gyakran alkalmazott Nash-egyensúly olyan megoldást jelent, amelytől fennállásakor egyetlen szereplőnek sem érdemes egyoldalúan eltérnie.

Az egyensúlyt (Nash) ezek után a következő egyenlőtlenség határozza meg:

$$\forall q_1, \Pi_1[\hat{q}_1, H_2(\hat{q}_1)] \geq \Pi_2[q_1, H_2(q_1)] \quad (9)$$
$$\text{és} \quad \hat{q}_2 = H_2(\hat{q}_1)$$

Az eredmény a következőképpen magyarázható: a vezető vállalat dönt, hogy mekkora mennyiséget visz a piacra, a követő ezt a mennyiséget fixnek tekintve határoz, hogy milyen mennyiség kibocsátásával maximálhatja a profitját; továbbá a vezető tisztában van a követő reakciójával, és ezt figyelembe is veszi a döntésekor. Tehát az egyensúlyi pontban – a fennálló információs struktúra figyelembevételével – az egyik vállalat sem tud úgy egyoldalúan változtatni döntésén, hogy profitja növekedjen (Nash).

A Cournot-modellben vizsgált konkrét költségfüggvényeket $(C_i(q_i) = cq_i)$ és piaci keresleti függvényt $(F(Q) = a - bQ)$ feltételezve Stackelberg megfontolásával a következő eredményre juthatunk:

$$(\hat{q}_1, \hat{q}_2) = \left(\frac{a-c}{2b}, \frac{a-c}{4b}\right) \text{ és } \hat{p} = \frac{a+3c}{4} \quad (10)$$

Illetve a két vállalat profitja:

$$\Pi_1 = \frac{(a-c)^2}{8b} \text{ és } \Pi_2 = \frac{(a-c)^2}{16b} \quad (11)$$

Az 1. vállalat (vezető) tehát a monopolista outputot állítja elő, ez kétszerese a követő vállalat kibocsátásának. Együttesen a tökéletesen versenyző output 3/4-ét termelik, ami nagyobb mint a Cournot-duopólium együttes kínálata. A vezető vállalat a Cournot-duopolisták esetében realizáltnál nagyobb profitot ér el, míg a követő kisebbet (ld. (7) képlet).

Chamberlin-duopólium

Ebben a modellben egyidejűleg érvényesül a Cournot-duopóliumra jellemző szimmetria és a rivális reakciófüggvényének ismeretére vonatkozó stackelbergi feltételezés: tehát mindkét vállalat viselkedését meghatározza a másik vállalat reakciófüggvényének ismerete.

Mindezek figyelembevételével az egyensúly: a reakciókra való teljes informáltságból felismerik a szimmetrikus helyzetüket, és profitjuk maximalizálása érdekében együttesen a maximális iparági profit (monopolista profit) elérésére törekszenek, amiből egyenlő arányban részesednek:

$$q_1 = q_2 = \frac{a-c}{4b}, \; p = \frac{a+c}{2}, \; \Pi_2 = \Pi_2 = \frac{(a-c)^2}{8b} \quad (12)$$

Ez az eredmény azonban nem indokolható a játékelmélet Nash egyensúlyával, és valójában e következtetés mögött inkább a kollektív racionalitásra való törekvés jegyei mutatkoznak meg: mindkét vállalat felismerve a számukra együttesen legkedvezőbb megoldást, önként vállalják a monopolista profiton történő osztozkodást. Ennek megvalósulása a gyakorlatban viszonylag ritka, mert kockázatos lehet a kollektív racionalitásra való törekvés (kartell megállapodás csökkentheti a kockázatot, de ez a téma már a kooperatív játékok területére vezet).

Bertrand-egyensúly

Bertrand a fentiekkel ellentétben a vállalatokról azt feltételezi, hogy nem a piacra vitt mennyiséget, hanem az árat választják stratégiai változónak, ebben a megközelítésben az eddigi eredményeink nem tekinthetők Nash-egyensúlyinak.

Induljunk ki továbbra is az eddig is feltételezett lineáris költség- és piaci keresleti függvényekből. Mivel homogén termékeket vizsgálunk, ha egy vállalat alacsonyabb árat szab meg, mint a többi vállalat, akkor a teljes piaci részesedést megszerezheti (ha többen kínálnak a legalacsonyabb áron, akkor osztozzanak egyenlően a piaci részesedésen).

Ha a legalacsonyabb ár nem egyenlő a határköltséggel (ami feltételezésünk szerint c konstans) akkor bármelyik vállalat, amelyik ennél alacsonyabb áron kínál növelni tudja profitját. Tehát egyensúly (Nash) csak akkor jön létre, ha a piacon a határköltséggel megegyező ár alakul ki, és ekkor az aggregált kibocsátás egyenlő a kompetitív esetben létrejövővel.

Hangsúlyozni kell azonban, hogy az előzőekben vizsgált modellek nagyon leegyszerűsített, szigorúan statikus megközelítést alkalmaznak, egyszeri szimultán döntéseket feltételezve; nem számolnak az esetlegesen piacra belépni ill. onnan kilépni kívánók körével; valamint sok idealizált feltevéssel élnek: tehát mindezek figyelembevételével szabad csak elfogadni a fenti gondolatmenetek eredményeit.

2. 2. A duopol együttműködés fogolydilemmája

Az eddigi modellek jellemzően (kivéve: Chamberlin) nem érintették az együttműködés témakörét. E fejezet az oligopol kooperáció kérdéskörének egyszerű eszközökkel való vizsgálatát tűzi ki célul: először végiggondolva, hogy vajon milyen körülmények befolyásolják az együttműködés kialakulását, majd a duopol együttműködést statikus, ill. dinamikus megközelítésben bemutatva.

Az együttműködést elősegítő körülmények

Számos olyan körülmény létezik, amelyek hatására a vállalatok közti együttműködés kialakulásának esélye jelentősen megnő. Ezeket vesszük sorra a következőkben.

A piacon működő vállalatok számának növekedésével csökken a kooperáció esélye, mert egyrészt jelentősen nő a páronkénti kapcsolattartások száma $(n * (n-1)/2)$, másrészt egyre nehezebb a mindenkinek megfelelő közös érdekek kialakítása. Ezenfelül a tapasztalat azt mutatja, hogy a piaci koncentráció növekedésével nő az együttműködés valószínűsége.

Ha a piacralépési korlátok magasak, akkor az együttműködés valószínűsége nagyobb, mivel a kooperáció révén keletkező extraprofit realizálását kevésbé veszélyezteti új belépő.

Eddigi vizsgálataink során a termékek tökéletes homogenitását feltételeztük, ez a valóságban közel sem ilyen egyszerű, az azonban elmondható, hogy a homogenitás növekedésével könnyebben állapítható meg a vállalatok által a közös ár (feltéve, hogy ennek kialakítása megállapodás tárgya) és így nagyobb az együttműködés esélye. A piaci keresleti görbe meredeksége is hatást gyakorol az összejátszásra: ha a kereslet rugalmatlan, akkor nagyobb ennek esélye, mivel nagyobb az így elérhető profit (az ár emelkedésével csak kis mértékben csökken a kereslet).

Tehát számos olyan együttműködést befolyásoló tényező létezik, amit modelljeinkben nem vettünk, ill. veszünk figyelembe, de azért oda kell rájuk figyelni.

Statikus vizsgálat

Tegyük fel, hogy a vizsgált piacon csak két vállalat osztozik. Továbbá kiindulásként feltételezzük, hogy a vállalatok szóbeli együttműködési megállapodást kötnek egymással, amelynek értelmében visszafogják mindketten kibocsátásukat, ill. csökkentik áraikat a profitjuk növelése érdekében. Mivel az effajta megállapodásokat általában a piacgazdasággal rendelkező országokban a törvény tiltja, a vállalatok igyekeznek titokban tartani azt, következésképp betartásának nincsenek jogi garanciái.

A vállalatok a megegyezést követően – annak függvényében, hogy betartják-e vagy sem a megállapodásban foglaltakat (egyoldalúan v. kétoldalúan megszegik) – különböző profitot érhetnek el. A legjellemzőbb költségfüggvényeket („U" alakú AC görbe, ellentétben az előző fejezetben feltételezett konstans átlagköltséggel: ahol egyébként a most következő gondolatmenet más eredményre vezetne) és piaci keresleti függvényt feltételezve a profit a következő táblázatban foglaltak szerint alakul a különböző esetekben: a táblázatokban szereplő számok csak a nyereségek növekvő sorrendjét hivatottak jelezni, annak tényleges nagysága nélkül.

2. sz. váll. / 1. sz. váll.	betartja a szerződést	nem tartja be
betartja a szerződést	3 / 3	4 / 1
nem tartja be	1 / 4	2 / 2

Mindenfajta számolgatás nélkül elég hihetőnek tűnnek az eredmények: a vállalat akkor jár a legrosszabbul, ha betartja a megállapodást ellenfele viszont nem (1), ennél jobban jár, ha ő sem tartja be (2), ill. ha ő és az „ellenfele"/„szövetségese" is betartja (3); míg a legtöbb nyereséghez akkor jut, ha ő nem, viszont ellenfele betartja a megállapodást.

Az ilyen típusú döntési helyzeteket nevezi a játékelmélet fogolydillemának, Merrill Flood és Melvin Drechser legelső a mi problémánkkal azonos eredményre vezető felvetése alapján (a feladatban két gyanúsítottnak kell választania a tanúskodás ill. a hallgatás közt).

Statikus esetben a következő gondolatmenet alapján határoz az első vállalat (feltételezzük, hogy mindkét vállalat tisztában van a helyzetével, és mindkettő teljesen racionálisan cselekszik):

- ha versenytársam együttműködik akkor, ha én is ezt teszem 3 egységnyi nyereséghez jutok, ha nem akkor pedig 4 egységhez, tehát jobb ilyen esetben nem együttműködni;
- ha versenytársam nem tartja magát a megállapodáshoz, akkor jobban járok ha én sem kooperálok, mert így 2 egység nyereséget érek el 1 helyett

Tehát akárhogyan dönt is a versenytársam én jobban járok, ha nem kooperálok. A gondolatmenet a másik vállalat esetében is hasonló: ő sem tartja magát a megállapodáshoz, ha racionálisan, önérdekének megfelelően dönt.

Így mindketten – racionális döntéshozók révén – versengeni fognak (nem tartják be a megállapodást) és *2,2* egységnyi profithoz jutnak ahelyett, hogy kooperálva *3,3* egységnyi nyereséget értek volna el. Játékelméleti fogalmak alapján a *verseng,verseng* stratégiapár Nash-egyensúlyi megoldást takar, hiszen ettől *egyoldalúan* egyik játékosnak sem érdemes eltérnie.

Sokmenetes játszmák

Eddigi vizsgálataink nem terjedtek ki a több esetleg végtelen menetből álló játszmákra. A játékelmélet megkülönbözteti a *„reapated game"* típusú játszmákat, ahol a játékosok más és más döntési helyzetekkel szembesülnek; illetve az ún. *„supergame"* néven ismert helyzetet, amikoris a játékosok ismételten ugyanabba a döntési szituációba kényszerülnek.

A minket érdeklő duopol fogolydillemát vizsgáljuk most az utóbbi megközelítésnek megfelelően (supergame), mivel ez azt a helyzetet modellezi jól, melyben a szereplők (vállalatok) egy bizonyos időszakra határozzák meg (pl. 1 hónap) kibocsátásukat, ill. áraikat; és döntéseiket hasonló körülmények közt (diszkontálás hatásától eltekintve) újra és újra meg kell hozniuk.

Ebben a sokmenetes helyzetben az a logika, amely egyértelműen versengésre vezet már nem állja meg a helyét, mivel csak az első játékkal számol. Ha a játék több fordulóból áll, akkor már nem csak a kooperálás és nem kooperálás stratégiája létezik, hanem bonyolult hosszú távú stratégiák is alkalmazhatóak. A stratégiák céljává a hosszú távú átlagnyereség maximálása válik. A játékosoknak lehetőségük nyílik egymás jutalmazására, ill. büntetésére.

A választ arra a kérdésre, hogy mi a megfelelő stratégia a sokmenetes fogolydilemma játszmában sokan próbálták megadni az utóbbi évtizedekben: Robert Axelrod amerikai politológus többek között azzal a kérdéssel is foglalkozott, hogy létrejöhet-e – és ha igen akkor mi módon – a kooperáció a fent leírt helyzetben olyan játékosok (mi esetünkben értelemszerűen a vállalatok) közt, akik kizárólag önérdeküknek megfelelően (racionálisan) cselekszenek. Versenyre hívott olyan tudósokat, akik munkájuk során a fogolydilemmával már foglalkoztak: mindenkinek, mint egy játékosnak egy program formájában meg kellett fogalmaznia stratégiáját a sokmenetes fogolydilemmára. A beérkezett programokat Axelrod ezután körmérkőzéses alapon egymás ellen játszatta, az nyert, amelyik összesen a legtöbb pontot gyűjtötte.

A győztes egy meglepően egyszerű stratégia lett: Anatol Rapaport, szociálpszichológus programja, amely a következő volt:

- az első menetben kooperál;
- a többiben azt tette, amit ellenfele az előző lépésben.

E stratégia *Tit for Tat* néven híresült el a későbbiekben. Az első megmérettetést újabb is követte, de a számos bonyolult fogalomrendszerrel ellenfeleit kiismerni kívánó program mellett ismét első helyen végzett ez a már túlontúl egyszerűnek tűnő stratégia.

A beérkezett pályázatokat Axelrod korábban sohasem látott módon elemezte, hogy választ kapjon a kérdésre: mitől jó egy stratégia. A pszichológiát segítségül hívva „személyiségvonásokkal" jellemezte az egyes programokat. Kutatásai azt mutatták ki, hogy a legjobb stratégiák a következő öt főbb tulajdonsággal rendelkeztek:

- *barátságosság* (barátságos az a program, ami sohasem kezdeményez versengést);

- *megbocsátás* (megbocsátó az, amelyik ellenfél „ballépését" követően hajlandó újra kooperálni);
- *provokálhatóság* (ha az ellenfél verseng, azt nagy eséllyel viszonozza);
- *reakcióképesség* (a válasz nagymértékben függjön az ellenfél lépéseitől);
- *kiismerhetőség* (ezt a jellemzőt a program hossza határozta meg).

A *Tit for Tat* stratégia sikerének titka valószínűleg az volt, hogy ezt az öt tulajdonságot a legjobban sikerült ötvöznie.

Az emberekkel végzett egymenetes fogolydilemma-kísérletek mintegy 40 %-ában fordult elő kooperáció, sokmenetes esetben ez az arány pedig 60 %-ra nőtt, ugyanakkor jellemző volt a bennragadás a versengésben. A sokmenetes játékokban gyakran megjelent a *Tit for Tat* stratégia, de nem teljesen tiszta formában.

Összefoglalva elmondható, hogy a valós világ sokmenetes fogolydilemmával leírható helyzeteiben, így a duopol versengés esetében is az Axelrod által felsorolt öt tulajdonság sokkal célravezetőbb lehet, mint a számító ész.

2. 4. Belépés, alkalmazkodás, kilépés

A belépés, alkalmazkodás, és a kilépés különösen hangsúlyozott szerepet játszik az olyan piacok esetében, ahol egyszerre csak néhány vállalat működik: ahol az oligopol piaci szerkezet a jellemző; így az ezen fogalmak kapcsán felmerülő kérdésekkel is foglalkozni kell.

Ezen piacokról elmondható – az előző fejezetek modelljeiben számszerűsítetten is vizsgáltuk – hogy az egyes szereplők extraprofitot ((gazdasági profit) realizálhatnak. Pontosan az extraprofit termelő képesség hosszú távú fennállása a jele annak, hogy a piacra való belépésnek korlátai vannak. Ezek a korlátok lehetnek mesterségesek: a kormányzat által valami módon létrehozottak, vagy természetesek. A továbbiakban csak a természetes belépési korlátokat vizsgáljuk: Bain (1956) öt olyan belépési korlátot sorolt fel, amelyek megvédik a piaci szereplőket attól, hogy a sorozatos belépések által az oligopol szerkezet eredményezte extraprofit-termelő képességük fokozatosan elenyésszen:

- *méretgazdaságosság* (economies of scale): ha a minimális üzemméret, amit működtetni érdemes a piac számottevő részét el képes látni, akkor jellemzően néhány vagy csak egy vállalat működhet hosszú távon a piacon;
- *abszolút költségelőny:* a működő vállalatok olyan költségelőnyökkel rendelkezhetnek, amelyek nem állnak rendelkezésükre a belépni kívánóknak; ezek származhatnak a sokéves tapasztalatból, innovációkból, az olcsó inputok szerződés alapján történő beszerzéséből stb.;
- *termékdifferenciálás előnyei:* sikeresen választották ki a leginkább keresett jellemzőkkel bíró terméket, és ezzel elnyerték a vevők a bizalmát;
- *tőkéhez jutás előnye:* a belépők nehezebben, ill. drágábban juthatnak csak tőkéhez a belépéssel járó nagy kockázat miatt.

Az irodalomban sokféle modell leírása található meg a vizsgált témakörben, amelyek eltérő eredményre vezetnek, természetesen más és más feltevésekből kiindulva; ezért nem lehet cél ezek felsorolása, bemutatása. Így a következőkben egy olyan modell bemutatása következik, amely véleményem szerint jól leírja (vagy legalábbis megközelíti) a távközlési szektor jellemzőit is.

A piacra történő belépésért, és annak újrafelosztásáért folyó harc legegyszerűbben egy kétmenetes játszma keretében vizsgálható. Mostanában Fudenberg és Tirole (1984), ill. Bulow, Geanakoplos, és Klemperer (1985) foglalkozott e kérdéssel, és egymástól függetlenül a következő modellt javasolták.

Tételezzünk fel két szereplőt: az 1. vállalat (a piacon eddig egyedüli) megválasztja K_1-et, hogy milyen mennyiségű tőkét akar felhalmozni, ezek után ennek alapján a 2. vállalat (aki belépni szándékozik) dönt, hogy be kíván-e lépni.

- *Ha nem*, akkor sem veszít semmit az ügyön (feltételezve, hogy eddig nem voltak költségei); az 1. vállalat továbbra is élvezi a monopol pozíció előnyét és $\Pi^{1m}(K_1, x_1^m(K_1))$ a profitja.
- *Ha igen*, akkor a játszma második részében mindkét vállalat egyszerre határoz x_1 és x_2 értékéről, amelyek stratégiai változókat jelölnek: lehetnek stratégiailag helyettesítő (mennyiségek), illetve kiegészítő szerepűek (árak). Így a két vállalat profitja:

$$\Pi^1 = (K_1, x_1, x_2) \text{ és } \Pi^2 = (K_1, x_1, x_2) \qquad (13)$$

Tételezzük fel, hogy döntésüket a vállalatok a Cournot-modellben leírt módon hozzák meg K_1 függvényében, és az így kialakult Nash-egyensúlyt jelöljük az alábbi módon:

$$\{x_i^*(K_1), x_2^*(K_2)\} \qquad (14)$$

Ezekután a feladat abban áll, hogy át kell tekintenünk az 1. vállalat viselkedését: miként határoz K_1 mértékéről a különböző helyzetekben.

A belépni szándékozók „elrettentése"

Az elrettentésen a következőt értjük: 1. vállalat K_1 mértékét úgy választja meg, hogy a 2. vállalatnak éppen ne legyen érdemes belépnie a piacra, azaz:

$$\Pi^2(K_1, x_1^*(K_1), x_2^*(K_1)) = 0 \qquad (15)$$

Ekkor fennáll a 2. vállalat profitmaximalizációja miatt, hogy:

$$\frac{\partial \Pi^2}{\partial x_2}(K_1, x_1^*(K_1), x_2^*(K_1)) = 0 \qquad (16)$$

Így K_1 hatását a második vállalat profitjára a következő derivált fejezi ki:

$$\frac{d\Pi^2}{dK_1} = \frac{\partial \Pi^2}{\partial K_1} + \frac{\partial \Pi^2}{\partial x_1}\frac{dx_1^*}{dK_1} \qquad (17)$$

A (17) egyenlet jobboldalának első tagját a tőkenövelés 2. vállalat profitjára gyakorolt *direkt* hatásának (direct effect) nevezzük (erre példa, ha az 1. vállalat a vásárlói bizalom növelése érdekében fektet be), a második tagot pedig a tőke 2. vállalat profitjára gyakorolt *stratégiai hatásának* (a tőkét a termelési kapacitásának fejlesztésére fordítja). A továbbiakban az egyszerűség kedvéért eltekintünk a tőke *direkt hatásától.*

Azt mondjuk, hogy az 1. vállalatot a beruházás *erősíti*, ha $(d\Pi^2/dK_1) < 0$; és *gyengíti*, ha $(d\Pi^2/dK_1) > 0$. Ahhoz, hogy elriassza ellenfelét (a 2. vállalatot) a

piacra lépéstől, minél erősebbnek kell mutatkoznia (ill. lennie). Így következő stratégiák közül, ha a beruházás erősíti a vállalatot a „top dog", ha gyengíti a „lean and hungry look" megnevezéssel meghatározottat tanácsos alkalmaznia:

- *„top dog":* túlzott beruházás, erőt és agressziviást sugallva;
- *„puppy dog":* a beruházók visszafogása ártalmatlannak tűnve;
- *„lean and hungry look":* beruházások visszafogása erőt sugározva;
- *„fat cat":* túlzott beruházások; erőtlennek, veszélytelennek tűnve.

A túlzott és visszafogott beruházás azt jelenti, hogy a vállalat a tőkefelhalmozás során nem a leghatékonyabb tőkeszerkezet mellett dönt, hanem figyelembe veszi, hogy a potenciális jövőbeni versenytársak által elérhető profitra saját tőkéje milyen befolyást gyakorol (a beruházás erősíti vagy gyengíti-e), és eszerint a szükségesnél többet vagy kevesebbet fektet be.

A belépés eltűrése

A monopol pozíciót nem mindig célszerű védeni, lehet, hogy ez sokkal nagyobb költséget jelent a vállalatnak, mint a piacvesztés. Éppen ezért, ha a piacon lévő vállalat (1.) úgy ítéli meg helyzetet, hogy túl költséges az előző fejezetben bemutatott piacvédő stratégia, akkor az újonnan belépő vállalattal is számolva kell maximalizálni a profitját:

$$\max_{K_1} \Pi^1(K_1, x_1^*(K_1), x_2^*(K_1)) \qquad (18)$$

Ez a függvény K_1 szerinti deriváltjának 0-vá tételével tehető meg:

$$\frac{d\Pi^1}{dK_1} = \frac{\partial \Pi^1}{\partial K_1} + \frac{\partial \Pi^1}{\partial x_2}\frac{dx_2^*}{dK_1} \qquad (19)$$

A tőkeemelés 1. vállalat profitjára gyakorolt *direkt hatását* (tőke határhaszna) az első tag, a *stratégiai hatást* (a másik vállalat kibocsátásának változása által közvetített hatás) a második tag mutatja. Túlzott a beruházás akkor, ha a direkt hatás negatívvá válik; visszafogott ha még nem érte el az üzem a méretgazdaságosságot és a direkt hatás még pozitív.

A beruházás kívánatos mértékét a *stratégiai hatás* előjele mutatja meg, ugyanis optimális esetben a két hatás összege nulla:

$$sign\left(\frac{\partial \Pi^1}{\partial x_2}\frac{dx_2^*}{dK_1}\right) = sign\left(\frac{\partial \Pi^2}{\partial x_1}\frac{dx_1^*}{dK_1}\right) \times sign(R_2') \qquad (20)$$

felhasználva a következőket:

$$sign\left(\frac{\partial \Pi^1}{\partial x_2}\right) = sign\left(\frac{\partial \Pi^2}{\partial x_1}\right) \quad \text{és} \qquad (21)$$

$$\frac{dx_2^*}{dK_1} = \left(\frac{dx_2^*}{dx_1}\right)\left(\frac{dx_1^*}{dK_1}\right) = R_2'(x_1^*) \cdot \left(\frac{dx_1^*}{dK_1}\right)$$

Tehát végül is a stratégiai hatás előjelét, és így a beruházás mértékét is az határozza meg, hogy vajon a *beruházás erősíti vagy gyengíti a vállalatot* (a 20-as szorzat első tagja ugyanis a 2. vállalat profitjára gyakorolt stratégiai hatását fejezi ki (17-es egyenlet jobboldalának második tagja), ami pont erre utal); és, hogy a *stratégiai változók helyettesítő vagy kiegészítő jellegűek-e* (R_2 derivált előjele).

Az alábbi táblázat összefoglalja az előző (Elrettentés – E) és az e fejezet (Alkalmazkodás – A) különböző eseteit, és az adott helyzetekben alkalmazható legjobb stratégiákat:

	A beruházás *erősíti* az 1. vállalatot	A beruházás *gyengíti* az 1. vállalatot
x_1, x_2 kiegészítő jellegűek, jellemzően árverseny	*A – „puppy dog"* *E – „top dog"*	*A – „fat cat"* *E – „lean and hungry"*
x_1, x_2 helyettesítő jellegűek, jellemzően outputvezérlés	*A és E esetben is „top dog"*	*A és E esetben is „lean and hungry"*

Egy esetet részletesen is megvizsgálva: tegyük fel, hogy a *beruházás erősíti az 1. vállalatot*, és a beruházás a termelőkapacitás hatékonyabbá tételére fordítódik (nem pedig a kapacitás bővítésére), tehát *árversenyt* eredményez. Lépésről lépésre végiggondolva, hogy a fenti elmélet milyen választ ad *alkalmazkodás* esetén:

- A beruházás erősíti a vállalatot, tehát a (17)-es képlet által meghatározott derivált negatív.
- A (17)-es egyenlet jobboldalának első tagját elhanyagoltuk, ezért a tőkeemelés 2. vállalat profitjára gyakorolt stratégiai hatása is negatív.
- A reakciófüggvény deriváltjának előjele pozitív, hiszen árversenyről van szó.
- A (20)-as képlet által meghatározott stratégiai hatás, amely az 1. vállalat profitjára vonatkozik, így szintén negatív előjelű. Tehát a (19)-es derivált csak úgy lehet zérus (azaz az 1. vállalat profitja maximális), ha annak első tagja, vagyis a tőkebefektetés határhaszna még pozitív.
- A tőkebefektetés határhaszna tipikus esetekben akkor pozitív, amikor a beruházás még nem érte el a maximális hatékonysághoz szükséges mértéket.
- Esetünkben a legjobb stratégia a *„puppy dog"* alkalmazása: a beruházók visszafogása ártalmatlannak tűnve.

E fejezet egyik tanulsága, hogy nem feltétlenül minden esetben növekszik a társadalom jóléte, ha a hatóság előzetes vizsgálat nélkül oligopol piaci struktúrák kialakítására törekszik a monopóliumok helyett, hiszen mint láttuk a társadalmi jólét növekedését már az ilyen egyszerű modell sem mutatja olyan egyértelműnek, mint az első látásra hinné az ember: a fenti elemzésben például a tőkeallokációs mechanizmusok nem a leghatékonyabb irányba terelik a gazdaságot. Így például az olyan kérdésekre, hogy célszerű-e a távközlés liberalizációja, milyen területekre, milyen mértékben terjedjen ki, és mikor menjen végbe – e dolgozat keretében nem – csak nagyon alapos előzetes vizsgálatok tükrében adható megnyugtató válasz.

IRODALOMJEGYZÉK

[1] Koppányi Mihály: Mikroökonómia, 1996 Műszaki Könyvkiadó
[2] Jean Tirole: The Theory of Industrial Organization, 1988 Cambridge MIT Press
[3] Eric Rasmusen: Games and Information, 1994 Blackwell Publishers
[4] Szép Jenő, Forgó Ferenc: Bevezetés a játékelméletbe, 1974 Közgazdasági és Jogi Könyvkiadó
[5] John Eatwell-Murray Milgate-Peter Newman: Game Theory, 1989 The Macmillan Press Limited
[6] Mérő László: Mindenki másképp egyforma, 1996
[7] Drew Fundenberg-Jean Tirole: Dynamic Models of Oligopoly, 1986 Harwood Academic Publishers

OLIGOPOL MARKETS ANALYSIS BY USING THE TOOLS OF THE GAME THEORY

FUTÓ PÉTER és TŐKEY ZOLTÁN

DEPARTMENT OF TELECOMMUNICATIONS AND TELEMATICS
FACULTY OF ELECTRICAL ENGINEERING AND INFORMATICS
TECHNICAL UNIVERSITY OF BUDAPEST
H-1111 BUDAPEST EGRY J. U. 18.

Oligopoly theory deals with markets in wich some firms sell a product to lots of customers. Because of the small number of the participants the actions of one firm affect the behavior of the others. Game theory is very useful for understanding the market processes and has found many applications in the field of industrial organizations. In this article we will briefly explain some of the central themes of oligopoly theory and emphasize the connection between these themes and developments in the theory of games.

In the first place we present a simple static oligopoly modell and use it to discuss the solutions of Cournot, Stackelberg, Chamberlain and Bertrand.

The next section contains an illustration of the divergence between invidual and collective rationality, using the Prisoner's Dillema concept. Decisions that are rational from the point of view of each individual may be defective from the point of view of both. In the last section we examine the barriers to entry, anything that allows incumbent firms to earn extra profits without threat of entry. Then we will deal with two kinds of behavior by incumbents in the face of an entry threat: the deterred entry: in this case the incumbents modifies their behaviour to successfully thwart entry; and the accomodated entry, when the incumbents find it more profitable to let the entrant enter than to erect costly barriers to entry.

Futó Péter 1994-ben kezdte meg tanulmányait a Budapesti Műszaki Egyetem villamosmérnöki szakán. Jelenleg ötödéves hallgatók a Távközlés és Telematika szakirányon. Emellett 1996-tól a Budapesti Közgazdaságtudományi Egyetem nappali tagozatos hallgatója.

Tőkey Zoltán 1994-ben kezdte meg tanulmányait a Budapesti Műszaki Egyetem villamosmérnöki szakán. Jelenleg ötödéves hallgatók a Távközlés és Telematika szakirányon. Emellett 1996-tól a Budapesti Közgazdaságtudományi Egyetem nappali tagozatos hallgatója.

TÁVKÖZLŐ BERENDEZÉSEK SZABVÁNYOSÍTÁSA NAPJAINKBAN

HORVÁTH GYULA független távközlési tanácsadó mérnök

1101 BUDAPEST, PONGRÁC ÚT 17. F/8 ÉPÜLET, TEL/FAX: 262-8832

A távközlési szabványosításnak a CCITT Ajánlásainak hajdani egyeduralmával jellemzett korszaka napjainkra alaposan megváltozott. Új szabványosítók jelentkeztek, a szabványalkotó bizottságok a nagy gyártó vállalatok küzdőterévé váltak. A szabványok jogi vonatkozásai megváltoztak, egyhangú helyett többségi döntés, kötelező helyett önkéntes alkalmazás, szabadalmazott megoldások okoznak gondot a szabványalkotásban, változnak a szabványok és a minőség közötti összefüggések. Hazánkban a szabványügyet az Európai Unióhoz csatlakozás jegyében alakították át.

1. EGY KIS TÖRTÉNELEM

1.1. Az ITU-val kezdődött

A távközlést eredetileg nem szabályozták közhasználatú szabványok, csupán a magán (Egyesült Államok) vagy az állami tulajdonú (PTT) szolgáltatók követelték meg beszerzéseik alkalmával saját szabványaik betartását. Ennek elsődleges oka az volt, hogy a távközlés a XX. században a nyolcvanas évekig monopolhelyzetű vállalatok tulajdonában volt, ezért nem volt szükség a verseny szabályozásának országos hatású eszközeire, köztük szabványokra sem. A saját szabványok célja az együttműködő berendezések (pl. távírógépek, telefonkészülék, telefonközpont, átviteltechnikai berendezések) kompatibilitásának és minőségének biztosítása. Egyedül a nemzetközi távíró- és telefonforgalom szorult nemzetközi egyezmények alapján szabályozásra, amire a világ legrégebben működő kormányközi szervezetét, az ITU-t hozták létre. Ennek működése az egyes országok hálózatának összekapcsolásakor érvényesítendő műszaki követelmények és a nemzetközi díjelszámolás szabályainak kidolgozására korlátozódott. A nemzetközi szabvány [1] funkcióját betöltő Ajánlások de facto kötelezők, mert a kapcsolatos Ajánlásoknak nem megfelelő berendezések a nemzetközi forgalomban nem, vagy nem megfelelően működnek együtt. Utóbbi esetben az emiatt felmerülő többletköltségeket az említett egyezmény szerint annak a PTT-nek kell viselnie, amelyik a érintett Ajánlást nem tartja be.

1.2. Egységesség szabványok nélkül

A telefonszolgáltatás tömegszerűsége miatt mind a szolgáltatóknak, mind a használóknak egyaránt érdekükben áll a szolgáltatások egységessége, vagyis az, hogy mindegyik telefonról ugyanazon fajta hívást ugyanúgy lehessen felépíteni, a különféle eredetű és típusú általános célú telefonkészülékeket egyformán kezelni. Ezt a szolgáltatók belső szabványaiba és üzletszabályzatába beépített előírásokkal, ill. kikötésekkel biztosították.

A helyi telefonközpontok első generációjában (Strowger, Rotary stb.) nem szabványok, hanem a gyártók törekvése versenyképességük megőrzésére kényszerítette ki bizonyos jellemzők azonosságát (pl. a számtárcsa sebessége [10 impulzus/s], maximális hurokellenállás [kb. 1500 Ohm], kapcsolófokozatok forgalmi vesztesége [0,01 %] stb.). Egyetlen gyártó sem kockáztatta ugyanis, hogy ezekhez képest kedvezőtlenebb paraméterek megadása miatt versenyhátrányt szenvedjen.

1.3. Kinek kell és kinek miért nem kell szabvány?

Habár a szabvány egyik funkciója a kompatibilitás biztosításának eszköze, hozzá nem minden esetben fűzodik gazdasági vagy éppen üzleti érdek. Nem egyszer fordul elő, hogy valamelyik cég saját gyártóspecifikus megoldásához ragaszkodik, mert ezzel tudja versenytársait a már megszerzett piacról távol tartani. Például az automata telefonközpontok legelső generációjának tagjait szándékosan úgy alakították ki, hogy ne, vagy csak nagy nehézségek árán legyenek képesek egymással együttműködni. Ezzel láncolták magukhoz az egyszer már nagy nehezen megszerzett vevőt, gyakorlatilag egy egész ország monopolhelyzetű szolgáltatóját.

A crossbar technika gyártói már érdekeltek voltak abban, hogy központjaikkal a hagyományos vagy más gyártó crossbar technikájával már kiépített hálózatokat bővíteni lehessen. Hirdették tehát, hogy vállalkoznak más rendszerű központokkal való együttműködés kidolgozására. Az elektronikus központok piacán a kompatibilitás már igen nagy érték, mert rá hivatkozással a gyártók nagyobb piacra számítanak, a vevők a gyártóktól függetlenséget remélnek. Következésképen az utóbbi évtizedekben jelentősen megnövekedett a szabványok iránti igény. De ha a szabvány csak annyit tartalmaz, amennyi a kompatibilitás biztosításához szükséges, vagy amennyiben megegyezésre lehetett jutni, előfordul, hogy egy cég saját gyártóspecifikus megoldása mellett azzal érvel, hogy a szabványban rögzítettnél többet vagy jobbat nyújt. Hálózat esetén arra számít, hogy az egységesség előnyeinek megőrzése végett a későbbiekben a hálózatot az ő termékével fogják bővíteni.

Aggasztó jelenség, hogy bár az egyhangú szavazás igényéről már lemondtak és egyre több szabványosító testület a többségi szavazásra tért át, az egyetértés elérése egyre nehezebb. Ezt fejezi ki markánsan az NGN 97 konferencián feltett következő kérdés és magyarázata [2]:

„Az ATM él vagy meghalt? Az ATM problémája, hogy szinte lehetetlen mindenkit bármiben is egyetértésre bírni."

1.3.1. A szabványos és a gyártóspecifikus termékek versenye

A verseny színtere a szabványosító bizottságokban alakult ki. Ezekben az egyes gyártók saját részmegoldásaikat szeretnék a kidolgozás alatt álló szabvány részévé tenni, e célból harcba keverednek egymással. Előfordult, hogy éppen a szabványosítás során derült ki, hogy üzleti szempontból előnyösebb gyártóspecifikus megoldáshoz ragaszkodni. Ekkor a szabványos és a gyártóspecifikus megoldások a piacon kerülnek versenybe egymással. Például a G.729A szabvány (hangtömörítő/kicsomagoló kodek) elterjedését megakadályozta, hogy a megalkotásában részt vett cégek és intézmények nem tudtak megegyezni abban, hogy ki mennyiben járult hozzá a szabvány megalkotásához. A gyártók végül mellőzték a szabványt és visszatértek saját gyártóspecifikus megoldásaikhoz [3]. Emellett még nincs kizárva, hogy más cégek e szabvány szerinti termékükkel megnyerik a vevők ama részét, akik függetlenségük megőrzése végett szabványban rögzített kodekhez ragaszkodnak.

1.3.2. Szabadalmak és szabványok

Ha egy szabványba szabadalmazott, vagy szabadalmazásra bejelentett megoldást is javasolnak, akkor az ITU szabadalmi politikája szerint „a szabadalommal rendelkezőknek írásbeli nyilatkozatot kell tenniök, melyben vagy lemondanak a kapcsolatos szabadalmi jogaikról, vagy vállalják, hogy megkülönböztetés nélkül, ésszerű feltételek mellett licenc adásáról tárgyalnak." [4]. A kérdés súlyát mutatja, hogy 1998 végén az ITU már figyelmeztetett, hogy az IMT-2000 számára benyújtott CDMA-alapú RTT javaslatok figyelmen kívül hagyása várható, ha a CDMA javaslatok körüli vitákban a fentieknek nem megfelelő nyilatkozatok miatt kialakult patthelyzetet határidőre nem oldják fel.

2. SZABVÁNYOSÍTÁS A JELENBEN

Ezek után általánosan fogalmazhatjuk meg a szabványosítás tárgyát, célját, feladatát és hatásait.

2.1. A szabványosítás tárgya

A szabványosítás tárgya lehet bármely termék vagy szolgáltatás mindazon jellemzője és azok vizsgálati eljárásai, amelyek egységességét a szabványalkotók szükségesnek [5] tartják és amely jellemzők értékeiben megegyezésre képesek. Ebből az is következik, hogy ha nem sikerül egyetértésre jutni, akkor nem lesz szabvány, továbbá, hogy ha csak kevés kérdésben tudtak megegyezni, a szabvány a gyakorlatban alig lesz használható.

2.2. A szabványosítás célja, feladata

1. Gép–gép közötti interfészek kiválasztása, definiálása és előírása, melynek eredményeképpen azonos célra szolgáló termékeket és szolgáltatásokat különböző gyártók csereszabatosan vihetnek piacra; aminek előnyei:
- hálózatok vagy részeik különböző termelők, vagy ugyanazon termelő szabványos interfészekkel ellátott különféle típusaiból építhetők fel és konfigurálhatók át (kompatíbilis termékek),
- verseny alakulhat ki a szabványos termékeket gyártók, illetve a szabványos szolgáltatásokat nyújtók között,
- ezt kihasználva a vásárlók a gyártóktól, illetve a felhasználók a szolgáltatóktól műszakilag függetlenné válnak, mert bármelyiktől vásárolhatnak;
- jogi lehetőség nyílik arra, hogy ugyanazon szabványt elfogadó országok közül az egyikben elvégzett vizsgálat eredményét a többi ország is elfogadja.

2. Szolgáltatások és vizsgálatok (protokoll-vizsgálat is) egyöntetűségének biztosítása, ami
- a gyártók és a szolgáltatók (és/vagy használók) között lehetséges viták jó részét kizárja,
- megkönnyíti azonos vizsgáló eszközök és eljárások használatát a különböző vizsgáló helyeken.

3. Közérdekű ügyekben informatív jellegű szabványok rögzíthetik azokat a műszaki követelményeket, melyek teljesítését közérdek kívánja meg (elsősorban biztonsági előírások, pl. tűz- és érintésvédelem; továbbá annak megelőzése, hogy különböző rendeltetésű berendezések egymást zavarják, például EMC kompatibilitás ismérvei). Az ilyen szabványok tájékoztatják mind a gyártókat, mind a felhasználókat arról, hogy milyen műszaki feltételek fennállása esetén tekinthetjük helyzetünket biztonságosnak, illetve környezetünket zavarmentesnek.
4. Olyan fogyasztói érdekek védelmében, amelyek érvényesítésére a fogyasztónak nincs lehetősége, fogyasztóvédelmi intézkedésként bizonyos termékeket meghatározott szabványokban foglalt előírások betartásának ellenőrzése után engedi csak a hatóság forgalomba hozni, még az esettanulmányban leírthoz hasonló gondok kizárása végett is.
5. Az ember–gép interfész rögzítése elemi követelmény, avégett, hogy azonos rendeltetésű készülékek kezelése gyártó- és gyártmányfüggetlen legyen. Ezenkívül azt is okvetlenül el kell érni, hogy a használó az alábbiakat sohasem érezze:
- hogy elveszett (példa: a hálózat nem tájékoztatja a használót arról, hogy végberendezését impulzusüzemű jelzési módról DTMF módra kell átkapcsolnia),
- hogy csapdába esett (példa a keretes esettanulmány),
- hogy jogtalanul megterhelik számláját (példa: nem egyértelmű és hozzá nem biztosan eljuttatott értesítés a díjszabás megváltozásáról).

6. Műszaki alapok szolgáltatása:
- egyes termékek forgalmazásának hatósági engedélyezéséhez [6] vagy betiltásához [7],
- magánjogi szerződésekhez. Erre példa az az elterjedt gyakorlat, hogy szállítási, létesítési szerződésekben rögzített szabványok teljesítését megkövetelik,
- általános hatályú, köztük a már említett fogyasztóvédelmi és biztonsági hatósági intézkedésekhez a vonatkozó szabványok kötelezővé tétele útján [8].

2.3. Szabvány és jog

Tekintélyük ellenére a szabványok önmagukban még nem jogforrások, vagyis jogokat és kötelezettségeket önmagukban nem alapítanak. Jogforrássá közvetve válnak azzal, hogy alkalmazásukat jogszabályok, hatósági intézkedések, nemzetközi vagy magánjogi szerződések előírják. Erre való tekintettel azonban a szabványoknak a jogszabályokkal szemben támasztott követelményeknek meg kell

felelniük, vagyis egyértelműeknek, betarthatóknak (műszakilag megvalósíthatónak) és ellenőrizhetőknek kell lenniük. Utóbbiakra számos műszaki eszköz és eljárás áll rendelkezésre (főleg paraméterek megállapítása méréssel), melyek nagy részét szintén szabványosítják.

2.4. A szabványok nyelve

A szabványok szövegük egyértelműsége végett rendszerint tartalmazzák a bennük használt szakkifejezések meghatározásait. Ebben az értelemben a szabványokban értelmező szótár van elosztva. Ezen túlmenően a szabványkészítő szervezetek szívesen adnak ki terminológiai szabványokat. Az új fogalmak megnevezéseit meghatározásukkal együtt a szabványok széles körben terjesztik. Felelős nyelvújítást végeznek tehát a szabványok alkotói és a nemzetközi szabványokat nemzeti nyelvre fordítók, akiknek ki kell vívniuk, hogy az új szakkifejezéseket a hazai szakemberek el is fogadják. Könnyíti a helyzetet, hogy az idegen nyelvű kifejezés meghatározása magyarra fordítva a kapcsolatos fogalom magyar megnevezését egyúttal pontosan értelmezi. Az 1. táblázatban a vezetékes távközlésre vonatkozó, hazánkban elérhető idevágó kiadványokat találjuk. Bár a későbbi kiadványok készítésekor a korábbiak tartalmát részben felhasználták, a felsorolt kiadványok szóhasználatának egységesítése még várat magára.

1. táblázat. A magyar terminológia forrásai [28]

A KIADVÁNY		
kiadásának éve	kiadója	címe
1964	TERRA	Barta – Kozma: Híradástechnika – Műszaki Értelmező Szótár
1972	KTE	PCM szótár
1978	Műszaki Könyvkiadó	Lajkó – dr. Lajtha: PCM a távközlésben, F.2 függelék
1983	Akadémiai Kiadó	Rédl – Oldal: Műszaki Értelmező Szótár
		Elektronika, Híradástechnika, Vákuumtechnika, I.-II. kötet
1988	KÖZDOK	Távközlési fogalmak és meghatározások (közismert nevén „Szürke könyv")
1994	MSZH	701. Kötet: Távközlés, csatornák és hálózatok (MSZ IEC 50)
1994	Távközlési Könyvkiadó	Távközlési Tezaurusz
1995	Távközlési Könyvkiadó	A távközlési szolgálatok fogalmai és meghatározásai
1995	Távközlési Könyvkiadó	Rétegnyelvi szógyűjtemény, magyar – angol és angol – magyar
1996	HIF	ISDN szakkifejezések értelmező szótára
1996	Távközlési Könyvkiadó	Földes – Reich – Zimányi: Angol betűszavak feloldó szótára [29]

KTE = Közlekedéstudományi Egyesület, KÖZDOK = Közlekedési Dokumnentációs Vállalat, MSZH = Magyar Szabványügyi Hivatal, HIF = Hírközlési Főfelügyelet

3. SZABVÁNYALKOTÁSI MODELLEK

3.1. Nemzetközi modell

A CCITT Ajánlásainak megalkotói törekedhettek a tökéletes megoldás megtalálására, mert a fejlődés akkori tempója ezt megengedte [9]. Az Ajánlások, nagy tekintélyük miatt a nemzetközi köztudatban egyre inkább mint világszabványok jelentek meg, amelyekre kényelmes volt a belföldön használandó berendezések megrendelésekor is hivatkozni, különösen a műszakilag kevésbé fejlett országokban [10]. Amikor pedig az állami szabványosító szervezetek ragaszkodtak ahhoz, hogy a távközlés területén is legyenek országos szabványok, akkor az éppen használatos berendezések jellemző műszaki adatait gyűjtötték össze.

3.2. Európai modell

Amióta az Európai Unió regionális szabványosító központként az ETS-t létrehozta, kialakult a korábbi, mára elavult európai modellnek [11] korszerű változata. Erre az egyes alapvető műszaki megoldásokat (példákat lásd a 2. táblázatban) hézagmentesen specifikáló szabványkészletek jellemzők, amelyeket az Európai Unió nem tekint kizárólagosaknak, hanem csak az egyik lehetséges konstrukció leírásának. Ezzel a szemlélettel Európa megelőzte a világot [12].

3.3. Amerikai modell

A nemzetközivel szemben az Egyesült Államokban kialakult „amerikai modell" a ‚tökéletes" helyett megelégszik a lehető legjobb megoldással azért, hogy a szabvány mielőbb megszülethessen. Egy másik oldalról nézve, a nemzetközi modell a nemzeti hatóságok, az amerikai modell az érdekeltek egyetértésén alapul, további oldalról nézve a kötelező, illetve az önkéntes szabályozás elvét valósítja meg.

Az amerikai modell egyik jellegzetessége, hogy az állami szabványosító intézet (ANSI) mellett szabványokat e célra szakosodott, magánkezdeményezésen alapuló szervezetek is készítenek. Ezek eleinte egymással versengő magánvállalatok voltak, amelyek szabványaik eladásából élnek, tehát érdekük, hogy szabványaikat minél több gyártó és felhasználó önként elfogadja, mert maga számára hasznosnak találja. Az egyes magán szabványalkotó vállalatok szabványainak megfelelő termékek minőségi szintje gyakran eltérő. Ez a szolgáltatók és a végfelhasználók számára lehetővé teszi az adott esetben megfelelő minőségű terméket leíró szabvány kiválasztását. Ezeknek a magánvállalatoknak rugalmasan kell alkalmazkodniuk az új igényekhez, amit a szabványosítási munkában résztvevő szakértők gondos kiválasztásával, csapatmunkájuk hatékony megszervezésével, döntéshozatalkor a többségi elv alkalmazásával érnek el.

2. táblázat. Rövidítések

ANSI	American National Standardization Institute Amerikai Országos Szabványosítási Intézet
CDMA	Code Division Multiple Access
CCITT	Comité Consultatif International Télégraphique et Téléphonique Nemzetközi Távíró és Távbeszélő Tanácsadó Bizottság <új neve: ITU-T>
CTR	Common Technical Regulation Közös Műszaki Szabályozás <az EU által kibocsátott kötelező jogszabály, amelytől a nemzeti szabályozás nem térhet el; alapja a TBR>
DECT	Digital Enhanced Cordless Telecommunications <eredetileg Digital European Cordless Telecommunications, új nevét az ETSI-től kapta> <európai digitális zsinórnélküli távközlés>
DPNSS	Digital Private Network Signalling System Digitális Magánhálózati Jelzésrendszer
DTMF	Dual Tone Multiple Frequency [signalling] <két hangfrekvenciás jelzésátvitel az ITU-T Q.23 Ajánlása szerint [30]>
E-ISDN	Euro-ISDN Európai ISDN <az ETSI szabványai szerint>
ECMA	European Association for Standardising Information & Communication Systems <Információs és Kommunikációs Rendszereket Szabványosító Európai Szövetség> <előző neve: European Computer Manufacturer's Association, Európai Számítógépgyártók Szövetsége>
ETS	European Telecommunication Standard Európai Távközlési Szabvány <kiadja az ETSI, nemzetközileg nem kötelező, nemyeti változatai között eltérések lehetségesek>
ETSI	European Telecommunications Standards Institute Európai Távközlési Szabványosítási Intézet <alapvető termékei: CTR, TBR, ETS; legfontosabb sikerei: E-ISDN; a világszabvánnyá válás útján lévő GSM, DECT és TETRA szabványok>
EU	European Union Európai Unió
GSM	Global System for Mobile Communication <eredetileg Group Special Mobile, új nevét az ETSI-től kapta> <világméretű mobil hírközlő rendszer>
IEC	International Electrotechnical Commission Nemzetközi Elektrotechnikai Bizottság
IM-2000	International Mobile Telecommunication 2000 <szabvány kidolgozás alatt>
INTUG	International Telecommunications Users Group Távközlési Felhasználók Nemzetközi Csoportja
ISDN	Integrated Service Digital Network Integrált Szolgálatú Digitális Hálózat
ISO	International Organisation for Standardisation Nemzetközi Szabványügyi Szervezet
ITU	International Telecommunication Union Nemzetközi Távközlési Egyesület
ITU-T	ITU – Telecommunication Standardisation Sector Távközlési Szabványosítási Ágazat
MoU	Memorandum of Understanding Szándéknyilatkozat <(legkevésbé szoros) együttműködési megállapodás>
MSZT	Magyar Szabványügyi Testület <a Magyar Szabványügyi Hivatal jogutódja>
PTT	Postal, Telegraph and Telephone Authorities (Administration) Postai Távíró és Telefon Hatóság (Igazgatás); <az országok saját nyelvén ismert, postai, távíró- és telefonszolgálatot nyújtó állami vállalatok közös nemzetközi rövidítése>
Q-SIG	<jelzésátviteli protokoll az ISDN referencia/modell Q interfészén> <a Q interfész két ISDN alközpontot összekötő társközponti vonalon van>
RTT	Radio Transmission Technologies
TBR	Technical Basis for Regulation A szabályozás műszaki alapjai <ezekre hivatkoznak a CTR-ek>
TBT	Technical Barriers of Trade Kereskedelem Műszaki Akadályai
TCP/IP	Transmission Control Protocol/Internet Protocol <átviteli vezérlő protokoll/Internet protokoll>
TETRA	Terrestrial Trunked Radio <eredetileg Trans European Trunked Radio, új nevét az ETSI-től kapta> <földfelszíni nyalábolt rádió>
URL	Universal Resource Locator <univerzális erőforrás helymeghatározó (szerverek Internet címei)>
WTO	World Trade Organisation Világkereskedelmi Szervezet

Megjegyzés: A < > közötti szövegek nem hivatalos fordítások vagy magyarázatok.

Az amerikai modell az Egyesült Államok világgazdasági helyzetének felel meg: a világ eme legnagyobb méretű nemzeti gazdasága megengedheti magának, hogy a saját körülményei között legeredményesebb módszereket alkalmazza, nem szorul mások szempontjai szerint kidolgozott szabványokra (lásd például a SI nemzetközi mértékrendszertől eltérő mértékegységek használatát). Ugyanebbe a helyzetbe kerültek – nemcsak Amerikában – gyártó nagyvállalatok is, amelyek Fórum, MoU és más elnevezésekkel egy körülhatárolt témakörben szabványok készítésével is foglalkozó közös munkacsoportokat alakítottak. Ezek lényegében az amerikai modell szerint működnek és nem egyszer más szabványosító szervezetek alvállalkozóiként szerepelnek [13].

Az amerikai szabványosítási kultúrára az is jellemző, hogy szívesen fogadnak el de facto szabványokat, vagyis egy gyár jól sikerült konstrukcióját. Erre legismertebb példa az először az IBM által kidolgozott személyi számítógép.

Távbeszélő-központok száma

(darab)

Megnevezés	1991	1992	1993	1994*	1995	1996	1997
Távbeszélő-központok száma összesen	1714	1680	1735	1774	1928	1797	1731
ebből:							
Előfizetői	..	..	1626	1729	1841	1698	1660
Kombinált	..	..	52	54	49	72	53
Tranzit	..	..	58	46	38	27	18
Automata összesen	652	688	879	1194	1581	1652	1731
ebből:							
Digitális	..	..	249	519	861	1061	1223
Elektromechanikus	581	599	630	570	603	485	412
Kézi összesen	1062	992	856	580	347	145	–

*Az adatok bizonytalanok a megváltozott tulajdonosok és nyilvántartások miatt.

Távbeszélő-központok kapacitása

(ezer vonal)

Megnevezés	1991	1992	1993	1994*	1995	1996	1997
Kapacitás összesen	1383	1603	1970	2335	2951	3453	3833
ebből:							
Automata összesen	1363	1526	1902	2271	2913	3443	3833
ebből:							
Digitális	108	262	640	..	1679	2246	2694
Elektromechanikus	1196	1264	1262	901	903	888	904
Kézi	80	77	68	52	39	10.3	–

*Az adatok bizonytalanok a megváltozott tulajdonosok és nyilvántartások miatt.

Távbeszélő-forgalom

(millió darab)

Megnevezés	1991	1992	1993	1994	1995	1996	1997
Beszélgetések száma	1464	1638	1837	2074	3090	3438	3791
ebből a hívó fél jellege szerint							
egyéni állomásról	687	775	830	916	1515	1685	2090
üzleti állomásról	635	712	840	972	1382	1547	1469
nyilvános állomásról	142	151	167	186	193	206	232
A hívás fajtája szerint							
helyi	1170	1298	1442	1576	2098	2340	2329
belföldi	254	289	334	425	923	1027	1383
nemzetközi távhívás	40	51	61	73	69	71	79

Forrás: HIF Távközlés-statisztikai évkönyv, 1997

Bekapcsolt fővonalak megoszlása

Megnevezés	1991	1992	1993	1994	1995	1996	1997
Használók szerint							(ezerl)
Fővonal összesen	1128	1291	1498	1785	2157	2651	3095
ebből:							
Lakásfővonal összesen	819	951	1135	1399	1742	2208	2627
Üzleti fővonal összesen	282	312	332	352	377	402	426
Nyilvános fővonal összesen	26.8	28.3	30.6	33.9	37.4	40.5	42.3
Várakozók száma	658	754	772	719	683	234	50
ebből:							
félévnél régebben	–	–	–	–	–	137	18
lakás-állomásra	608	678	703	718	633	245	40
Állomás típusok szerint							
Különvonalú	654	786	1021	1343	1827	2354	2861
Ikervonalú	474	505	476	442	330	310	234
ISDN	–	–	–	–	1	11	39
Központ gépesítettség szerint							
Automata kapcsolású	1069	1232	1445	1735	2133	2640	3095
ebből:							
Digitális összesen	82	159	397	706	1178	1749	2300
Analóg összesen	10	10	11	42	210	228	125
Elektromechanikus összesen	977	1063	1037	987	745	663	670
Kézi kapcsolású	59.4	59	53	50	23.6	10.6	..
Gépesítettség foka (%)	94.7	95.4	96.5	97.1	98.8	99.6	100

Távközlő hálózat nyomvonalhossza

				(1000 vonal-km)			
Megnevezés	1991	1992	1993	1994	1995	1996	1997
Fém-vezetőjű távközlő-hálózat hossza							
Föld feletti összesen	36.8	40.7	45	46.9	39.7	40.7	85
ebből:							
helyi	23.3	27.8	32.6	35.6	30.2	32.6	76
helyközi	13.5	12.9	12.4	11.3	9.5	8.1	8.7
Föld alatti összesen	75.6	78.9	83.5	91.5	107.7	109	113
ebből:							
helyi	60.0	62.4	66.4	71.6	87.5	94.9	98
helyközi	15.6	16.5	17.1	19.9	20.2	14.1	15
Fény-vezetőjű távközlő-hálózat hossza							
Összes fény-vezetőjű	..	..	..	..	5.9	9.4	13.5
Mikrohullámú távközlő hálózat hossza							
Mikrohullámú összeköttetések összesen	..	..	..	..	15.6	19.3	*23

*Becsült érték a hiányos adatszolgáltatás miatt.

Forrás: HIF Távközlés-statisztikai évkönyv, 1997

Országos közcélú távbeszélő-ellátottság településkategóriánként – 1991–1997

Település-kategóriák	100 lakosra jutó fővonalak						
	1991	1992	1993	1994	1995	1996	1997
–500 lakos	2.39	3.58	4.64	7.43	10.77	15.33	20.59
501–1000	2.56	4.25	4.75	7.52	10.75	15.21	21.59
1001–1500	2.79	3.93	5.46	7.62	10.44	15.26	21.47
1501–3000	2.82	4.47	6.45	8.76	11.17	15.36	21.90
3001–5000	4.10	5.09	7.07	9.86	13.37	18.10	23.70
5001–10 000	4.38	6.03	8.24	10.08	12.82	18.41	24.48
10 001–20 000	6.07	7.94	9.67	12.86	15.60	21.23	26.40
20 001–35 000	7.04	8.01	11.13	13.19	15.28	21.37	28.93
35 001–50 000	9.15	10.57	14.77	17.87	32.78	25.33	28.72
50 000–	18.35	20.94	25.71	28.77	32.82	37.27	42.50
összesen	9.95	11.85	14.87	17.55	21.11	25.54	31.15

Távbeszélő-ellátottsági jellemzők – 1997

Település-kategóriák	Települések száma	Igénylők száma	Igénylőknek a bekapcsolt vonalakhoz viszonyított aránya
–500 lakos	1001	4 554	7.96
501–1000	713	7 261	6.45
1001–1500	377	6 556	6.66
1501–3000	569	16 068	6.12
3001–5000	198	9 283	5.27
5001–10 000	134	14 708	6.48
10 001–20 000	77	13 020	4.51
20 001–35 000	33	14 559	5.57
35 001–50 000	7	2 129	2.51
50 000–	20	39 368	2.44
összesen	3129	127 506	4.01

A közcélú távbeszélő-szolgáltatás minőségi adatai

Megnevezés	1991	1992	1993	1994	1995	1996	% 1997
Sikertelen hívások aránya							
körzeten belül (TBM4)	9.25	7.94	6.16	4.87	2.88	2.03	1.75
belföldi távhívások (TBM5)	25.31	20.63	10.49	7.86	4.69	3.56	2.16
nemzetközi távhívás (TBM6)	22.20	17.15	8.35	6.23	3.33	1.87	1.16
Közönségszolgálati munkahelyek 30 mp-en belüli jelentkezésének aránya (TBK2)	60.74	75.19	75.99	85.25	86.91	90.94	94.58
A híváskezdeményezéstől számított 12 mp-en túl érkezett tárcsahang aránya (TBM3)	13.68	5.12	2.34	0.95	0.03	0.05	0.08
Nyilvános távbeszélő-állomások üzemkészsége (TBK1)	72.40	80.62	83.34	87.52	91.27	94.55	95.37
Előfizetői hozzáférés létesítése iránti igény teljesítésének átlagos ideje (TBE4) [év]	3.91	3.20	2.90	2.30	2.20	1.80	1.30

Forrás: HIF Távközlés-statisztikai évkönyv, 1997

Villamos Elosztó'99

BUDAPEST, 1999. MÁRCIUS 17-18.
BME SCHÖNHERZ KOLLÉGIUM

A Villamos Elosztó99 elnevezésű állásbörzén célzottan a Villamosipari és informatika szakma, illetve a végzős mérnökhallgatók találkozását szeretnénk lehetővé tenni. Az állásbörze idén a hatodik alkalommal kerül megrendezésre a Budapesti Műszaki Egyetem Schönherz Kollégiumában, amely közel 1000 villamosmérnök és informatikus hallgatók "otthona". Ebben a tanévben mintegy 1500 hallgató érdeklődését várjuk, akik a kar, illetve más egyetemek és főiskolák végzős diákjai.

Helyszín: Budapest, XI. Irinyi József u. 42.
Kollégium nagytermei

További információk a rendezvényről:

Almás Béla főrendező
Tel: 372-51-05
Fax: 372-51-59
e-mail:eloszto@sch.bme.hu

The Blue House
Budapest

További jellemzője rokonszenv az ITU által is alkalmazott minimális szabályozás elve iránt, melynek szélsőséges példája az Internet, amellyel kapcsolatban csak a TCP/IP és az URL, valamint a domain-nevek megalkotása és kiosztása van szabványosítva [14].

3.4. Szabványok elfogadása

Bármelyik modellt is követik, a szabványalkotók megállapodhatnak abban, hogy a végső döntéseket egyhangúlag, vagy többségi szavazatok alapján hozzák meg. Az ITU-ban, mint kormányközi szervezetben, eddig az egyhangúság elve érvényesült, de felülvizsgálatával már foglalkoznak. Az ETSI-ben súlyozott szavazással döntenek [15], az egyre szaporodó Fórumokon a többségi szavazás más formáit is alkalmazzák. A szabvány természetének jobban megfelelő egyhangúságtól gyakorlati okból, a munka meggyorsítása végett térnek el.

A gyakorlatban e két modell alkalmas kombinációja célravezető. A 3. táblázat foglalja össze azokat a területeket, ahol az egyik, vagy másik modell követése látszik szerencsésnek.

3. táblázat. Szabványkészítés

Európai (nemzetközi) modell	Amerikai modell
Élet- és vagyonbiztonság, zavarvédelem (EMC stb.)	Korlátozott mélységű szabályozás, a verseny elősegítésére
Fogyasztók által nem érvényesíthető igények (szolgáltatásminőség, egyöntetű kezelés stb.), interfészek rögzítése	Korlátozott szakterület (például értéknövelt szolgálatok, ATM) szabványainak kidolgozása
Nemzetközi és szolgáltatók közötti hívások műszaki, forgalmi és díjelszámolási előírásai	Gyári belső műszaki előírások elfogadása *de facto* szabványként

4. SZABVÁNYOK ÉS A TERMÉKEK MINŐSÉGE

4.1. Minőségi rendszer

A szabványos termékek minőségével szemben támasztott követelmények megfogalmazása és teljesítésük ellenőrzése a vevő dolga. Utóbbi megkönnyítésére vezetik be napjainkban a minőségbiztosítás és a minőségirányítás tevékenységeket összefoglaló minőségügyi rendszereket, melyek alapvető célja, hogy a gyártásból hibás termék kibocsátását gyakorlatilag eleve megakadályozzák, és hogy erről arra feljogosított intézmények tanúsítványt adhassanak ki.

4.2. ISO 9000 szabványsorozat

A minőségügyi rendszerek kialakítására az ISO 9000 sorozatú nemzetközi szabványokat dolgozták ki [16]. A minőségügyi rendszerekkel, megvalósításukkal és a tanúsítási eljárással bőséges irodalom foglalkozik [17]. Ezen szabványok szerinti tanúsítvány azonban nem jelenti azt, hogy birtokosa meghatározott minőségű, bármilyen szabványnak is megfelelő terméket gyárt vagy szolgáltatást nyújt. A távközlő berendezések EU szintű típusjóváhagyásáról EU direktívák intézkednek [6].

5. SZABVÁNYOSÍTÁS MAGYARORSZÁGON

5.1. A megújult törvény

Hasonlóan azokhoz az országokhoz, amelyekben a távközlési szolgálatot monopolhelyzetű állami tulajdonú vállalat látta el, nálunk is ágazati szabványként a Magyar Posta előírásai érvényesültek. A nemzeti szabványosításról szóló 1995. évi XXVIII. törvény megszüntette az ágazati szabványokat, ezek és az állami szabványok helyébe nemzeti szabványok léptek [18]. Ezek alkalmazása általában nem kötelező, csak akkor, ha miniszteri rendelet – a hatáskörébe eső területen – kötelezővé nyilvánítja. Természetesen magánjogi szerződésben bármely szabvány alkalmazását ki lehet kötni. A távközlési törvényen kívül a KHVM rendeletei is jelentős jogforrások. Legújabban a Hírközlési Főfelügyelet is elkezdte – nem kötelező – Ajánlások kibocsátását [19].

5.2. Európai szabványok honosítása

Az új törvény intézkedései az EU-hoz csatlakozás előkészítéseként születtek. Az EU szabványokat magyar nemzeti szabványként a következő módszerekkel lehet bevezetni [20]: elsősorban szöveghű bevezetés; ha nem lehetséges, akkor másodsorban jóváhagyó közleménnyel bevezetés, és ha ez sem lehetséges, akkor átszerkesztéses bevezetés (pl. amikor szükséges, hogy a magyar nemzeti szabvány több vagy kevesebb, szigorúbb vagy enyhébb előírásokat tartalmazzon).

A távközlés területén több magyar szervezet tagja az ETSI-nek, amiből következően kötelesek az ETS-eket honosítani. Nagy tömegükre való tekintettel legtöbbször egynyelvű (angol), szöveghű bevezetésükre kerül sor, mert pontos lefordításukhoz sem megfelelő fordítói kapacitás, sem elegendő pénz nem áll rendelkezésre. További egyszerűsítésként bevezették az ún. jegyzékes bevezetést is, ami egyszerűen abból áll, hogy a Szabványügyi Közlönyben jegyzékben felsorolt szabványokról közzéteszik, hogy azok egyúttal érvényes magyar szabványok is. Ezek hivatalos magyar fordítására egyelőre tehát nem lehet számítani. Az angol nyelvű bevezetés azt jelenti, hogy esetleges jogvitában az eredeti angol szöveg irányadó. Mivel az ETS-eket használó szakemberek jelentős része tud angolul, e szabványok használata nem sok nehézségbe ütközik. Ha pedig hivatalos eljáráshoz (pl. polgári per) hiteles magyar fordításra van szükség, elegendő azt az okvetlenül szükséges terjedelemben elkészíteni. Véleményem szerint ezzel az első pillantásra furcsa helyzettel meg kell barátkoznunk. Amikor már látni lehet, hogy mely szabványokra van tartósan vagy széles körben szükség, indokolt ezeket lefordítani. Ésszerű, hogy a fordítás költségeihez a szabványok eladásából származó bevétel észrevehetően hozzájáruljon [21].

5.3. Termékfelelősség

Nem maradhat említés nélkül, hogy a termékfelelősségről szóló, az EU előírásaival azonos termékfelelősségi törvény (1993. évi X. törvény) kimondja, hogy „a termék gyártója felel a termék hibája által okozott kárért." Az EU bevezetés alatt álló irányelvei (direktívái) szerint pedig „a szabványok előírásainak megfelelő termék nem tekinthető hibásnak." Eszerint a gyártó mentesül a szabványos terméke által okozott kárból eredő kárfelelősség alól. Fokozott érdeke lesz tehát önként szabványos termékeket gyártani, azokba szükség szerint más gyártók szabványos termékeit beépíteni. Ugyanakkor ezt a túl általánosan megfogalmazott szabályt még finomítani kell. Köztudott például, hogy a mai bonyolult szoftverek hitelesítése (verifikálása) és érvényesítése (validálás) teljes mértékben nem lehetséges, mert a bemenő jelek összes lehetséges kombinációjának előállítása és a hozzátartozó kimenő jelek ellenőrzése elviselhetetlenül hosszú időt igényelnek. [22] Előfordulhat tehát, hogy egy telefonközpont, vagy egy átviteli út a szoftver hibájából átmenetileg használhatatlanná válik, és emiatt az üzleti használók nagy károkat szenvednek el [23]. Lehet-e ezért a szoftvergyártótól kártérítést kérni?

6. KÖVETKEZTETÉSEK

A nemzetközi szabványosításban a legnagyobb gyártók igyekeznek, hogy saját konstrukciójuk legalább részben de facto szabvánnyá váljék, ezért a szabványosító szervezetekben igyekeznek a vezető szerepet nagy mértékben átvenni. Evégett mind a hagyományos, mind az új szabványosító szervezetekben befolyásukat erőteljesen növelik. Erre a törekvésre a hagyományos (ITU, ETSI) szervezetek erőteljes reformokkal és szoros együttműködéssel válaszolnak. A három nemzetközi szervezet, az ISO, az IEC és az ITU vezetői minden évben, a szabványosítás napján kiadott Üzenetükben festi le a világméretű szabványosítás helyzetét és jelöli meg az aktuális tennivalókat (lásd keretben).

Bizonyos termékeket, megoldásokat egyes gyárak még azok szabványosítása előtt kidolgoznak. Ezzel érdekeltté válnak a szabványosítás késleltetésében, hogy vevőiket gyártóspecifikus megoldásukhoz lakatolják. A többi gyár viszont a vevők szabadsága mellett tör lándzsát azzal, hogy a szabványosítást sietteti [24]. Egyre több termék kifejlesztése már a szabványosítási folyamat alatt megindul (pl. DPNSS), de van példa arra is, hogy csak a szabványosítás befejezése után (Q-SIG).

Miközben a szabványosító bizottságok a piacokért folytatott verseny színterévé válnak, a használók érdekeinek érvényesítése gyengül. Ezzel kapcsolatban a nagyvállalatok magatartása kétarcú: marketing tevékenységük egyik része a felhasználók igényeinek kutatása, másik része a kifejlesztett termékek elfogadtatása. Lényegi céljuk itt is gyártásuk jövedelmezőségének (nagy sorozatok) és piaci erejük fokozása. A néhány meglévő civil fogyasztói érdekvédelmi szervezet (pl. az INTUG) alig jut szóhoz a szabványosító szervezetekben, pedig legalább az ember–gép interfésszel kapcsolatban előbb felsorolt, tulajdonképpen az előfizetők által támasztott követelményeknek kellene érvényt szereznüük.

Hazánkban a Fogyasztóvédelmi Főfelügyelet egyelőre csak eseti ügyekben tud fellépni (kirívó panaszok szolgáltatókkal szemben, egyes termékek forgalmazásának vagy használatának betiltása). Valamivel több várható a Távközlési Érdekegyeztető Fórumtól, hatékony munkamódszereinek kialakulása után. Az ETS-ek honosítása során a Hírközlési Főfelügyeletnek van hathatós lehetősége fogyasztói érdekek érvényesítésére.

Új probléma a szabványokban megtestesülő szellemi tulajdon védelme. Arról az esetről van szó, amikor egy szabvány előírásainak betartásához valamely szabadalom felhasználása elkerülhetetlen. Az ilyen esetekkel eddig nem törődtek [2], [25], a fennálló problémák azonban egyre nagyobb gondokat okoznak. (Maguk a szabványok szintén szellemi tulajdon tárgyai, amit tulajdonosaik, ha kívánják, a sokszorosítás, harmadik félnek átadás stb. megtiltásával megfelelő záradék útján [24] biztosíthatják.)

Az európai cégek megjelenése Amerikában, az amerikai cégek aktivitása Európában segíti a kétféle modell célszerű alkalmazását. Jelentős előrelépés a minimális szabályozás elvének terjedése, továbbá annak deklarálása, hogy a szabványok alkalmazása alapvetően önkéntes, de megvan a kötelezővé tétel mechanizmusa is. E tekintetben a magyar szabályozás jó, mert a miniszterek egyenként jelölhetik ki az illetékességi körükben kötelező szabványokat és kijelölésüket a törvényben meghatározott módon meg is változtathatják.

Az ISO 9000 szabványsorozat csak a kiváló minőségű gyártásra való felkészültség tanúsítási eljárását szabványosítja. Tanúsított ISO 9000 rendszer néhány év alatt elérhető, míg egy sikeres minőség-központú irányítási rendszer bevezetése átlagosan tíz évet igényel. [26] Ezután viszont a termék vevői a bejövő árú minőség-ellenőrzést mellőzhetik. Az így elért költségcsökkenés megosztása a beszállítóval a piaci erőviszonyok függvénye lesz [27].

Sok műszaki feladat széles körben elfogadott általános megoldását koncepcionális szinten szabványokból tudhatjuk meg. A legalább műszaki leírás szintjén ismert konkrét termékek számunkra fontos tulajdonságaira (például egymás közötti kompatibilitására) a vonatkozó szabványok ismeretében következtethetünk.

7. ESETTANULMÁNY (PÉLDA A CSAPDÁRA)

Alközpontokban városi beszélgetés közben hagyományosan a földelőgomb, újabban a flash gomb lenyomásával a használó egyértelműen jelzi a központnak, hogy visszahívást kezdeményez, tehát az ezután tárcsázott számokat mellékállomás számaként kell értelmeznie. Ez az eljárásmód megfelel az ember–gép interfésszel szemben támasztott elemi követelményeknek. Újabb elektronikus központokban ezt a jelzést időzítéssel helyettesítik, aminek időtartamáról gondos cégek a használót a készülék kezelési utasításában tájékoztatják. A hazánkban forgalomban lévő alközpontok nem mindegyike ilyen, használójukat kellemetlen meglepetések érték. Amikor ugyanis kimenő hívás közben az időzítést meghaladó szünetet tartottak, a további számjegyeket a központ helyi számként értelmezte és egy, esetleg kényelmetlen, de mindenesetre zavaró helyi kapcsolatot létesített. Ez előfordulhat akkor is, ha közvetett beválasztásra berendezett alközpontot hívnak, mert ekkor a csengetés, valamint a bejelentkezés alatt az időzítés könnyen lejárhat. E bosszúság megelőzése végett cél-

szerű lenne, ha e problémáról és elfogadható megoldásairól az érintettek nemzetközi szabványból értesülnének.

8. ÜZENET A SZABVÁNYOSÍTÁSI VILÁGNAP ALKALMÁBÓL [31]

1998. október 14.

Bár többnyire csak akkor gondolunk a szabványokra, amikor ezek hiánya okoz kellemetlenséget, valójában nehéz elképzelni a mindennapi életet szabványok nélkül. Képzeljük bele magunkat bármilyen szituációba, meg leszünk lepve, hogy milyen sok szabványra támaszkodik a mindennapi épet ezerféle mozzanata. Attól a pillanattól kezdve, hogy reggel felébredünk, egész nap szabványok segítenek – más-más formában – napi teendőink ellátásában, abban, hogy amit teszünk, könnyebb, kényelmesebb, biztonságosabb és kellemesebb legyen.

Képzeljük el például: milyen kellemetlen lenne, ha nem tudnánk pénzt kivenni egy bankkártya automatából, mert a kártya nem fér be a nyílásba, vagy ha az elem nem illik elektromos készülékünkbe, vagy mit kezd az áruház azzal az áruval, amelyen nincs vonalkód, és nem tudni a tömegét és az árát, s vajon hogyan lehetne az Internetet használni, ha nem létezne szabványos helymegjelölés. Manapság, amikor elvárjuk, hogy a kommunikáció gyors és hatékony legyen, biztosítani kell a villamos készülékek csatlakozását és együttes működését, és ugyanakkor azt is elvárjuk, hogy eszközeink, fogyasztási cikkeink és termékeink olcsóak, könnyen beszerezhetők és kiváló minőségűek legyenek. Ehhez feltétlenül szükség van nemzetközi szabványokra, még akkor is, ha ezek szerepe többnyire láthatatlan és magától értetődőnek tűnik. Ha betöltik szerepüket, eszünkbe sem jut, hogy minket nemzetközi szabványok védtek meg a bosszúságtól.

Az „utca emberének" szemében a szabványok valamiféle mércét képviselnek, amelyet mintául választottak, hogy tárgyakat vagy cselekedeteket hasonlíthassunk össze velük.

A végső felhasználónak megmutatják: milyen kritériumok alapján ítélkezhet, lehetőséget adnak a minőség mérésére, és bizonyos mértékig garantálják a csatlakoztathatóságot, a közös használatot más termékekkel. A nemzetközi szabvány a mindennapi élet szilárd oszlopa, akár azt a szabványt vesszük példaként, amely a telefonhálózatban teszi lehetővé a kapcsolatot, vagy azt, amely az elektromágneses tűrőképességen belüli orvosi műszer segítségével életet ment a kórházban, vagy épp azt, amely a vállalatot segíti abban, hogy a minőséget kézben tartsa és a környezetet kímélje. Az élet minőségét javítja azzal, hogy hozzájárul biztonságunkhoz, egészségünk és környezetünk védelméhez.

A szabványok azért olyan hasznosak a mindennapi életben, és azért olyan kiterjedt az alkalmazási körük, mert a mindennapi élet tapasztalataira támaszkodnak, a különböző helyeken és területeken működő emberek igényei alapján készülnek. A szabvány tehát a tapasztalat eredménye, amely megkeresi a használható kompromisszumot a technika mai állása és a gazdasági korlátok között.

A nemzetközi szabványok közmegegyezésen alapuló dokumentumok, amelyeket nemzeti vagy regionális szinten önkéntes alapon fogadnak el. Az ISO, az IEC és az ITU, amelyek szabványalkotói működési körei egymást kiegészítik, együtt az önkéntes nemzetközi műszaki megegyezések kialakításának teljes rendszerét képviselik. Akár nemzetközi szabvány, akár ajánlás néven jelennek meg ezek, a megállapodások, mindig azt célozzák, hogy a technika világméretekben kompatíbilis legyen. Ha gépek, rendszerek vagy készülékek együtt tudnak működni, azt többnyire a nemzetközi szabványoknak köszönhetjük, akkor is, ha nem gondolunk rájuk.

A szabványok azért készülnek, hogy kielégítsék a mai igényeket: a három szervezet munkaprogramja pedig azt a célt szolgálja, hogy a holnapi igények számára is rendelkezésre álljanak a nemzetközi szabványok, a nap mint nap megújuló technika örökké változó spektrumában is.

Mr. Liew Mun Leong (ISO) Mr. Bernard H. Falk (IEC) Dr. Pekka Tarjanne (ITU)

JEGYZETEK ÉS IRODALOM

[1] dr. Gosztonyi Géza: Az ITU-T Ajánlás – valójában szabvány. Magyar Távközlés, 1995/5

[2] McQuillan: Beszámoló az NGN 97 konferenciáról. Business Communication Review, 1989/1

[3] Alan Joch: Megszólalnak az adathálózatok. BYTE Magyarország, 1. kötet, 1. szám (1997 dec.)

[4] Forrás: ITU/98-34 Sajtótájékoztató.

[5] ETSI tapasztalata szerint nem mindig elegendő az interfészeket szabványosítani, mert egyre gyakrabban mutatkozik szükségesnek az interfészek vizsgálati módszereinek kiterjesztése a végtől-végig operabilitás ellenőrzésére. (Keselyák Péter közlése.)

[6] Szathmáry Csaba: Távközlési végberendezések engedélyezése az EU-ban. Magyar Távközlés, 1997/3

[7] Például Szingapúrban a GSM 900 MHz-es sávjában működő zsinórnélküli telefonok és távmegfigyelő video-kamerák behozatalát és eladását tiltották be, nehogy a mobil telefonálást zavarják (ITU News, 1998/5 szám, 23. old.)

[8] A fogyasztók egyre kevésbé vannak abban a helyzetben, hogy a megvásárolni szándékolt áru megfelelőségét és/vagy minőségét ellenőrizzék. Előnyös tehát számukra, hogy ezekről a gyártóktól és kereskedőktől független forrásból, célszerűen a kötelező szabványokból értesüljenek különösen akkor, ha ezek betartását hatóságilag ellenőrzik is.

[9] De ha a műszaki fejlődés egyes esetekben, mint pl. vivőhullámú berendezések kapcsán az 50-60-as években a vonatkozó Ajánlásban foglaltakat mégis meghaladta, akkor a műszaki követelményekben a CCITT Ajánlásokban megadott értékek 2/5-ét írták elő.

[10] A fejlődő országok érthetően keveset tudtak és tudnak a nemzetközi szabványok kidolgozásához hozzájárulni. Ez ma is nehézségeket okoz az ITU munkájában, ezért az ITU támogatja a regionális szabványosítási szervezetek kialakulását, melyek a „világszabványok" előkészítésekor régiójuk érdekeit sokkal jobban közvetíthetik.

[11] Lindström, Tom: Standardisation in the world of information and communications technology. Ericsson Review, 1997. 2. szám.

[12] Martin Bangemann: a Global 360-at megnyitó beszéde, Bécs, 1998. nov. 30.

[13] Például a Q-SIG jelzésrendszer szabványait az ETSI megbízásából az ECMA dolgozta ki.

[14] A minimális szabályozás elve szerint az ITU szabványosítási tevékenysége csak azokat az elemeket és tevékenységeket fedi le, amelyek a távközlési hálózatok globális összekapcsolhatóságát és együttműködését biztosítják.

[15] dr. Gosztonyi Géza: Változások érlelődnek az ITU-T-ben. Magyar Távközlés, 1996/4 szám

[16] Rabbitt-Bergh: The ISO 9000 book; White Plains, New York, 1993.

[17] Lásd például Földesi Tamás: Minőségügyi rendszerek c. írását, amely a MSZT egyik oktatási anyaga.

[18] Kádár Aba: A szabványok alkalmazásának új rendje, Elektrotechnika, 88. kötet, 2. szám (1995)

[19] HIF ajánlás: A PSTN használhatósága és megbízhatósága, Híradástechnika, 49. Kötet, 5-6 szám, 1998 május-június.

[20] MSZ 250:1996, Magyar nemzeti szabványok alaki és szerkesztési előírásai

[21] Szabó Zoltán: A magyar elektrotechnikai szabványosítás múltja és jelene. ELEKTROTECHNIKA, 89. Kötet (1996), 4. szám

[22] Krüger, M.: Prüfen von Software — aber richtig. Elektronik, 1993/24. szám

[23] Bernstein, L.: Innovative Technologies for Preventing Network Outages. AT&T Technical Journal, 72. kötet (1993), 4. szám

[24] Andrew Emerson: Who needs standards anyway? Philips Business Communications, 7. kötet, 1. szám (1995 március)

[25] dr. Gosztony Géza: Szellemi tulajdonjog-politika, Magyar Távközlés, 1995/6 szám.

[26] Boncsarovszky István: Amíg a minőségügy eljutott odáig..., Magyar Távközlés, 1996/1 szám

[27] Meg kell azonban jegyezni, hogy nem minden tanúsító szervezet által kiadott tanúsítvány egyformán értékes. Az ISO 9000 szerinti tanúsítvány felmutatásakor tehát érdemes ellenőrizni, hogy jóhírű intézménytől származik-e. Emiatt gondos cégek több helyről is szereznek ISO 9000 tanúsítványt. Hazánkban tanúsítványok kiadására az MSZT törvényi felhatalmazás alapján jogosult.

[28] Ezek jórészt tartalmazzák a CCITT, illetve az ITU-T által kiadott Q.9 (Vocabulary of switching and signalling terms), és az I.112 (ISDN; General structure. Vocabulary of terms for ISDNs) háromnyelvű (angol, francia, spanyol) terminológiai szabványokban tárgyalt fogalmak magyar megfelelőit is.

[29] A feloldások magyar fordítását is tartalmazza.

[30] dr. Izsák Miklós főszerk.: Távközléstechnikai Kézikönyv, Műszaki Kiadó, Budapest, 1979, 242. old.

[31] Magyar Mérnöki Kamara, Mérnök Újság, 1998. november. A röplap formájában kiadott angol nyelvű eredeti szöveg fordítása.

TELECOMMUNICATIONS STANDARDISATION IN HUNGARY

GY. HORVÁTH

H-1101 BUDAPEST, PONGRÁC ÚT 17. F/8 ÉPÜLET
TEL/FAX: 262-8832

Since the quiet era of CCITT Recommendations the methods of elaborating standards, the standardising bodies are growing rapidly. The standard committees became the arena of fight between manufacturing corporations.

Legal aspects changed: majority instead of unanimously, voluntary instead of obligatory, patented solutions lead to problems, the relation between standards and quality changes.

The standardisation in Hungary has been reformed with regard to the adherence to the European Union.

Horváth Gyula a Budapesti Műszaki Egyetemen 1943-ban gépészmérnöki (villamos tagozat) oklevelet kapott. 1945-1990 között a Standard Villamossági Rt-nél, illetve a BHG-ban a vállalat életében a telefonközpontokkal, és az egész távközléssel, azok gazdasági és humán vonatkozásaival kapcsolatos új problémák önálló megoldásával foglalkozott, 80 dolgozatot publikált. Tagja a Híradástechnikai Tudományos Egyesületnek, alapító tagja a Nemzetközi Méréstechnikai Szövetségnek, melynek legnagyobb kitüntetését 1989-ben Houstonban (USA) kapta meg. Puskás Tivadar díjat két ízben kapott, másodszor életműért. Jelenleg független távközlési tanácsadóként dolgozik.

A RED ALGORITMUS VIZSGÁLATA

BAJKÓ GÁBOR, BÓDOG GYULA, KASZA TAMÁS

BUDAPESTI MŰSZAKI EGYETEM
VILLAMOSMÉRNÖKI ÉS INFORMATIKAI KAR, TÁVKÖZLÉS ÉS TELEMATIKA TANSZÉK
NAGYSEBESSÉGŰ HÁLÓZATOK LABORATÓRIUM (HSNLAB)
1111 BUDAPEST, PÁZMÁNY PÉTER SÉTÁNY 1/D

A cikkben egy aktív puffer menedzsment implementációt, a RED (Random Early Detection) algoritmust és tulajdonságait mutatjuk be. Szimulációs eredményeinkkel megpróbálunk rávilágítani az előnyökre és a hátrányokra, majd ezeket összehasonlítjuk a FIFO pufferével. Bemutatjuk a RED lehetséges továbbfejlesztéseit, az adaptív RED és az FRED algoritmust.

1. BEVEZETÉS

Az Internet felhasználók száma jelentősen megnövekedett, ez egyben nagy forgalmi terhelést jelent a hálózatnak. A szolgáltatók célja, hogy a kihasználtság, és a felhasználóknak nyújtott szolgáltatás minősége minél jobb legyen. A megnövekedett forgalom a hálózat egyes részein (az útvonalválasztók puffereiben) torlódást okozhat.

Az IP alapú hálózatokban (Internet) a torlódásvezérlést a TCP (Transmission Control Protocol) szállítási protokoll segítségével oldják meg. A TCP küldő kliens (a TCP protokoll adó oldali entitása) egy ún. torlódási ablakot használ, mely a hálózatban lévő nyugtázatlan csomagok számát határozza meg. A küldő az érkező nyugták ütemében növeli az ablak méretét, a növekedés egy TCP kapcsolat elején exponenciális. Ezt a szakaszt hívjuk *slow start*-nak [3], mely során a TCP küldő körbefordulási időnként megduplázza a torlódási ablak méretét. Bizonyos idő után a nagy számú elküldött csomag torlódást okozhat, amit a *congestion avoidance* algoritmussal lehet elkerülni. Egy küszöbértékkel tudjuk megbecsülni azt, hogy mikor kell a *slow start*-ról áttérni a *congestion avoidance* algoritmusra. Amikor a TCP a csomagokat a congestion avoidance alapján küldi, akkor a torlódási ablak értékét körbefordulási időnként csak eggyel növeli, mely sokkal lassabb az előző *slow start* fázishoz képest (exponenciális helyett lineáris jelleg). Ha az aktív kapcsolatok átviteli kapacitása meghaladja a hálózat kapacitását, csomagvesztés történik. A TCP küldő a csomagvesztést ismétlő nyugták vételével, vagy az időzítés lejártával érzékeli; majd a torlódási ablak méretét megfelezi, és újraküldi az elveszett csomago(ka)t. Az utóbbi eljárásokat *fast retransmit* és *fast recovery* algoritmusoknak hívjuk [3]. Számos TCP implementáció (Tahoe, Reno, Vegas stb.) terjedt el, melyek közt a különbség a torlódás kezelésében van [7].

A TCP torlódásvezérlésével azonban van egy probléma. A küldő adási sebességét csak egy, a hálózatban történt csomagvesztés után csökkenti. Ez azért jelent gondot, mert jelentős idő is eltelhet a csomag vesztése és érzékelése között. Ez idő alatt az adó továbbra is nagy sebességgel küldi a csomagokat, amely további csomagvesztéseket okozhat. A nagy számú csomagvesztés a hálózat kihasználtságának csökkenéséhez vezet. A problémára megoldást jelent az aktív puffer menedzsment alkalmazása, mely meg próbálja elkerülni a puffer túlcsordulás miatti csomagvesztést. Az aktív puffer menedzsment alapelve, hogy a torlódást a puffer betelte előtt érzékelni kell. Például a kezdeti torlódás érzékelésekor eldobhatunk egy csomagot, amivel a forrás felé azt kívánjuk jelezni, hogy az vegye vissza adási sebességét a torlódást elkerülendő. A cikkben egy ilyen aktív puffer menedzsment tulajdonságait, előnyeit és hátrányait kívánjuk bemutatni.

2. A RED ALGORITMUS

A RED (*Random Early Detection*) algoritmus működésének lényege az átlagos puffer méret speciális kiszámításán alapszik [1]. A későbbiekben részletezett eljárás során egy ún. exponenciális súlyozású mozgó átlag (*EWMA*: Exponential Weight Moving Average – exponenciális súlyozású mozgó átlag) számítást adunk meg. Az így kiszámított átlagos puffer méretet két előre megadott küszöbértékkel hasonlítjuk össze, a minimális és a maximális küszöbbel (*minimum threshold* és *maximum threshold*). Ha az átlagos puffer méret kisebb a minimális küszöb értékénél, akkor p_a az útvonalválasztó egyetlen csomagot sem dob el, ha az átlag a két küszöbérték között van, akkor valószínűséggel fogja eldobni a beérkező csomagot, míg ha ez az átlagérték a maximális küszöb fölött van, akkor minden beérkező csomagot eldob. A p_a csomagdobási valószínűség az átlagos puffer méret függvénye.

A RED algoritmus valójában tehát két különálló eljárásból tevődik össze:
a) az átlagos puffer méret számítása;
b) a csomagdobási valószínűség számítása.

a) Attól függően, hogy a puffer üres volt vagy sem, az átlagos puffer méret (*avg*) a következő módon számolandó (minden egyes csomagbeérkezés után):

- Ha a puffer nem volt üres:

$$avg \leftarrow (1 - \omega_q) \cdot avg + \omega_q \cdot q \qquad (1)$$

- Különben:

$$m \leftarrow f(time - q\_time) \qquad (2)$$

$$avg \leftarrow (1 - \omega_q)^m \cdot avg \qquad (3)$$

ahol q_time: az az időpont, amikor a puffer mérete nullává vált ($q\_time \leftarrow time$, ha a puffer üres); ω_q: az exponenciális súlyozású mozgó átlag paramétere; q: az aktuális puffer méret; $time$: az aktuális idő; $f(t)$: az idő lineáris függvénye.

Ha a puffer üres, akkor az átlagos puffer méret számításakor azt becsüljük meg, hogy hány darab kis méretű csomag tudott volna távozni, amíg a puffer üres volt.

b) A következőkben a RED algoritmust részletesen is ismertetjük:

Az inicializáció során nullára állítjuk az átlagos puffer méretet (*avg*), és -1-re az utolsó eldobott csomag után érkezett csomagok számát (*count*).

$$avg \leftarrow 0 \tag{4}$$

$$count \leftarrow -1 \tag{5}$$

Vezessük most be a minimális, illetve maximális küszöb értékek jelölésére a $\min_{\text{th}}$, illetve a $\max_{\text{th}}$ változókat. Ha az átlagos puffer méret (*avg*) értéke a két küszöb között van, vagyis $\min_{\text{th}} \leq avg \leq \max_{\text{th}}$, akkor az útvonalirányító p_a valószínűséggel eldobja a beérkező csomagokat. Az ilyen típusú csomagdobást nevezzük „early drop"-nak.

$$p_b \leftarrow \max_p \cdot \frac{(avg - \min_{\text{th}})}{(\max_{\text{th}} - \min_{\text{the}})} \tag{6}$$

$$p_a \leftarrow \frac{p_b}{1 - count \cdot p_b} \tag{7}$$

ahol p_b: a csomagdobási valószínűség kiszámításához szükséges segédparaméter, melynek értéke lineárisan változik 0 és a maximális csomagdobási valószínűség ($\max_p$) között; p_a: a tényleges csomagdobási valószínűség, látható hogy értékét a *count* számláló jelentősen befolyásolja.

Ha a beérkező csomagot nem dobjuk el, akkor a *count* értékét eggyel megnöveljük, csomagdobás esetén a változót lenullázzuk ($count \leftarrow 0-$).

Az átlagos puffer méret (*avg*), a minimális és maximális küszöb ($\min_{\text{th}}$, $\max_{\text{th}}$), az aktuális puffer méret (q) és a *count* változó értékét csomagok helyett bájtokban is számolhatjuk. Ebben az esetben a csomagdobási valószínűség arányos a csomag méretével; így az útvonalválasztó nagyobb valószínűséggel fogja a nagy méretű FTP (File Transfer Protocol) csomagokat dobni, mint a kis méretű TELNET csomagokat.

Ha az átlagos puffer méret nagyobb, mint a maximum korlát, vagyis $\max_{\text{th}} < avg$, akkor az összes beérkező csomagot eldobjuk, és a *count* értékét nullára állítjuk ($count \leftarrow 0$).

Ha viszont az átlagos puffer méret kisebb, mint a minimum korlát, vagyis $\min_{\text{th}} < avg$, akkor egyetlen csomagot sem dobunk el, és a *count* számláló értékét -1-gyel tesszük egyenlővé ($count \leftarrow 0$).

Végül összefoglaltuk a legfontosabb előforduló változókat és jelentésüket:

avg: átlagos puffer méret (csomagban vagy bájtban)
q_time: az az időpont, amikor a puffer mérete nullává vált
count: az utolsó eldobott csomag után érkezett csomagok/bájtok száma
ω_q: az exponenciális súlyozású mozgó átlag paramétere
$\min_{\text{th}}$: minimális küszöb értéke (csomagban vagy bájtban)
$\max_{\text{th}}$: maximális küszöb értéke (csomagban vagy bájtban)
p_a: az aktuális csomagdobási valószínűség
q: az aktuális puffer méret (csomagban vagy bájtban)
time: az aktuális idő
$f(t)$: az idő lineáris függvénye

A RED tehát egy dinamikusan számított valószínűség szerint dobja el a beérkező csomagokat, amikor a pufferben lévő csomagok száma túllépi a minimum korlátot [5]. Ez a valószínűség az átlagos puffer mérettel és az utolsó csomagdobás utáni elfogadott csomagok számával növekszik. A RED előnye, hogy könnyű és egyszerű implementálni a már meglévő útvonalválasztókban, mert csak a beérkező csomagokat dobja el, és felhasználja a FIFO sorozást. (Például a Cisco útvonalirányítókban.)

A RED célja, hogy a csomagokat mindegyik folyamból a folyam által a kimeneti linken használt sávszélesség arányában dobja el. Minden beérkező csomagot egyenlő valószínűséggel dob el, a legnagyobb bemeneti sebességű összeköttetés rendelkezik a legnagyobb csomagdobási valószínűséggel. Tételezzük fel, hogy az átlagos puffer méret nem változik egy rövid (időtartam alatt, tehát a RED egy fix p valószínűséggel dobja el a csomagokat; és tételezzük fel, hogy az i-edik összeköttetés aktuális bemeneti sebessége λ_i (vagy $(\lambda_i * \delta)$ csomag (δ idő alatt). Az i-edik összeköttetésből eldobott csomagok csomagdobási valószínűsége:

$$\frac{\lambda_i \cdot p}{\sum \lambda_i \cdot p} = \frac{\lambda}{\sum \lambda_1} \tag{8}$$

Az FCFS (*First Come First Served*) kiszolgálás szerint az elfogadott csomagok aránya:

$$\frac{\lambda_i \cdot (1-p)}{\sum \lambda_i \cdot (1-p)} = \frac{\lambda}{\sum \lambda_1} \tag{9}$$

A fenti két egyenlőségből adódik, hogy a RED a csomagokat az összeköttetések kimeneti sávszélesség kihasználásának FCFS ütemezés szerinti arányában dobja el.

Az összes összeköttetés szempontjából a csomagdobási valószínűség egy rövid δ időtartam alatt $\frac{\lambda \cdot p}{\lambda} = p$, ami független a sávszélesség használattól. Ha a torlódás állandó, ami azt jelenti, hogy a RED által használt átlagos puffer méret egy minimum értékkel rendelkezik a minimum korlát felett, a dobási valószínűségnek egy nem nulla minimuma van, és ez okozza azt, hogy az összeköttetések minimum dobási sebességgel rendelkeznek, függetlenül a sávszélesség használatuktól. A rendelkezésre álló sávszélesség ún. *fair* megosztásáról akkor beszélhetünk, ha mindegyik folyam pontosan ugyanolyan kiszolgálást kap, ugyanakkora sávszélességet használhat. Az arányos dobás azonban nem *fair* link osztást jelent a következő esetekben:

1. Az a tény, hogy az összes összeköttetés ugyanazt a vesztési arányt látja, azt jelenti, hogy bár az összeköttetés a *fair* osztásnál jóval kisebb sávszélességet használ, mégis lehet csomagdobás. Az alacsony sávszélességű TCP összeköttetés ekkor soha nem éri el a *fair* osztás szerint igénybe vehető sávszélességet, mivel torlódás esetén a TCP összeköttetés lecsökkenti az ablak méretét.

2. Ha egy összeköttetésből „beengedünk" a pufferba egy csomagot, akkor a dobási valószínűség a többi kapcsolat jövőbeli csomagjai számára is megnövekszik, hacsak nem igényel a többi kapcsolat kevesebb sávszélességet. Ez egy ideiglenes és nemkívánatos nem-arányos dobást eredményezhet az azonos tulajdonságú folyamok esetében is.

Egy ún. nem-tanuló (*non-adaptive*) összeköttetés „kényszerítheti" a RED-et, hogy nagy arányban dobjon el csomagokat az összes összeköttetésből. (Ilyen például a CBR (Constant Bit Rate – konstans sebességű (összeköttetés)), konstans bitsebességű kapcsolat.) Ez azt eredményezi, hogy ebben az esetben a RED képtelen *fair* osztást biz-

tosítani a tanuló (*adaptive*) összeköttetéseknek az agresszív felhasználók jelenléte esetén.

3. FAIRNESS

Több adatkapcsolat vizsgálata esetén fontos kérdés az ún. *fairness*. Ezzel a tulajdonsággal lehet jellemezni az összeköttetés teljesítményét. A *fairness* lényegében azt jelenti, hogy a különböző adatfolyamok közt milyen arányban oszlik el a link átviteli kapacitása.

Jelöljük $x_1, x_2, \cdot, x_n$-nel az $1, 2, \ldots n$ kapcsolatok teljesítőképességét. A Jain-féle képlet szerint [4]:

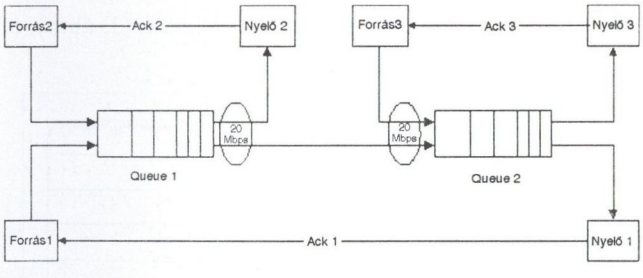
$$f(x_1, x_2, \cdot, x_n) = \frac{\left(\sum_{i=1}^{n} x_i\right)^2}{n \sum_{i=1}^{n} x_i^2} \qquad (10)$$

A (10) formula szerinti *fairness* érték 0 és 1 közé esik. Ha mindegyik teljesítőképesség egyenlő, akkor az érték 1. Azt mondhatjuk, hogy a hálózat fairness tulajdonsága annál kedvezőbb, minél jobban megközelíti az 1-et. (Például egy Internet szolgáltató minden egyes előfizetőjének körülbelül ugyanazt a sávszélességet biztosítja, ha a *fairness* 1-hez közeli.)

4. RED PUFFER ÉS FIFO PUFFER ÖSSZEHASONLÍTÁSA

Vizsgálataink során a kaliforniai Berkeley Egyetemen kidolgozott Network Simulatort használtuk.

4.1. RED puffer vizsgálata



1. ábra. A vizsgált hálózat topológiája

A vizsgált hálózat logikai topológiája az 1. ábrán látható. A forrás 1, 2, 3 modulok mindegyikében 10-10 db FTP forrást; a nyelő 1, 2, 3 modulokban pedig a nyelőket definiáltuk. A nyugtáknak külön linket hoztunk létre, melyre 20 ms-os késleltetést és 20 Mbps sávszélességet állítottunk be. Az adatcsomagok 20 Mbps sávszélességű linken áramlanak. A pufferek mérete 200 csomag. A RED puffer paraméterei:

- az átlagos puffer méret minimum határa 10 csomag;
- az átlagos puffer méret maximum határa 30 csomag;
- a maximális csomagdobási valószínűség értéke 5 %.
- a csúszó átlag paramétere 0.002.

Szállítási protokollként Reno TCP-t használtunk, melynek paraméterei:

- maximális szegmens mérete (MSS): 512;
- maximális átviteli egység (MTU): 552;
- a maximális ablak méret: 32K.

A szimuláció célja az volt, hogy megvizsgáljuk a RED puffer viselkedését összehasonlítva a FIFO pufferrel jelentős forgalmi terhelés mellett. Az összehasonlítás alapja az eldobott csomagok száma, a sikeresen átvitt csomagok száma (teljesítőképesség), és az adatfolyamok közti szinkronizáció (korreláció).

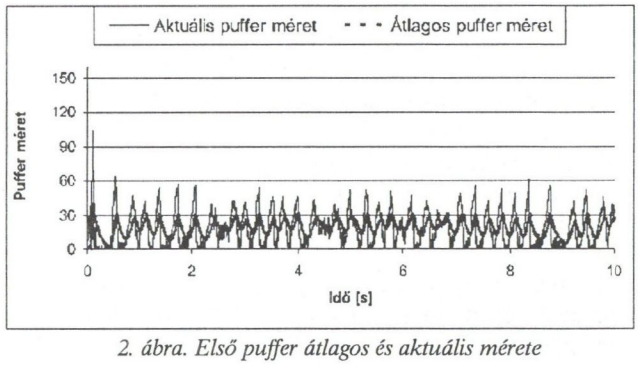
1. táblázat. Folyamstatisztikák

	Elküldött csomagok száma		
Folyamok sorszáma	1. forrás	2. forrás	3. forrás
1	1586	2994	3309
2	1189	3236	4015
3	1236	2926	2579
4	1678	3747	3710
5	1411	3153	2828
6	1343	3142	2937
7	1547	2799	2661
8	1315	3440	3612
9	1747	2398	3211
10	1269	2654	2415

Az 1. táblázatban, folyamokra lebontva láthatjuk az elküldött csomagok számát. A táblázatban lévő adatok alapján számítjuk ki a *fairness* értékeket (10) szerint:

- az első forrás adatfolyamai közt: 0,9836;
- a második forrás adatfolyamai közt: 0,9856;
- a harmadik forrás adatfolyamai közt: 0,9746.

Azt mondhatjuk, hogy RED puffer alkalmazásakor a *fairness* 1-hez közeli, kedvező érték.



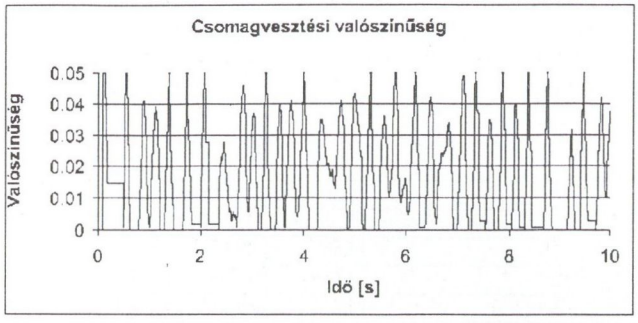
2. ábra. Első puffer átlagos és aktuális mérete

A 2. ábrán az első puffer átlagos és aktuális méretének alakulását láthatjuk. A puffer mérete a szimuláció elején felmegy 150 körüli értékre, mert mindegyik kapcsolat *slow start* szerint kezdi adni az adatait, és emiatt a puffer nagyon hamar megtelik. Az exponenciális csúszó átlag paraméter nagyságától függően követi az átlagos puffer méret az aktuális puffer méretet. A jelenlegi esetben az látható, hogy az átlagos puffer méret viszonylag gyorsan követi a puffer méretének alakulását. Emiatt az átlagos puffer méret gyorsan eléri a 30-as értéket, ami fölött viszont minden beérkező csomagot eldob. Az eldobott csomagok a küldő TCP-t visszafogják az adásban, ezért a puffer mérete lecsökken. A 2. ábráról az is leolvasható, hogy a puffer mérete 30 körül ingadozik.

A 3. ábrán látható a RED algoritmusban szereplő csomagdobási valószínűség alakulása, amely az átlagos puffer méret értéke függvényében változik.

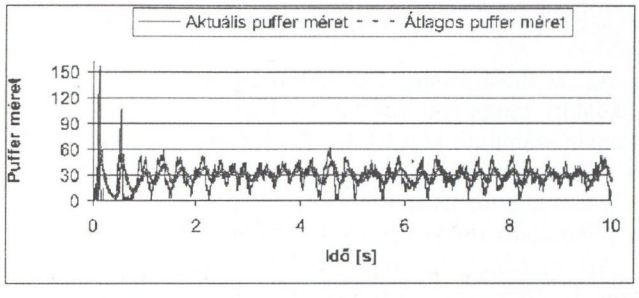
Ahogy az átlagos puffer méret megközelíti, ill. eléri a 30 értéket, úgy növekszik a csomagdobási valószínűség is. Jól látszik, hogy a szimuláció elején, amikor a puffer méret

hirtelen megnőtt, a dobási valószínűség elérte maximális, 5 %-os értékét.



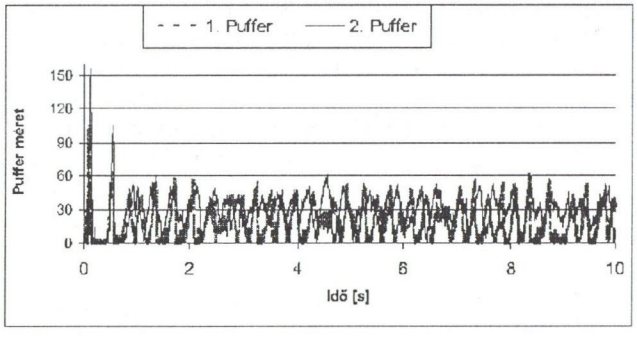
3. ábra. Első pufferben a csomagdobási valószínűség

A második puffer mérete (4. ábra), valamint az elküldött csomagok számának alakulása is hasonló az első puffernél kapott eredményekhez.



4. ábra. Második puffer átlagos és aktuális mérete

Az 5. ábrán együtt ábrázoljuk a két puffer méretét, melyből a szinkronizációra tudunk következtetni.

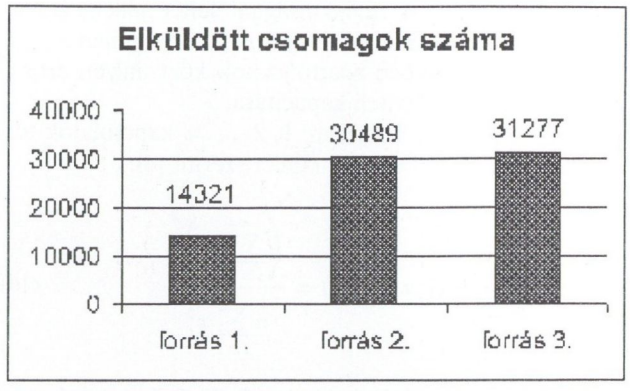


5. ábra. a két puffer aktuális mérete

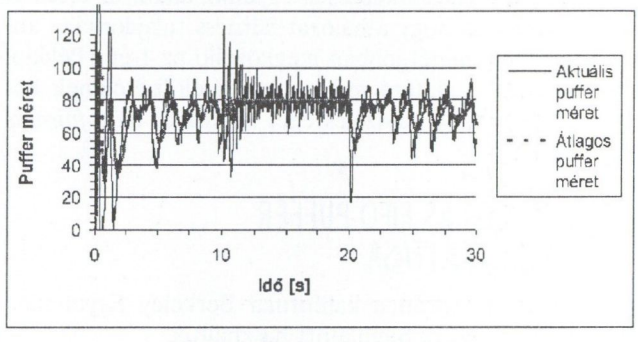
A két puffer között szinkronizáció figyelhető meg. Ennek oka az, hogy ha az első puffer telítődik, akkor a mindkét pufferen áthaladó csomagokból csak csekély számú jut át a „megtelt" első pufferen, melynek következtében kevesebb csomag érkezik a második pufferbe, amelynek a mérete ekkor sokkal kisebb.

A 6. és 7. ábrán grafikonok segítségével mutatjuk be az egyes források által elküldött csomagok mennyiségét és a csomagvesztések számát.

Jól látható, hogy az első forrás fele annyi csomagot tudott elküldeni, mint a másik két forrás egyenként, mert az első forrás csomagjai mind a két RED pufferen áthaladtak. Ezzel szemben a csomagdobások számában a három forrás csomagjait tekintve nincs nagy különbség. Az első forrás csomagjainak 3,8 %-a veszett el, melynek 66 %-a *early drop* volt. A második, illetve a harmadik forrás csomagjainak a vesztési aránya 2,1 %, ill. 2,3 % volt. Arányaiban nézve látható, hogy az első forrás csomagjai kétszer nagyobb mértékben vesztek el. Ez a forrás a másik kettőhöz képest csak feleannyi csomagot tudott átküldeni a hálózaton, mert a sok csomagvesztés visszafogta a küldő TCP-t.



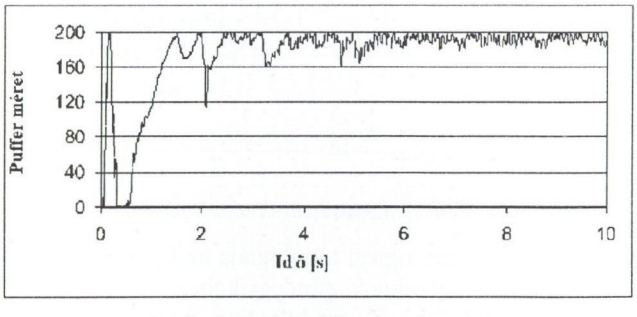
6. ábra. Elküldött csomagok száma



7. ábra. Csomagdobások száma

4.2. FIFO puffer

A vizsgált hálózat topológiája nem változott (1. ábra), a RED puffert FIFO-ra cseréltük.



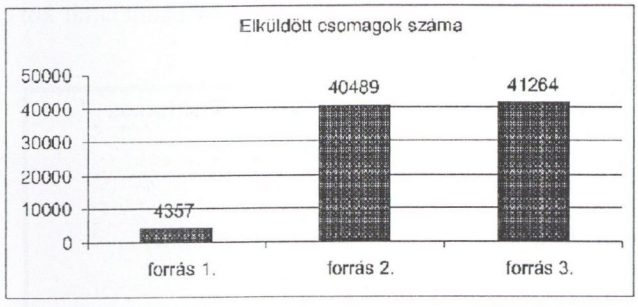
8. ábra. Az első puffer aktuális mérete

A 8. ábrán az első FIFO puffer méretét láthatjuk. A 4.2. fejezetben tárgyalt esethez képest jelentős különbséget tapasztalunk. A puffer mérete 160 és 200 között ingadozik, és ez sokkal nagyobb, mint amit a 2. ábrán láthatunk. A csomagvesztések puffer túlcsordulás miatt következnek be, míg RED használata esetén a dobások nagy részét az algoritmusnak köszönhetjük.

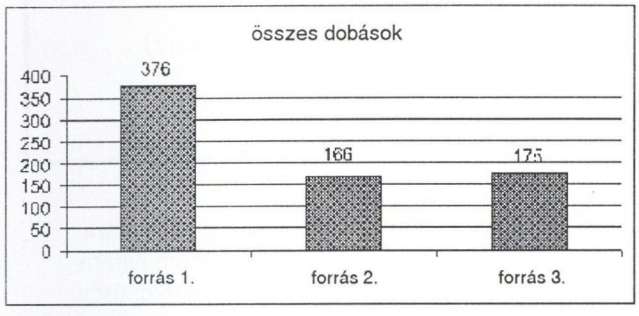
A 9. és a 10. ábrán hasonlíthatjuk össze az egyes források által elküldött csomagok és csomagvesztések számát.

Az első forrás körülbelül tizedannyi csomagot tudott elküldeni, mint a másik kettő. Az első forrás által elküldött csomagok 8.6 %-a veszett el, míg a másik két forrásnál ez az arány mindössze 0,4 %. A három forrás által

elküldött csomagok száma több, mint 10 %-kal kevesebb volt RED puffer alkalmazásakor, mint FIFO puffer esetén. Külön nézve a forrásokat, azt láthatjuk, hogy RED puffer használatakor a második és a harmadik forrás körülbelül negyedannyival kevesebb csomagot tudott elküldeni, mint FIFO puffer esetén; az első forrás viszont háromszor többet küldött a RED esetén.



9. ábra. Az elküldött csomagok száma



10. ábra. A csomagvesztések száma

2. táblázat. Folyamstatisztikák

	Elküldött csomagok száma		
Folyamok sorszáma	1. forrás	2. forrás	3. forrás
1	415	4670	1985
2	362	4590	2204
3	408	3454	3829
4	364	2648	5649
5	342	3195	4537
6	393	4857	5110
7	375	4876	4196
8	274	4741	4608
9	309	4166	4538
10	1115	3292	4608

A 2. táblázatban az elküldött csomagok száma látható adatfolyamonként. A (10) szerinti *fairness*:

- az első forrás folyamai közt: 0,78184;
- a második forrás folyamai közt: 0,9639;
- a harmadik forrás folyamai közt: 0,9318.

A szimulációk során arra jutottunk, hogy RED puffer alkalmazása esetén kedvezőbb *fairness* értéket kapunk, mint FIFO puffer használata esetén, viszont az elküldött csomagok száma (a teljesítőképesség) több, mint 10 %-kal csökkent A RED puffer alkalmazásakor.

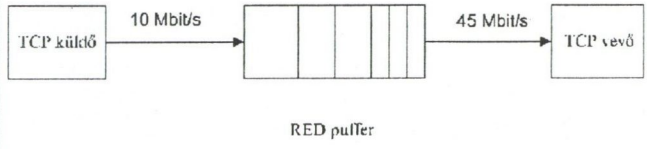
5. ADAPTÍV RED

A 4. fejezetben vizsgált RED puffer egyik hátránya, hogy a torlódásvezérlés nem függ a kapcsolatok számától. Nagy számú összeköttetés esetén a torlódás elkerüléséhez megfelelő számú kapcsolat sebességét kell visszafogni, ugyanakkor nem szabad túl sok kapcsolat sebességét sem csökkenteni, mert az kedvezőtlen link kihasználtsághoz vezet.

A problémát a következő példával tudjuk szemléltetni: egy 10 Mbit/s sávszélességű linket 100 kapcsolat között egyenlő mértékben osztunk meg. Ha torlódás miatt egy kapcsolat sebességét visszafogjuk, akkor a link terhelése 9,95 Mbit/s-ra csökken. Ha viszont a linken csak két kapcsolat van, akkor az egyik sebességét visszafogva, a link terhelése 7,5 Mbit/s-ra csökken. Általánosságban is elmondhatjuk, hogyha egy linken N összeköttetés van, akkor egy forrást torlódás miatt visszafogva, a link terhelése $(1 - \frac{1}{2N})$ faktorral csökken. Ha N értéke nagy, akkor a RED algoritmus korai torlódás felismerő hatása elvész, és egyszerű FIFO pufferként működik. Kis N értékek esetén a link kihasználtsága lesz alacsony.

Ezt a problémát egy egyszerű hálózaton elvégzett szimuláció segítségével mutatjuk meg.

A vizsgált hálózat topológiája a 11. ábrán látható.

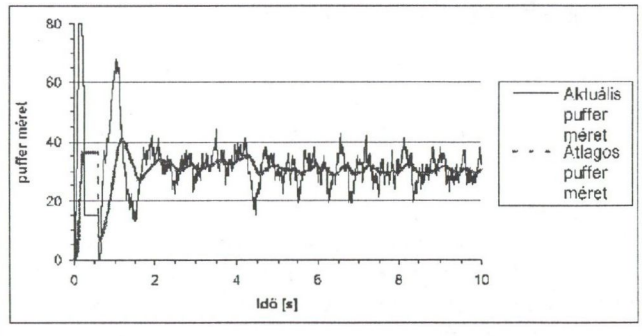


11. ábra. A vizsgált hálózat topológiája

A TCP küldő és vevő között először 10, majd 40 TCP kapcsolatot hoztunk létre FTP forgalommal. A RED puffer paraméterei:

- az átlagos puffer méret minimum határa: 20 csomag;
- az átlagos puffer méret maximum határa: 80 csomag;
- maximális csomagvesztési valószínűség: 0,25, ill. 0,016;
- az exponenciális csúszó átlag paramétere: 0,002;
- a puffer mérete: 80 csomag.

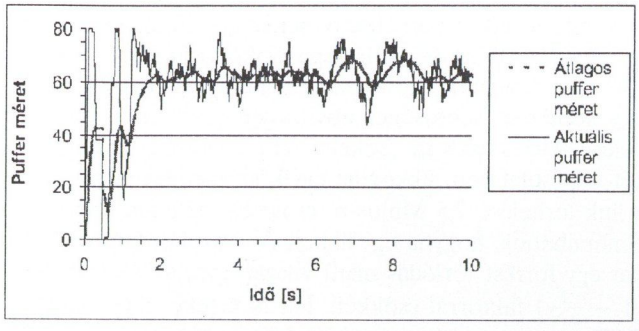
Ilyen paraméterek mellett azt tudjuk vizsgálni, hogy a RED algoritmus milyen hatékonyan tudja érzékelni a torlódást. Ha puffer túlcsordulás miatt történik csomagvesztés, akkor a RED algoritmus működése nem a megfelelő.



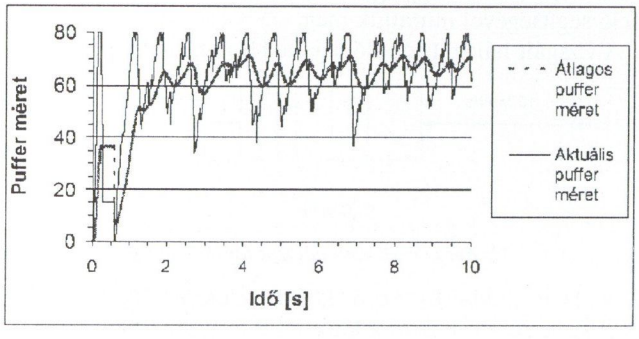
12. ábra. 10 TCP kapcsolat, 25 %-os maximális csomagvesztési valószínűség

Ha a maximális csomagvesztés értékét túl nagyra választjuk, akkor a RED algoritmus miatti csomagvesztések lesznek túlsúlyban, a túlcsordulással szemben. 10 TCP kapcsolat esetén (12. ábra) a puffer mérete az idő nagy részében túl alacsony, és a link kihasználtsága kedvezőtlen. A RED algoritmus torlódás érzékelése túl „agresszív", azaz túl hamar dobál el csomagokat. 40 TCP kapcsolat esetén

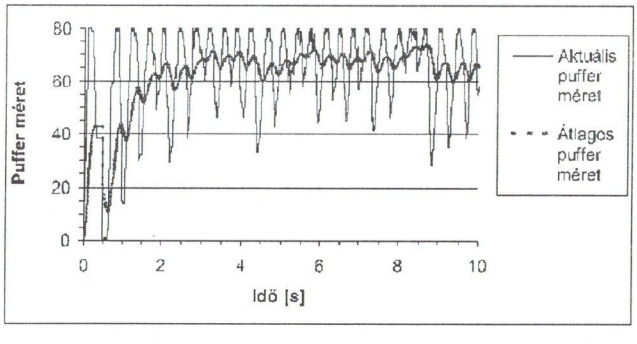
(13. ábra) megfelelőbb működést kapunk. A puffer mérete viszonylag magas, de a túlcsordulás miatti csomagvesztések száma minimális.



13. ábra. 40 TCP kapcsolat, 25 %-os maximális csomagvesztési valószínűség



14. ábra. 10 TCP kapcsolat 1,6 %-os maximális csomagvesztési valószínűség



15. ábra. 40 TCP kapcsolat, 1,6 %-os maximális csomagvesztési valószínűség

A maximális csomagvesztési paramétert kicsire választva a RED hatása csökken (14. és 15. ábra), és a puffer inkább a FIFO működéshez közelít. Ekkor beszélünk konzervatív működésről. Az eredményekből arra következtethetünk, hogy a konzervatív működés kis számú kapcsolatok, míg az agresszív működés nagy számú kapcsolatok esetén ad kedvező eredményt. Ezért vált szükségessé a RED algoritmus módosítása, melyben a paraméterek megadásakor figyelembe vesszük az aktuális forgalmi terhelést [6]. Az algoritmus mögött az az alapgondolat áll, hogy a puffer átlagos mérete változásának figyelésével állítjuk be a RED paramétereit. Ha az átlagos puffer méret a minimum határ környékén ingadozik, akkor ez azt jelenti, hogy a RED túl agresszív, ha viszont az átlagos puffer méret a maximum határ körül ingadozik, akkor a RED túl konzervatív. Ez az új algoritmus a RED paraméterei közül a maximális csomagvesztési valószínűséget változtatja, mivel lényegében ez a paraméter határozza meg, hogy a RED agresszív vagy konzervatív legyen.

A 16. ábrán látható az adaptív RED algoritmus leírása. A maximális csomagvesztési valószínűséget két faktor segítségével (α és β) változtatjuk aszerint, hogy az átlagos puffer méret a minimum határ vagy a maximum határ környékén ingadozik.

Az átlagos pufferméret Q(ave) minden frissítésekor:

if $(\min_{th} < Q(ave) < \max_{th})$

status=Between;

if $(Q(ave) < \min_{th}$ && $status != Below)$

status=Below;

$$\max_p = \frac{\max_p}{\alpha};$$

if $(Q(ave) > \max_{th}$ && $status != Above)$

status=Above;

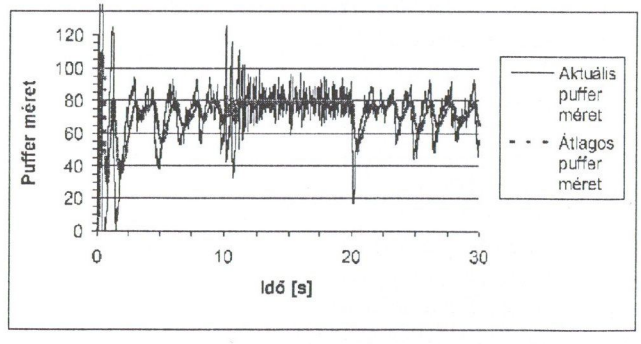
$$\max_p = \max_p * \beta;$$

- $Q(ave)$: Az átlagos pufferméret
- $\min_{th}$: Az átlagos pufferméret minimum határa
- $\max_{th}$: Az átlagos pufferméret maximum határa
- $\max_p$: A maximális csomagvesztési valószínűség

16. ábra. Az adaptív RED algoritmus

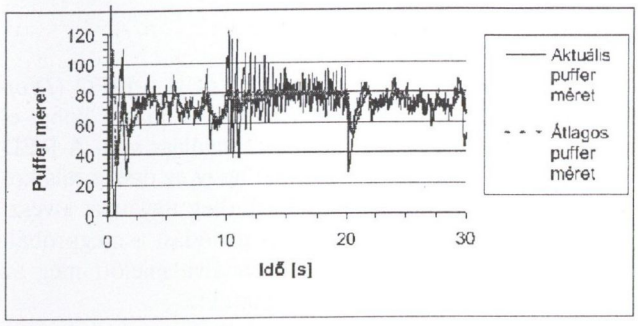
A 11. ábrán látható hálózaton elvégeztünk olyan szimulációt is, amelyben változtattuk az aktív TCP kapcsolatok számát:

- 0 és 10 másodperc között 10 TCP kapcsolat,
- 10 és 20 másodperc között 40 TCP kapcsolat,
- 20 és 30 másodperc között 10 TCP kapcsolat van.



17. ábra. Statikus RED paramétereket használva

Statikus paramétereket használva (17. ábra) a RED algoritmus működése az éppen aktuális kapcsolatok számától függően vagy túl agresszív, vagy megfelelő, vagy konzervatív. Ha a RED agresszivitását meghatározó maximális csomagvesztési paramétert dinamikusan változtatjuk (18. ábra), akkor kiküszöbölhető a RED előbbiekben ismertetett hibája, azaz ne legyen túl sok túlcsordulás, vagy a link kihasználtsága ne legyen kedvezőtlen.



18. ábra. Adaptív RED algoritmust használva

6. FORGALMI KATEGÓRIÁK

Az Internet forgalom számos, különböző tulajdonságú forgalom keverékéből adódik. Néhány forrás torlódásvezérlési mechanizmusokat használ, mint például a FTP (mely TCP-t használ); mások, mint például az állandó sebességű (CBR) videó, nem reagálnak a torlódásra. A TCP más és más verziói és implementációi másképp reagálnak a torlódásra. Már akkor is, amikor az implementációk azonosak, két TCP összeköttetés is másképp viselkedhet, ha különböző ablakméretekkel és körbefordulási időkkel rendelkeznek. A forgalmakat a következő három csoportba kategorizálhatjuk, aszerint, hogy a forgalom hogyan kezeli a torlódást:

1. Nem-tanuló (*non-adaptive*) forgalmak: az ilyen típusú összeköttetések annyi sávszélességet használnak, amennyit igényelnek, és nem lassítanak le torlódás esetén sem. Néhány audió és videó alkalmazás esik ebbe a kategóriába.
2. Robusztus (*robust*) forgalmak: ezeknek az összeköttetéseknek mindig van továbbküldeni való adatuk, és annyi sávszélességet használnak, amennyit a hálózat megenged; lelassítanak, ha torlódást detektálnak. A robusztus folyamok képesek az elveszett csomagok gyors újraküldésére. Gyorsan feltornásszák a sávszélesség használatot, ha szabad hálózati kapacitást érzékelnek. A robusztus folyamok általában elegendő bufferelt csomaggal rendelkeznek az útvonalirányítónál ahhoz, hogy elérhessék legalább a *fair* sávszélesség megosztást. A robusztus összeköttetések gyakran nagyobb ablakkal, vagy rövidebb körbefordulási időtartammal rendelkeznek, mint a *fragile* összeköttetések.
3. Gyenge alkalmazkodású (*fragile*) forgalmak: ezek az összeköttetések szintén torlódásérzékenyek, de a csomagvesztésekre is érzékenyek és lassabban alkalmazkodnak a nagyobb elérhető sávszélességhez. Kevesebb bufferelt csomaggal rendelkeznek az útvonalválasztóknál, mint a robusztus folyamok; ugyanakkor nem körvonalazható minden esetben egyértelműen a különbség a robusztus és a *fragile* forgalmak között. Például, a legtöbb interaktív terminál-alkalmazás, mint például a *telnet* csak szakaszosan rendelkezik továbbküldendő adattal.

Amikor a különböző számú bufferelt csomaggal rendelkező TCP összeköttetések „versenyeznek" az útvonalválasztónál a sávszélességért, az arányos mértékű csomagdobás nem mindig garantálja a *fair* sávszélesség osztást. Ennek oka az, hogy a TCP a csomagdobást, mint torlódást érzékeli, függetlenül az elveszett csomagok számától. A *fair* sávszélesség osztásnál kevesebb sávszélességet használó TCP összeköttetés le fogja csökkenteni a torlódási ablakát egyszeres csomagvesztés esetén. A pufferben lévő csomagszám eltéréseket a torlódási ablakok és a várakozási késleltetések különbözőségei okozzák, általánosságban tehát az útvonalválasztónál a nagy ablakkal és kis körbefordulási idővel rendelkező összeköttetések kapják meg a legnagyobb puffer kapacitást.

7. A FLOW RED ALGORITMUSRÓL

Egy adott pillanatban egy Internet útvonalválasztón folyamok, forgalmak ezrei áramolhatnak át [5]. A forgalmak intenzitása azonban jelentős mértékben ingadozhat és a forgalomforrások a legtöbb esetben mohó módon működnek, vagyis minél nagyobb sávszélességet akarnak lekötni maguknak. Tehát az útvonalválasztónál a sorbaállítási rendszernek képesnek kell lennie sorba állítani a csomagokat, de biztosítani kell a negatív visszacsatolást is a küldési intenzitás visszafogásának céljából. Az ilyen, ún. puffer stratégiának vagy aktív puffer menedzsmentnek meg kell akadályoznia a nagy késleltetést a puffer méret limitálásával. El kell kerülnie azt, hogy a pufferek túl rövidek legyenek, ami alacsony kihasználtságot okozhat; és a negatív visszacsatolást *fair* módon kell biztosítania.

A nagy méretű ablakkal rendelkező TCP összeköttetések sokkal érzékenyebbek a csomagdobásra, mint a kis ablakméretűek. Ugyanis egy nagy ablakos összeköttetésnek csak egy körbefordulási idő szükséges, hogy helyrehozza a többszörös csomagvesztést, míg egy kicsi ablakú folyamnál egy 1 vagy több másodperces *timeout*-ra (timeout – TCP újraküldési időzítésének lejárta) lehet szükség egy egyszeres csomagvesztés visszaállításához. Ha a folyamokból eldobott csomagok száma egyenes arányban áll a felhasznált sávszélességükkel, akkor biztos hogy nem beszélhetünk *fair* sávszélesség megosztásról, mivel a csomagok mérete eltérő lehet.

A *Flow Random Early Drop* (FRED) a RED egy módosított változata, amely feljavítja a *fairness* értékét, amikor más és más forgalmi típusok (pl. FTP, TELNET) osztoznak az útvonalválasztó sávszélességén. Az FRED sokkal hatékonyabb a „rossz magaviseletű", vagyis a torlódáshoz nem alkalmazkodó folyamok izolálásában, jobb védettséget biztosít a börsztös (csomós) és az alacsony sebességű folyamoknak is. Az FRED az állapot követésével biztosítja ezeket az előnyöket azoknak a folyamoknak, amelyek bufferelt csomagokkal rendelkeznek a útvonalválasztónál. Ahogyan a RED, úgy az FRED is könnyen implementálható a már meglévő FIFO-alapú útvonalválasztókban.

Ahelyett, hogy a véletlenszerűen kiválasztott összeköttetések csomagjai közül arányosan dobnánk el, az FRED negatív visszacsatolást generál azon összeköttetéseknek, amelyek nagyszámú bufferelt csomaggal rendelkeznek. Az FRED minden egyes folyamot nyilvántart, folyamonkénti statisztikákat (*per-flow statistics*) vizsgál.

Az FRED hasonlóan működik, mint a RED, de a következő kiegészítésekkel:

- Az FRED bevezeti a csomagok minimális és maximális számát minden folyam esetében.
- Az FRED bevezet továbbá egy globális változót, egy becslést az átlagos folyamonként felhasznált buffer ka-

pacitásra; kedvezőbb helyzetbe kerülnek azok a folyamok, amelyek ezen értéknél kevesebb csomaggal rendelkeznek a pufferben, azokkal szemben, amelyek több csomaggal rendelkeznek.

- Az FRED minden folyamra definiál egy új számlálót az aktuálisan bufferelt csomagok számlálására.
- Végül, az FRED minden folyamnál fenntart egy változó ütközési értéket, amely azt számolja, hogy a folyam hányszor válaszolt sikertelenül a torlódás jelzésére; az FRED azokat a folyamokat bünteti, amelyek nagy ütközési értékkel rendelkeznek.

(A részletes algoritmust és kódot [5] tartalmazza.)

8. ÖSSZEFOGLALÁS

A RED algoritmus kidolgozásának célja a FIFO (*Drop Tail* – FIFO puffer, mely a beérkező csomagot dobja el túlcsorduláskor) hiányosságainak korrigálása volt. A RED a véletlenszerűséget használja arra, hogy az összes találkozó összeköttetésnek biztosítsa közelítőleg ugyanazt a vesztési arányt, illetve sávszélességet. A torlódást is megpróbálja megelőzni csomagdobásokkal reagálva mielőtt még az útvonalválasztó puffere teljesen megtelne.

A cikkben bemutattuk a RED algoritmust és tulajdonságait. Szimulációs eredményeinkkel rávilágítottunk az előnyökre és a hátrányokra, majd ezeket összehasonlítottuk a FIFO pufferrel. Bemutattuk a RED lehetséges továbbfejlesztéseit, az adaptív RED és a FRED algoritmust.

IRODALOM

[1] Floyd S., Jacobson V.: Random Early Detection gateways for Congestion Avoidance. *IEEE/ACM Transactions on Networking*, Vol. 1, No. 4. 1993. 397-413 old. http://wwwnrg.ee.lbl.gov/floyd/red.html

[2] Jacobson V.: Congestion Avoidance and Control. *SIGCOMM Symposium on Communications Architectures and Protocols*, 314-329 old., 1988. ftp://ftp.ee.lbl.gov/papers/congavoid.ps.Z

[3] W. Stevens: RFC 2001, 1997. http://www.ietf.org

[4] R. Jain: The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurement, simulation and Modelling. John Wiley and Sons, Inc., New York, 1991

[5] Dong Lin, Robert Morris: Dynamics of Random Early Detection, Division of Engineering and Applied Sciences, Harvard University, Cambridge, MA 02138 USA

[6] W. Feng, D. Kandlur, D. Saha, K. Shin: Techniques for Eliminating Packet Loss in Congested TCP/IP Networks, Department of EECS, University of Michigan

[7] Fall K., Floyd S. 'Comparisons of Tahoe, Reno, and Sack TCP' 1995. Elérhető: ftp://ftp.ee.lbl.gov/papers/sacks.ps.Z

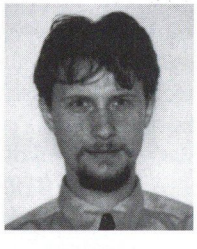
TESTING THE RED ALGORITHM

G. BAJKÓ, GY. BÓDOG, T. KASZA

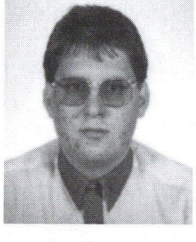
TECHNICAL UNIVERSITY OF BUDAPEST, DEPARTMENT OF TELECOMMUNICATIONS & TELEMATICS

Active queue management has been proposed as a solution for preventing losses due to buffer overflow. The idea behind active queue management is to detect incipient congestion *early* and convey congestion notification to the end-hosts, allowing them to back off before queue overflow and packet loss occur. One form of active queue management is RED (*Random Early Detection*). RED maintains an exponentially weighted moving average of the queue length which it uses to detect congestion. The RED also maintain two thresholds: a minimum ($\min_{\text{th}}$) and a maximum threshold ($\max_{\text{th}}$). When the average queue size (avg) exceeds a minimum threshold, packets are randomly dropped with a given probability (p_a). This probability depends on the average queue size, the time elapsed since the last packet was dropped ($count$), and an initial probability parameter ($\max_p$). When the average queue size exceeds a maximum threshold, all arriving packets are dropped.

We examine this RED queue with the Network Simulator. We introduce the RED algorithm and its behaviour; our simulation results show advantages and disadvantages of this form of queue management. We compare RED and FIFO queues and we report the adaptive RED and FRED algorithms also.



Bajkó Gábor 1996-ban szerzett villamosmérnöki oklevelet. Azóta a Budapesti Műszaki Egyetem PhD hallgatója, főbb kutatási tevékenységei között a TCP algoritmusok, puffer management, routing protokollok és MPLS hálózat szerepel.



Bódog Gyula végzős hallgató a Budapesti Műszaki Egyetem Villamosmérnöki és Informatikai karán. 1997-től tanulmányait a Távközlési és Telamatika szakirányon folytatja. 1998 nyarán Svédországban MPLS hálózat szimulációjával foglalkozott. Az egyetemen kutatási témája a TCP implementációk vizsgálata, valamint a RED puffer szimulációs analízise volt. 1998-ban a Tudományos Diákköri Konferencián ezzel a témával harmadik díjat nyert Kasza Tamással.

Kasza Tamás a Budapesti Műszaki Egyetem diplomatervező hallgatója a távközlés és telematika fő- és a mobil hírközlés mellékszakirányon. 1997-ben a Deutsche Telekom multimédia és távközlés pályázatának nyertese. A Tateyama Kagaku Ind. Co. Ltd. (japán) cég ösztöndíjasaként szórt spektrumú mikrohullámú átvitellel foglalkozott 1998-ban. Az egyetemen kutatási témája a TCP implementációk vizsgálata, valamint a RED puffer szimulációs analízise volt.

ADATVÉDELMI RENDSZEREK ATM HÁLÓZATOKBAN

TÖRÖK ATTILA, FISCHER LAJOS, SIMON CSABA

BUDAPESTI MŰSZAKI EGYETEM
TÁVKÖZLÉS ÉS TELEMATIKA TANSZÉK
NAGYSEBESSÉGŰ HÁLÓZATOK LABORATÓRIUM (HSNLAB)
1111 BUDAPEST, PÁZMÁNY PÉTER SÉTÁNY 1/D

Ebben a cikkben egy ATM tűzfal általunk javasolt protokoll rendszert mutatjuk be. A cikk első részében röviden áttekintjük a jelenlegi ajánlásokat az ATM hálózatok adatvédelmére majd rátérünk a saját ajánlásunk bemutatására. Az általunk ajánlott módszer lehetővé teszi az integritásvédelem használatát a köztes hálózati elemekben is. A módszerünk egy másik előnye, hogy megkönnyíti a tűzfalak konfigurálását. Cikkünk végén szimulációk segítségével megvizsgáltuk a protokollunk viselkedését. Elemeztük a kapcsolók sorainak a változását, a kapcsolatok kiépülési idejét és az eldobott hívások számának változását.

1. BEVEZETÉS

Napjaink megnövekedett információátviteli igénye miatt az Aszinkron Átviteli Módú (Asynchronous Transfer Mode) hálózatok széles körű elterjedésének vagyunk tanúi. A jelenleg használatban lévő ATM hálózati elemek nem rendelkeznek adatvédelmi funkciókkal, viszont a szélesebb körű elterjedéshez szükség van a felhasználói adatok biztonságos átvitelére is. A biztonsági szolgáltatásokat különösen a nagy felhasználók (bankok, multinacionális cégek, kormányszervezetek és kutatási intézmények) igénylik. Az ilyen felhasználókra jellemző, hogy több, földrajzilag elhatárolt kirendeltségük van, amelyek belső hálózata biztonságosnak tekinthető, ellenben a vállalati hálózat (Virtual Private Network – VPN) megvalósításához szükséges ezen kirendeltségek összekötése. Ez adatvédelemmel nem rendelkező nyilvános hálózatokon keresztül történik.

Ezért van szükség a tűzfalak használatára, amelyek a lokális, biztonságos hálózat-szigetek összekötésére szolgálnak, egy nyilvános, nem védett hálózaton keresztül. A tűzfalak feladata a belső magán hálózat védelme, ezt a védelmet a rajtuk átmenő csomagok szűrésével és/vagy titkosításával valósítják meg. A tűzfalak megjelenését több tényező is befolyásolta: egyrészt a hálózati protokollok tervezésekor az adatvédelmi infrastruktúra kiépítésének a hiánya, másrészt pedig a komplex hálózati védelemmel rendelkező rendszerek adatvédelmi koncepciójának a tervezési és karbantartási nehézségei.

Az ATM hálózatok adatvédelmi protokollrendszere még nincs kidolgozva, fejlesztés alatt áll. Az ATM Forum jelenleg dolgozik egy adatvédelmi specifikáción [1], ugyanakkor még léteznek más ajánlások is [12], [6].

Mivel az ATM hálózatok protokollrendszere sem tartalmaz adatvédelmi funkciókat, természetesebbnek tűnik, hogy ezen hálózatok protokolljainak megváltoztatása nélkül előbb tűzfalakat implementáljunk.

Az általunk kidolgozott tűzfal protokollrendszere lehetővé teszi az adatok biztonságos átvitelét és védelmét. Egy új módszer segítségével a tűzfal felderítheti más tűzfalak címeit, így megkönnyíti a rendszergazda feladatát a tűzfal konfigurálásánál. Ezenkívül lehetőség nyílik többszintű védelmi rendszer kiépítésére egy VPN-en belül.

2. A NEMZETKÖZI EREDMÉNYEK ÁTTEKINTÉSE

Jelenleg, az ATM hálózatok egyik gyenge pontja az, hogy nem biztosítanak adatvédelmi szolgáltatásokat a felhasználóknak. Erre a problémára számos javaslat született az utóbbi időben. A fejezet első részében az ATM hálózatok adatvédelmére javasolt megoldásokat ismertetjük, majd ezeket elemezzük és összehasonlítjuk. Ismertetjük az ATM referencia modellben igényelt módosításokat, a javaslatok által nyújtott adatvédelmi szolgáltatásokat és ezek megegyezési mechanizmusait, a szinkronizációs és kulcscserélő módszereket.

Az ATM hálózatokban a védelem megvalósításához szükség van arra, hogy az adatvédelmi eszközök egymás között biztonságosan kommunikáljanak. Ennek érdekében egymás között meg kell egyezzenek, hogy a kapcsolat során milyen védelmi stratégiát és algoritmusokat fognak alkalmazni a felhasználói adatok védelmére.

Több lehetőség is létezik, hogy az adatvédelmet biztosító hálózati elemek megvalósítsák az egymás közti védelemmel kapcsolatos információcserét. Új információs elemek (Information Element – IE) beiktatásával a vezérlési síkban végezhető el az információcsere, ekkor a csatornát felépítő jelzési üzenetekbe kerül az új védelmi információs elem. Ez a módszer a jelenlegi hálózati elemek protokolljainak a megváltoztatását igényli, mivel ezek fel kell tudják ismerni az új információs elemeket és ezen elemek tartalma alapján ezeket feldolgozzák vagy transzparensen továbbküldjék. A speciális IE-k használata lehetővé teszi a jelzési üzenetek védelmét, viszont a nagy mennyiségű plusz információ és ennek a feldolgozása leterhelheti a köztes kapcsolókat [16].

Egy másik módszer speciális OAM (Operation And Maintanance) [17] cellák segítségével oldja meg az adatvédelmi információk kicserélését. Ebben az esetben is szükségessé válik, hogy a protokollokat módosítsuk, mert fel kell tudják ismerni ezeket a speciális cellákat. Az információcsere, ezen cellák segítségével, csak a kapcsolat kiépítése után történhet meg, mivel az OAM cellák a VPI/VCI szerint irányítódnak.

A harmadik módszer (segédcsatornát használó módszer) a felhasználó által küldött kapcsolatfelépítő jelzési üzenetek (SETUP, CONNECT) után küldené az adatvédelmi információkat mielőtt az első felhasználói adatok megérkeznének a védelmet megvalósító hálózati elemhez. Ebben az esetben csak az adatvédelmi elemek protokolljait kell módosítani mivel az adatvédelmi információk transzparensen haladnak át a hálózaton. A vevő védelmi rendszer ezen

adatokat kiveszi a csatornáról, nem hagyja, hogy a végfelhasználóhoz jussanak. A jelzési üzeneteket nem lehet védeni, mivel ezek nem tartalmaznak új információs elemeket.

Természetesen ezen módszereket kombinálni is lehet tetszés szerint.

A felhasználói adatok védelme a felhasználói sík (user plane) különböző rétegeiben is megtörténhet, ezt az ATM rétegben, az AAL rétegben, esetleg az AAL réteg fölött lehet megvalósítani.

A következőkben rövid áttekintést nyújtunk a jelenleg kidolgozás alatt álló adatvédelmi módszerekről, amelyek az ATM hálózatok biztonságát hivatottak szolgálni.

2.1. Az ATM Forum adatvédelmi specifikációja [1]

Ez a legjelentősebb adatvédelmi specifikáció az ATM hálózatok védelmére, amely mindhárom fent említett lehetséges módszert tárgyalja az adatvédelmi információk átvitelére.

Az első módszer egy adatvédelmi információs elemet ír elő, amelyet a jelzési üzenetekbe kell beletenni. Ez magába foglalja a hitelesítést, a hozzáférés védelmet (acces control), a kétutas kulcscserélő algoritmusokat és az adatvédelmi paraméterek (security context) egyeztetését. Ily módon lehetségessé teszi a végpontok és a hálózati kapcsolók közti biztonságos adatcsatorna kiépítését a kapcsolat kiépítésével egyidőben, ugyanakkor a jelzési információk védelmét. A jelzési információ védelmét egy segédcsatornán előre kicserélt kulcs felhasználásával oldja meg. A jelzési üzenetben cseréli ki az úgynevezett fő kulcsot, amely a szesszió kulcsok kicserélésénél a titkosításban játszik szerepet. A szesszió kulcsokkal fogjuk az adatokat titkosítani, ezeket a kulcsokat gyakrabban kell cserélni. Két lehetséges stratégiát dolgozott ki az ATM Forum a kommunikáció védelmére a nyilvános hálózatokon keresztül.

Az első szerint csak a végfelhasználók használnának adatvédelmi funkciókat a saját adataik megvédésére a nyilvános hálózati elemek segítsége nélkül, vagyis a felhasználók által kódolt adatok transzparensen haladnának át a közcélú hálózaton. A második stratégia szerint a köztes hálózati elemek is részt vesznek a védelem megvalósításában, így csomópontonként változhat a kommunikáció védelme.

Egy, a nyilvános hálózaton felépült kapcsolat védelmére a biztonsági felek meg kell egyezzenek egy védelmi stratégiában, ezt egy új mezőben végzik el (security association section), amelyet az adatvédelmi IE-hez illesztenek.

A második módszer speciális OAM cellák használatával tenné lehetővé az adatvédelmi rendszer menedzselését és karbantartását (pl. kulcscsere). Ez a módszer biztosítani tudja a szinkronizációt a kicserélendő adatvédelmi információ és a felhasználói adatfolyam között. A szesszió kulcsok cseréje két lépésben történik. Először az új szesszió kulcs továbbítódik a hálózaton az adatvédelmi partnernek, a második lépésben ez a kulcs aktiválódik, hogy az ezután küldött felhasználói adatokat kódolja, illetve dekódolja. Az OAM cella, amely a szesszió kulcsot tartalmazza a jelzési üzenetekben kicserélt fő kulccsal lesz titkosítva.

Az ATM Forum által ajánlott harmadik módszer a már felépült felhasználói csatornán keresztül küldi az adatvédelemhez szükséges információkat, a kapcsolat felépítés után, a felhasználói adatok ideiglenes leblokkolásával. Ez a módszer a második módszerrel közösen használható, hogy az adatvédelmi paramétereket a védelmi partnerek egymás között az adatcsatorna kiépítése után is kicserélhessék.

Ezek a módszerek a kapcsolat kiépítés védelmére a következő szolgáltatásokat teszik lehetővé: hitelesítés, integritás védelem (integrity), visszajátszás elleni védelem (replay detection), kulcscsere, adatvédelmi szolgáltatások kiegyezése, hozzáférés védelem (acces control).

Az ATM Forum mindhárom ajánlása esetében a felhasználó adatainak a titkosítása az ATM rétegben történik, az ATM cellák szintjén. A titkosítás történhet végpontok között vagy lépésenként, viszont az integritásvédelem csak végpontok között lehetséges. Az integritásvédelem és a visszajátszás elleni védelem az AAL rétegben történik, a védendő AAL SDU-hoz illesztve a következő mezőket: aláírás (amelyet az AAL SDU-ra számítunk ki), időpecsét (timestamp) és sorszám (sequence number).

A fent említett módszerek közül az első és a második szükségessé teszi a jelenleg használatban lévo hálózati elemek protokolljainak a módosítását. Ugyanakkor, az első módszer a nagy mennyiségű információ miatt, amely a speciális védelmi IE-be kerül bele, leterhelheti a köztes kapcsolókat, amikor ezek egymás között is védelmet akarnak biztosítani, ugyanis ezen információk feldolgozása elég időigényes.

Ugyanakkor az első módszer további hátránya, hogy nem teszi lehetővé a felek között a digitális aláírási algoritmus típusának a tetszoleges kiválasztását, továbbá a kölcsönös hitelesítést sem kérheti a hívott védelmi fél. Ráadásul csak a kétutas kulcscserét teszi lehetővé. A második módszer hátránya, hogy mivel az OAM cellák igen kis mennyiségben iktathatók be a felhasználói adatok közé így nem lehetséges a használatuk valós idejű adatátvitelnél, továbbá az egyoldali kommunikációt sem támogatja. Előnye a jó szinkronizáció a kulcsok és az adatok között.

A harmadik módszer hátránya, hogy a felhasználói adatok leblokkolása esetén megtörténhet az adatok elvesztése. Ugyanakkor az adatok késleltetődnek és nagy puffereket kell használni a tárolásukra.

2.2. A Stevenson-féle ajánlás [12]

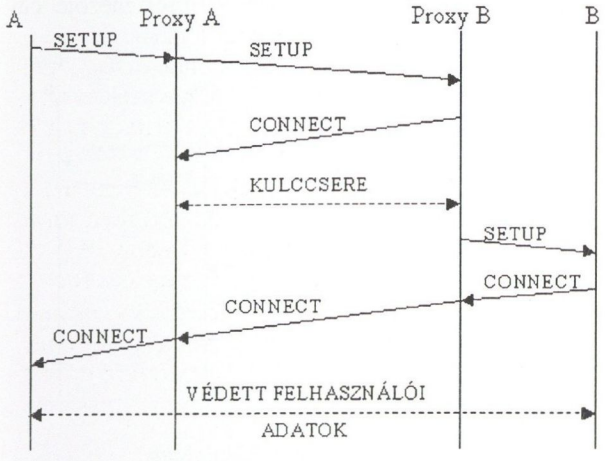
Ez az ajánlás a harmadik módszert használja fel az adatvédelmi kapcsolat kiépítésére.

Stevenson az adatvédelem megvalósítására kriptográfiai proxy-kat használ, ezek leginkább azon LAN hálózatok határán helyezkednek el amelyeknek a védelmét kell biztosítsák, amikor a nyílt hálózaton kommunikálnak egymással. A kulcsok kicserélése a kapcsolat felépítése után történik a felhasználó által kiépített csatornán, az adatok átvitele előtt. Az A felhasználó küld egy SETUP üzenetet a saját proxy-jának amely továbbküldi ezt a B felhasználó proxy-jának. Mielőtt a két felhasználó között a kapcsolat felépülne a két proxy kicseréli egymás között a szesszió kulcsokat. Ezután befejeződik az A által kezdeményezett kapcsolat felépítése azzal, hogy a B proxy-ja elküldi B-nek a SETUP üzenetet, amelyre B egy CONNECT-el válaszol.

Az 1. ábrán a módszer működését vázoltuk.

A protokoll a kapcsolaton átmenő felhasználói adatok titkosítására egy szesszió kulcsot használ. A Stevenson-féle megoldás a felhasználói adatok védelmére csak titkosítást

szolgáltat, amelyet az ATM Forum megoldásához hasonlóan a felhasználói sík ATM rétegében végez el.



1. ábra. A Stevenson-féle segédcsatornát használó modell

A modell hátránya, hogy a megegyezett adatvédelmi paramétereket nem lehet újratárgyalni a kapcsolat időtartama alatt és nem teszi lehetővé a felhasználói adatok integritásvédelmét.

Előnye, hogy az adatvédelmi felek között az adatvédelmi paraméterek kiegyezési ideje alatt tetszoleges mennyiségű információcsere lehetséges. Így lehetővé válik a két vagy háromutas protokollok használata is. További előnye, hogy nem kell módosítani a köztes kapcsolók protokolljait.

Az ATM Forum modellje leginkább abban különbözik a Stevenson-féle modelltol, hogy egy külön csatornát használ a paraméterek kicserélésére, továbbá abban, hogy a kapcsolat ideje közben is leblokkolhatja az adatokat a paraméterek kicserélése idejére.

2.3. A Laurent-féle ajánlás [6]

Az ATM Forum módszeréhez hasonlóan ez a módszer is egy új adatvédelmi információs elemet tesz be a jelzési üzenetekbe. Ez az információs elem több védelmi egységre van osztva, ezekbol mindegyik a különböző adatvédelmi szolgáltatások kiegyezésére vagy a szolgáltatás biztosítására elhivatott. Ezek a szolgáltatások vonatkozhatnak a jelzések vagy az adatok védelmére és mindegyikük opcionális.

A Laurent-féle modell egy adatvédelmi protokollrendszert határoz meg, amelyet azokba az ATM kapcsolókba kell implementálni, amelyekhez közvetlenül a felhasználók kapcsolódnak. A speciális IE által a jelzések védelmére nyújtott szolgáltatások a következők: hitelesítés, integritás védelem és visszajátszás elleni védelem, továbbá titkosítás, a felhasználó identitásának elrejtése (anonymity) és az adatvédelmi paraméterek kiegyezése.

A felhasználói adatok védelmét szolgáló réteg az AAL réteg fölé van beillesztve (Secure Data Exchange-SDE) és a következő szolgáltatásokat teszi lehetővé: felhasználói adatok titkosítása, integritás védelme és hitelesítése. A szinkronizáció az SDE PDU-jában valósul meg úgy, hogy az AAL csomagok rakományába szinkronizációs információt helyezünk. Ezek lehetnek a szesszió kulcsok sorszámai vagy az inicializáló vektor.

Ez az ajánlás nyújtja a legteljesebb körű szolgáltatásokat a jelzések védelme érdekében. Lehetővé teszi a jelzési üzenetek (SETUP, CONNECT) titkosítását és a mezőinek az elrejtését. Továbbá lehetséges a felhasználó címének az elrejtése is, azáltal, hogy titkosítva belekerül a speciális IE-be és a helyére az adatvédelmet nyújtó kapcsoló címe kerül. Hátránya akárcsak az ATM Forum ajánlásainak, hogy módosítani kell az aktuális protokollokat. További hátrányaként említhető, hogy mivel az AAL réteg fölött helyezkedik el, nem tud nagy mennyiségű adatfolyamot kezelni.

3. A TŰZFALAK KÖZÖTTI PROTOKOLLRENDSZER

A tűzfalak, a felhasználói adatok biztonságos átvitele érdekében egymással fel kell vegyék a kapcsolatot, hogy megegyezzenek a nyújtani kívánt adatvédelmi szolgáltatásokban.

A hagyományos IP alapú hálózatokban alkalmazott tűzfalak esetében, minden tűzfal rendelkezik egy adatbázissal amely tartalmazza a többi, ismert tűzfal címét. Ezeket a címeket a rendszergazda manuálisan állítja be. Amikor egy tűzfal egy felhasználói adatcsomagot kap, akkor ennek a címe alapján tudja azonosítani, hogy a csomag egy más tűzfal által védett hálózatba megy-e. Ha igen, akkor a csomagon végrehajtja a másik tűzfallal előre megbeszélt algoritmusokat, az egymás között kicserélt kulcsokat használva. A fenti módszernek két hátránya is van:

- Előfordulhat olyan eset amikor a csomag egy olyan hálózatba irányul, amelyben van tűzfal, viszont a küldő tűzfalnak nincs tudomása erről. Ebben az esetben a tűzfal nem kódolja a csomagot, legfennebb csomagszűrést alkalmaz.
- A rendszergazda manuális kell konfigurálja a tűzfalak címtáblázatait.

A fent vázolt okok miatt szükség lesz egy olyan módszerre, amelynek segítségével egy tűzfal fel tudja deríteni, hogy a célhálózatban létezik-e egy másik tűzfal, az adatok biztonságos elküldése érdekében.

A módszerünkben, a küldő tűzfal a felhasználótól kapott SETUP üzenet AAL5 farokrészének user-to-user indication mezőjébe egy információt helyez. A vevő tűzfal megvizsgálja ezt a mezőt és ha megtalálja az illető információt akkor tudja, hogy egy másik tűzfal küldte a SETUP-ot. A user-to-user mezőt jelenleg semmilyen protokoll sem használja, egy következő fázisban viszont lehetne speciális IE-t használni ez a mező helyett.

3.1. Az adatvédelmi eszközök azonosítása

Egy komplex WAN hálózatban előfordulhat, hogy a kiépítendő útvonalon több adatvédelmet megvalósító hálózati eszköz is működik. Ezek az eszközök lehetnek tűzfalak, adatvédelmi funkciókkal ellátott kapcsolók, kriptográfiai proxy-k, vagy egyéb hálózati elemek. A kiépítendő kapcsolat védelme érdekében ezek az eszközök egymás között fel kell vegyék a kapcsolatot és megegyezzenek a védelmi politikát illetően.

Mielőtt a tűzfalak azonosító procedúráját felépítenénk, megemlítjük, hogy a jobb biztonság érdekében lehetővé kellene váljon egy biztonságos hálózaton belül további biztonságos alhálózatok létrehozása. Erre például akkor lehet szükség amikor egy intézményt a külvilágtól egy tűzfallal védünk, ugyanakkor az intézményen belül a fontosabb al-

hálózatokat (pl. kutatási részleg, gazdasági részleg) szintén tűzfalakkal, vagy adatvédelmi proxy-kal védjük. A védelmi berendezéseket közvetett módon, a címük szerint fogjuk azonosítani. Egy adatvédelmi eszköz csak akkor fog a kapott üzenetre reagálni amikor a kapott üzenet eszköz azonosító mezője megegyezik a saját azonosítójával.

A mi esetünkben két helyzet fordulhat elő, amikor egy tűzfal egy kapcsolatfelépítő üzenetet kap egy felhasználótól.

Az első esetben a tűzfal ismeri a célhálózatot, amelybe a kapcsolatkiépítési kérelem irányul, akkor a védelmi politikájának megfelelően meg tudja határozni, hogy a védelmi szolgáltatásokkal rendelkező hálózati elemek közül melyikkel/melyekkel vegye fel a kapcsolatot. Nyilvánvalónak tűnik, hogy a megfelelő tűzfal kiválasztása még a kapcsolatkiépítés közben meg kell történjen. A célállomás címe annak a tűzfalnak a címét fogja tartalmazni amellyel a kezdeményező tűzfal kapcsolatba akar lépni.

A végfelhasználó címe a két tűzfal által kiépített csatornán fog titkosítva átkerülni a céltűzfalhoz, így ezúttal a felhasználó identitását is eltitkoljuk, akárcsak a Laurent-féle modell egyik szolgáltatása.

A második esetben (2. ábra) a tűzfal egy ismeretlen hálózatba irányuló SETUP üzenetet kap. Ekkor elsőre nem tudja megállapítani, hogy milyen adatvédelmi egységekkel tudna adatvédelmi kapcsolatot kiépíteni, így fel kell derítse a még ismeretlen hálózatot. Ilyenkor a felderítő típusú jelzés folyamot kell használja.

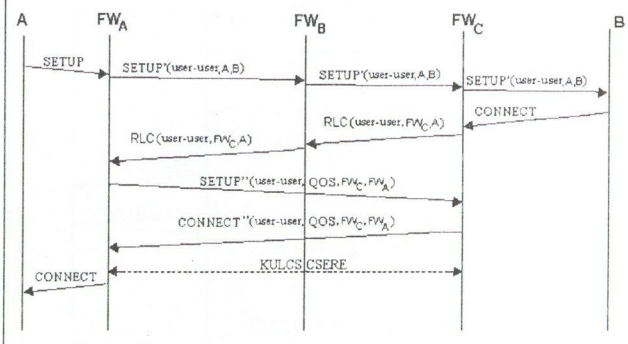
Amikor az FWA tűzfal egy SETUP üzenetet kap a felhasználótól akkor a SETUP üzenet AAL5 farokrészének a user-to-user mezőjébe beleír egy azonosítót amely jelezni fogja, hogy a SETUP üzenet átment egy tűzfalon.

A tűzfalak között a felhasználó által igényelt sávszélességet meg kell növelni, hogy biztosítva legyen az átvitel az adatvédelmi információk számára. A sávszélesség növelése a következő problémákat vonja maga után: ha az FWA tűzfal a felhasználói SETUP üzenet QoS-ét megváltoztatja és így elküldi akkor előfordulhat, hogy ez a módosított SETUP' üzenet eljut a címzett felhasználóhoz. Ez abban az esetben fordulhat elő, amikor a túlsó oldalon nem létezik tűzfal amely a megváltoztatott SETUP' üzenetet fogadja. Ilyenkor feleslegesen foglalódik le a megnövelt sávszélesség.

Amikor egy tűzfal egy felderítő típusú SETUP jelzést kap, akkor nem válaszol azonnal egy RELEASE COMPLETE üzenettel, hanem először továbbküldi a SETUP üzenetet. Így megállapítja, hogy van-e még tűzfal közte és a címzett felhasználó között. Ha a visszajövő CONNECT üzenet a user-to-user mezőjében nem tartalmazza a megfelelő azonosítót akkor ez azt jelenti, hogy nincs tűzfal a vonal további részén. Az utolsó tűzfaltól visszafele már nem a CONNECT üzenet hanem egy RELEASE COMPLETE üzenet lesz továbbítva. Ez a RELEASE COMPLETE egészen a kezdeményező tűzfalig fog terjedni, amely ezt megkapva egy növelt sávszélességű kapcsolat kiépítését fogja kezdeményezni. A növelt sávszélességű kapcsolat a két szélső tűzfal között fog kiépülni.

A következő jelöléseket használtuk és használjuk még a továbbiakban is:

- SETUP(QoS): megváltoztatott sávszélesség lefoglalás a SETUP üzenetben. Ez azért szükséges, hogy a felhasználói adatok közé beszúrt speciális cellák átvitelére is biztosítva legyen a sávszélesség.
- SETUP(user-user): az AAL5 user-to-user mezője egy azonosítót tartalmaz.



2. ábra. A felderítő típusú jelzésfolyam

A köztes tűzfalak speciális cellákban kell a kezdeményező tűzfallal kicseréljék az információkat. A kezdeményező tűzfal a felderítő SETUP' üzenetbe a hívó fél címét kénytelen beletenni, ugyanis abban az esetben ha nincs más tűzfal, a címzett felhasználóhoz a rendes kezdeményező felhasználó címe kell eljusson.

Az utolsó tűzfal a visszaküldött RELEASE COMLETE üzenetbe beleteszi a saját címét, innen a kezdeményező tűzfal tudni fogja, hogy kinek címezze a bővített sávszélességű SETUP'' üzenetet.

A fent leírt felderítő típusú jelzések kiválóan alkalmazhatóak abban az esetben amikor a célhálózatról tudott, hogy létezik benne tűzfal, csak nem tudjuk a címét. Ilyen esetek előfordulhatnak például az intézmény VPN-jének a védelme kiépítésekor, intézmények közti kapcsolatfelvételkor (pl. videokonferencia).

Abban az esetben amikor nem tudjuk, hogy van-e tűzfal a másik hálózatban és egy támadó épül be az éppen létrejövő kapcsolatba a következő eset állhat elő. Feltételezzük, hogy a támadó képes módosítani a jelzéseket. Megtörténhet, hogy a támadó kiveszi a jelzés user-to-user mezőjéből az azonosítót, így a másik tűzfal azt hiszi, hogy egy tűzfal nélküli hálózatból kapta a jelzést. Ez a tűzfal egy hagyományos jelzéssel válaszol, így a két tűzfal között nem jön létre a védelmi kapcsolat.

Annak elkerülésére, hogy a támadó ne tudja a tűzfalakat kicselezni az alábbi módszert alkalmazzuk.

A kezdeményező tűzfal T hosszúságú ideig a felhasználói AAL csomagok közé véletlenszerűen speciális védelmi AAL csomagokat iktat be. Ezeknek a feladata jelezni a másik tűzfalnak, hogy a kapcsolat kezdeményezője egy tűzfal volt. A támadó nem tehet semmit, mert nem tudja megállapítani, hogy melyek a speciális csomagok és melyek a felhasználói adatcsomagok, így kénytelen továbbengedni őket. A speciális csomagok úgy vannak kódolva, hogy a támadónak ne legyen ideje azokat dekódolni. Ez a kódolás egy időzáras rejtvény (time-lock puzzle) [12] segítségével valósul meg, amelynek a lényege, hogy csak egy bizonyos hosszúságú, folyamatos dekódolás után derül ki a védett csomag tartalma. A dekódolás idejét nem lehet felgyorsítani párhuzamos feldolgozással sem. A speciális csomagok CRC kódját a kezdeményező tűzfal el kell rontsa, ezzel meggátolja azt, hogy ezek a felhasználónál értelmezésre

kerüljenek. A vevő tűzfal a T idő alatt összes bejövő csomagot megpróbálja dekódolni, hogy megkapja a speciális csomagot, nyugodtan továbbengedheti az összes csomagot mivel a speciális csomagokat a felhasználó úgyis eldobja.

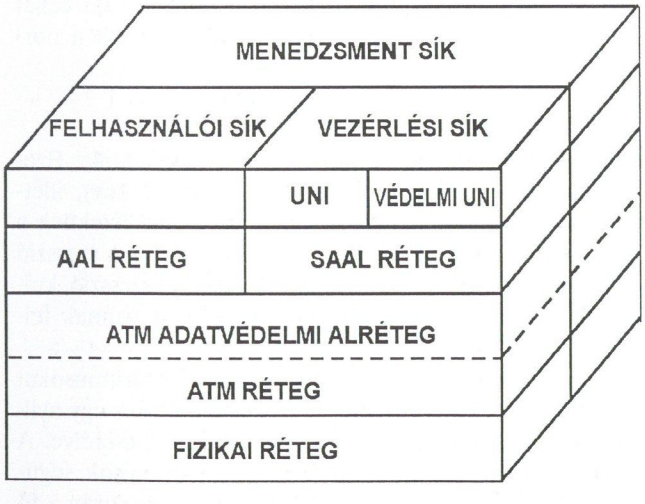
4. A FELHASZNÁLÓI ADATOK BIZTONSÁGOS ÁTVITELE

4.1. A módosított referencia modell

A felhasználói adatok nagyobb biztonságának garantálása érdekében az adatvédelemmel kapcsolatos információkat ki kell tudjuk cserélni az adatvédelmi felek között, az adatcsatorna kiépülése után is. Ezek az adatvédelmi információk lehetnek a felhasználói adatok hitelesítésére szolgáló aláírások, időpecsétek, szesszió kulcsok stb.

Attól függően, hogy az adatok titkosításáról vagy integritásvédelméről van szó az első fejezetben ismertetett ajánlások különböző protokoll rétegeket használnak. Az integritásvédelmet megvalósító réteg az ismertetett modellekben mindig az AAL rétegben vagy az AAL réteg fölött helyezkedik el. A titkosítást végzo réteg az ATM rétegben vagy fölötte helyezkedik el. Az ATM rétegben megvalósított titkosítás előnyei között megemlíthetjük, hogy sokkal gyorsabb kódolás érhető el vele, mivel a titkosítás hardverbol végezhető el, továbbá a kódolás is egyszerűbb, mivel az átkódolandó adatblokkok mérete állandó (48 bájt az ATM cellák rakománya). Még megfigyelhetjük, hogy az integritásvédelem az ismertetett modellekben csak végpontok között működik, a nyilvános hálózat adatvédelmi elemei nem végeznek integritásvédelmet.

A tűzfalon igen nagy sebességű és nagy mennyiségű adat haladhat át, így nem lesz arra lehetőség, hogy a kapott ATM cellákat a tűzfalban várakoztatjuk majd összerakjuk AAL csomagokká, elvégezzük rajtuk a szükséges műveleteket, majd megint feldaraboljuk és továbbküldjük őket. Tehát nem lehet egy AAL szintű adatvédelmi protokollt használni, ezért a mi modellünkben a titkosítást és az integritásvédelmet is az ATM rétegben fogjuk megvalósítani. Az általunk módosított referencia modellt a 3. ábrán ismertetjük.



3. ábra. A módosított ATM referencia modell

Először is azt kell megjegyeznünk, hogy a fenti ábrán bemutatott változtatásokat csak a tűzfalak referencia modelljében kell eszközölni, a hálózat többi elemén nem kell semmiféle módosítást végrehajtani.

A tűzfalak a köztes UNI protokollt használják, úgy tekinthetőek mint terminálok így a speciális cellák transzparensek lesznek a nyilvános hálózaton működo kapcsolók számára.

A vezérlési sík megváltoztatása azért szükséges mert a tűzfalak egymás között a módosított jelzési folyamokkal kell, hogy kommunikáljanak.

A védelmi ATM réteg figyeli az SAAL rétegtol kapott csomagokat és jelzéseket, innen fogja megtudni, hogy mikor épült ki az adatcsatorna, vagyis mikor fogja tudni megkezdeni a másik tűzfallal az információk kicserélését a speciális cellák segítségével. Az SAAL rétegtol kapott csomagokat nem kódolja át. A védelmi UNI bizonyos információs elemeket kivehet az elküldendő jelzési üzenetbol (pl. a címzett felhasználó címét kicseréli a másik tűzfal címére), viszont nem tesz bele új információs elemeket, amelyeket a hálózat elemei nem ismernének fel. Az adatvédelmi információk kicserélése nem valósulhat meg a vezérlési síkban mivel ez új információs elemek használatát igényelné. Ezért használjuk a speciális cellákat. Az ATM rétegbe beépített védelmi réteg fogja a speciális cellákat kezelni. Ez a réteg kódolja a felhasználó adatait és generálja a speciális cellákat. Ugyanakkor a feladata a kapott cellák azonosítása, hogy megállapítsa speciális cellák-e vagy sem. A címzett tűzfalnál pedig a felhasználói adatok dekódolása és a speciális cellák eltávolítása a csatornáról.

Szükség van arra, hogy a védelmi ATM réteg, bizonyos információk kicserélésekor a két tűzfal között, biztonságos átvitelt biztosítson. Ugyanakkor az adatvédelemmel kapcsolatos információk, amelyeket a speciális cellákba helyez különböző hosszúságúak lehetnek.

4.2. A speciális cellák

Ahhoz, hogy az adatvédelmi információkat elküldhessük a másik tűzfalnak, szükségünk van egy azonosítási módszerre amellyel a másik tűzfal meg tudja őket különböztetni a felhasználói adatoktól. Mivel az ATM rétegben dolgozunk, ATM cellákba kell csomagoljuk az adatvédelemmel kapcsolatos információkat, ezek lesznek a speciális cellák. Tehát a speciális ATM cellák szerepe, hogy a felhasználói adatok védelmével kapcsolatos információkat (digitális aláírás, időpecsét stb.) hordozzák a két tűzfal között, továbbá, hogy a két tűzfal közti adatvédelmi információk kicserélését (algoritmusok kiegyezése, adatvédelmi paraméterek újratárgyalása, kulcsok cseréje) is lehetővé tegyék. Fontos megemlítenünk, hogy a speciális cellák szinkronban kell legyenek az adatcellákkal, mivel olyan információkat hordozhatnak (pl.: kulcsok) amelyek helytelen használata (a deszinkronizáció miatt) a felhasználói adatok elvesztéséhez vezethet.

Az általunk alkalmazott módszer a következő lesz: a felhasználó által kiépített csatornán a rendes adatcellák közé iktatjuk be a speciális cellákat. Ennek a módszernek az előnye, hogy a felhasználói adatcellák és a speciális cellák között a szinkronizáció nem fog megszakadni, mivel mindkét típusú cella ugyanabban a csatornában halad, tehát a hálózat ugyanúgy fog viselkedni mindkét típusú cellára nézve. A speciális cellák adatcellákként a nyilvános

hálózaton transzparensen fognak áthaladni, csak a tűzfalak fogják ezeket felismerni. Így nem lesz arra szükség, hogy a hálózat elemeinek a protokolljait megváltoztassuk.

4.2.1. A speciális cellák azonosítása

A speciális cellák azonosítása az ATM cella rakományában elhelyezett azonosító kód és CRC kód alapján fog történni. A vevő tűzfal megvizsgálja minden egyes ATM cella rakományának az első 16 bitjét (az azonosító kódot) és ha az megegyezik a speciális cellák azonosítójával akkor elvégzi az egész rakományra egy CRC kód kiszámítását. Ha ez talál a rakományban kapott CRC kóddal akkor ez azt jelenti, hogy speciális cellát kapott, ezt fel kell dolgozza, és ki kell vegye az adatcsatornáról. Ha az azonosító kód talál de a CRC nem talál akkor vagy a cella hibásodott meg, vagy pedig egy olyan adatcellát kapott amelynek az első 16 bitje véletlenül megegyezik a speciális cellák azonosítójával. Mivel a hibák esélye nagyon kicsi az ATM hálózatokban [11], a második esetet kell venni.

A CRC kód kiszámítása és az azonosító megvizsgálása hardver elemekkel valósul meg, ezen műveletek nem fognak késleltetést okozni az adattovábbításban.

Ahhoz, hogy a speciális cellákat használni tudjuk a két tűzfal közti kommunikációban, a két tűzfal között a felhasználótól kapott SETUP üzenet által kért sávszélességet meg kell növeljük azért, hogy a plusz védelmi cellák beférjenek a két tűzfal között lefoglalt sávszélességbe. A vevő tűzfal a kezdeményező tűzfalhoz visszaküldött CONNECT üzenetbe szintén a növelt sávszélességet teszi vissza. A későbbiekben optimalizálni fogjuk a sávszélesség igényt.

A speciális cellák használatának egy másik előnye az, hogy a tűzfalak PVC csatornák esetén is használhatóak, mivel minden adatvédelemmel kapcsolatos információ ezekben cserélődik ki. A PVC csatornák használatakor elég ha a tűzfalat manuálisan beállítjuk, hogy milyen más tűzfalakkal kommunikáljon. A módosított jelzéseket használó ajánlások [1], DGL???, [5], [6] ilyen esetben nem használhatóak, mivel az adatvédelemmel kapcsolatos információkat a jelzésekben küldik át.

4.3. Hitelesítés a speciális cellák segítségével

A speciális celláknak több funkciója is van, ezeknek a funkcióknak a függvényében fognak bekerülni a felhasználói adatcellák közé. Ha például a felhasználói adatok hitelesítését végzik akkor akár periodikusan is bekerülhetnek bizonyos számú felhasználói adatcella közé. Ekkor a kezdeményező tűzfal a sorra kapott cellákon elvégzi a hitelesítési algoritmust, amelyik cellán elvégezte azt tovább is küldi a vevő tűzfal felé, majd amikor elküldte az utolsó adatcellát is (amely még a periódus része), elküldi a periódus adatcelláin végzett hitelesítést egy speciális cellába ágyazva. Szóval n darab adatcella után küld egy hitelesíto speciális adatcellát.

A felhasználó által kért QoS paraméterek és az adatátvitel sebességének a függvényében fog változni a felhasználói adatcellák száma, amely után bekerül a csatornába egy hitelesítést tartalmazó speciális cella. Ha egy nagy sávszélességű adatfolyamunk van akkor nem iktathatunk be túl sűrűn speciális cellákat mivel a sávszélesség nagyon megnone. Viszont ha alacsony az adatátviteli sebesség akkor sűrűbben kell betegyük a speciális cellákat mert különben a késleltetés nő meg. Azzal az eshetőséggel is kell számoljunk, hogy a kezdeményező tűzfal egy változó előszlású sebességgel rendelkező cellafolyamot kap.

Ebben az esetben nem végezheti periodikusan a hitelesítést mert lehet, hogy sokat kellene várjon arra, hogy megkapja az összes adatcellát amelyre a hitelesítést kiszámolja. Ilyenkor egy bizonyos idő eltelte után egy speciális cellában elküldi a hitelesítést azokra a cellákra amelyek a be nem fejeződött periódushoz tartoztak.

A vevő tűzfal kétféle képpen cselekedhet amikor felhasználói adatcellákat kap:

1. Elvégzi rajtuk a hitelesítést és addig várakoztatja őket amíg meg nem kapja a rájuk vonatkozó hitelesíto speciális cellát. Ez a hitelesíto cella, egy a kezdeményező tűzfal által kiszámítőtt számú adatcella után fog megérkezni (egy periódus), vagy esetleg hamarább ha a kezdeményező tűzfalnál egy időzítő át lett lépve. Ekkor az adatcellákon végzett hitelesítést összehasonlítja a kapott hitelesítéssel és ha azok találnak akkor elkezdheti továbbküldeni az adatcellákat a felhasználóhoz, mivel ezek hitelesek. A speciális cellát a vevő tűzfal kiveszi a csatornáról, vagyis nem küldi el a felhasználónak.
2. A második esetben a beérkező adatcellákon elvégzi a hitelesítés kiszámítását és ezután tovább is küldi őket, nem várakoztatja őket addig amíg megérkezik a hitelesítésük a speciális cellában. A hitelesítés megérkezése után ezt összehasonlítja a felhasználói adatokon elvégzett és eltárolt hitelesítéssel. Ha megegyeznek akkor minden rendben van, ha különböznek akkor figyelmezteti a felhasználót (vagy a rendszergazdát), esetleg felbontja a kapcsolatot.

A második módszer még használható abban az esetben is amikor a kezdeményező tűzfal börsztös forgalom miatt nem tudja a speciális cellákat periodikusan beszúrni. Ekkor elküld egy speciális cellát amelyben jelezni fogja, hogy a kriptográfiai QoS legyengült és, hogy nem küld egyelőre aláírást, viszont az átmenő cellákon folyamatosan kiszámítja. A vevő tűzfal ezt tudomásul veszi és a kapott adatcellákat a fent említett módon továbbküldi. Amikor megkapja a hitelesítést a börsztben szereplo cellákra, akkor elvégzi a hitelesítések összehasonlítását. A kezdeményező tűzfal a forgalmi csúcs lejárta után szintén küld egy speciális cellát amelyben jelzi, hogy a kriptográfiai QoS visszaállt a normális értekre.

4.4. Kulcscserék a speciális cellákban

Protokollunkban két típusú kulcsot használunk. Ezeket a kulcs típusokat fő kulcsoknak (master key), illetve szesszió kulcsoknak (session key) nevezzük. Ezeknek a kulcsoknak különböző szerepe van: a fő kulcsok a szesszió kulcsok kicserélésénél játszanak szerepet, a szesszió kulcsok pedig a felhasználói adatok titkosítására vannak felhasználva.

Minkét típusú kulcscserénél különböző algoritmusokat használunk. A fő kulcsok hosszú élettartamúak és egy nyilvános kulcsú algoritmus segítségével lesznek kicserélve. A szesszió kulcsok cseréje szimmetrikus algoritmusok segítségével történik, rövid élettartamúak és a csere során a fő kulccsal lesznek titkosítva. Mivel a nyilvános kulcsú algoritmusok lassúak, a nagy sebességű adatokat csak szimmetrikus algoritmusok segítségével lehet titkosítani. Miután a két tűzfal között kiépült egy kapcsolat, a tűzfalak ki kell

cseréljék egymás között a fő és szesszió kulcsokat. A kapcsolat élettartama során szintén szükség van a szesszió kulcsok felfrissítésére. Mindkét típusú kulcscserét a speciális cellákban végezzük el.

A kulcscserékhez több speciális cellára is szükség van, mivel egy speciális cellába nem férnek bele a szükséges adatok. Ezért minden speciális cella egy fejlécet kell tartalmazzon amely mutatja, hogy még folytatódnak-e az adatok más speciális cellákban. Ugyanez a fejléc mutatja a speciális cella típusát.

A speciális cellák a következő típusúak lehetnek: hitelesítésre szolgáló, kulcscserére szolgáló, szinkronizációra szolgáló, állapotinformációk szállítására szolgáló speciális cellák.

A fő kulcsok kicserélése két vagy háromutas protokollok segítségével történhet [4], [8], [10], [13]. A szesszió kulcsok kicserélésére háromutas protokollt használunk.

Amikor a tűzfalak felveszik a kapcsolatot egymás között, akkor egyszerre kicserélnek egy fő kulcsot és több szesszió kulcsot. Minden egyes szesszió kulcs érvénybe léptetését egy speciális szinkronizációs cella segítségével oldjuk meg. Ez a cella egy azonosítót fog hordozni, amely a következőkben használandó szesszió kulcsot azonosítja. Ezt a cellát nem árt többször is elküldeni, hogy biztos megkapja a vevő tűzfal.

5. A PROTOKOLL TELJESÍTMÉNYÉNEK VIZSGÁLATA

Ebben a fejezetben szimulációs módszerrel vizsgáljuk az általunk kifejlesztett, felderítő típusú jelzésfolyam által okozott hálózati állapot-paraméterek változását. Céljainkra egy, a tanszéken kifejlesztett szimulátort [13] alakítottunk át. A szimulátort a tűzfalak módosított jelzésfolyamai és a tűzfalak közötti sávszélesség növelés miatt kellett átalakítanunk.

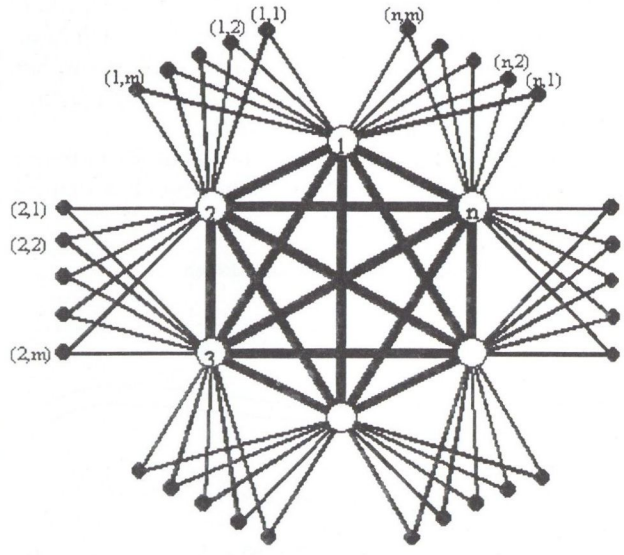
A szimulációkban használt hálózat kapcsolói két koncentrikus körben voltak elhelyezve. A belső kör kapcsolói (ú.n.: gerinchálózati kapcsolók – backbone switch) összekötésére egy teljes kapcsolatú (full mesh) topológiát vettünk alapul. Ilyen típusú hálózatokat általában a nagyvárosi szolgáltatók használnak [15]. A hálózat minden külső kapcsolóját két belső gerinchálózati kapcsolóra kötjük rá, ezt nevezik dual-homing-nak. A dual-homing szerepe a nagyobb biztonság megvalósítása, ugyanakkor a hálózat terhelésének az egyenletes elősztása.

A szimulációk során az összes hívást három percig exponenciális előszlással generáltuk, míg a forrás és a cél állomásokat egyenletes előszlás szerint választottuk ki. A szimulációk szerepe, hogy megvizsgáljuk a hálózat állapot paraméterein a módosított jelzésfolyam által bevitt terhelést.

5.1. A kapcsolók jelzési terhelésének vizsgálata

Három típusú hívást generáltunk, ezek sávszélesség igényei 1 Mbps, 10 Mbps és 35 Mbps. A hívások előfordulásának valószínűségét úgy határoztuk meg, hogy a kisebb sávszélességet igénylo hívások forduljanak elő a legnagyobb valószínűséggel. Ebből adódóan több hívást tudunk generálni a hálózat blokkolásának az eléréséig, így a sorok viselkedését jobban tudjuk vizsgálni. A hívások előfordulási arányai: 70, 20, illetve 10 százalék.

A tűzfal nélküli hálózat hat gerinchálózati kapcsolót és huszonnégy külső kapcsolót tartalmazott. A tűzfalakat tartalmazó hálózat hat gerinchálózati kapcsolót, tizennégy külső kapcsolót és tíz tűzfalat tartalmazott.

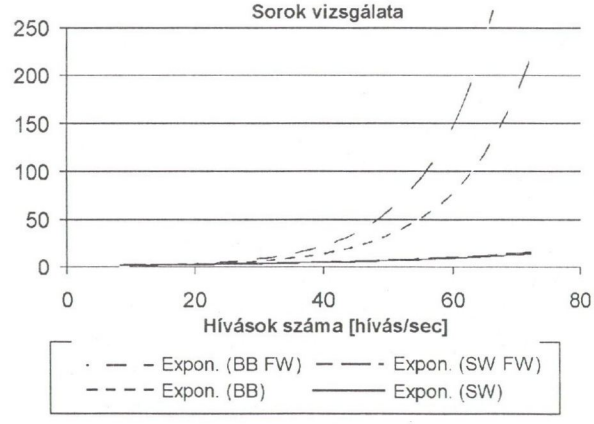


4. ábra. A hálózat topológiája

Két fajta mérést végeztünk a kapcsolók sorai terhelésének tanulmányozása céljából. A mérések folyamán a hálózatot az alacsony terhelésétol egészen a blokkolásáig akartuk vizsgálni. Ennek megfelelően változtattuk a hívások számát 1500-tól egészen 13000-ig.

Az első mérésnél azt vizsgáltuk, hogy a jelzések növekedésének a függvényében hogyan változik a sorok terhelése. Ezzel a méréssel azt akartuk megállapítani, hogy milyen mennyiségű hívásnál kezdenek blokkolódni a hálózatok.

A hívások számát 1500 hívástól (9 hívás/sec) egészen 13000 hívásig (72 hívás/sec) változtattuk. A 5. ábrán láthatjuk az eredményekre ráillesztett trendeket.



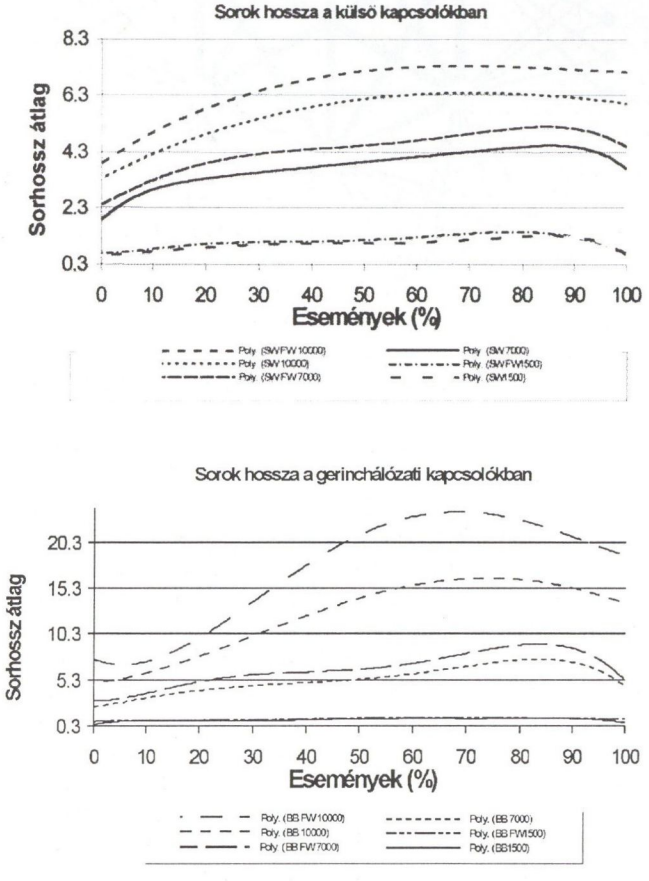
5. ábra. A hívások száma a jelzések növekedésének a függvényében

Észrevehetjük, hogy a gerinchálózati kapcsolók körülbelül 8000 hívásig (45 hívás/sec) bírják a tűzfalak terhelését, 10000 hívásnál (56 hívás/sec) már a két hálózat kapcsolóinak a sorai közötti különbség számottevo. Az 1500, 7000 számú hívások esetében nincs blokkolás a hálózatban.

A tűzfal nélküli hálózat 8000 hívásnál már kezd blokkolni, ezért a tűzfalak jelenléte esetén nem tud megbirkózni a nagy mennyiségű hívásszámmal.

A második mérés sorozatra azért volt szükség, hogy megvizsgálhassuk a tűzfalak és a kapcsolók viselkedését különböző jelzés mennyiségek esetén. Ezért minden egyes hívás mennyiség időbeni változásának a függvényében megvizsgáltuk a kapcsolók sorhosszát. A hívások számai a következők voltak: 1500, 7000 és 10000.

A 6. ábrán a kapcsolók sorainak az alakulását mutatjuk a hívási periódus alatt. Az ábra alapján képet alkothatunk a sorok nagyságrendjéről.



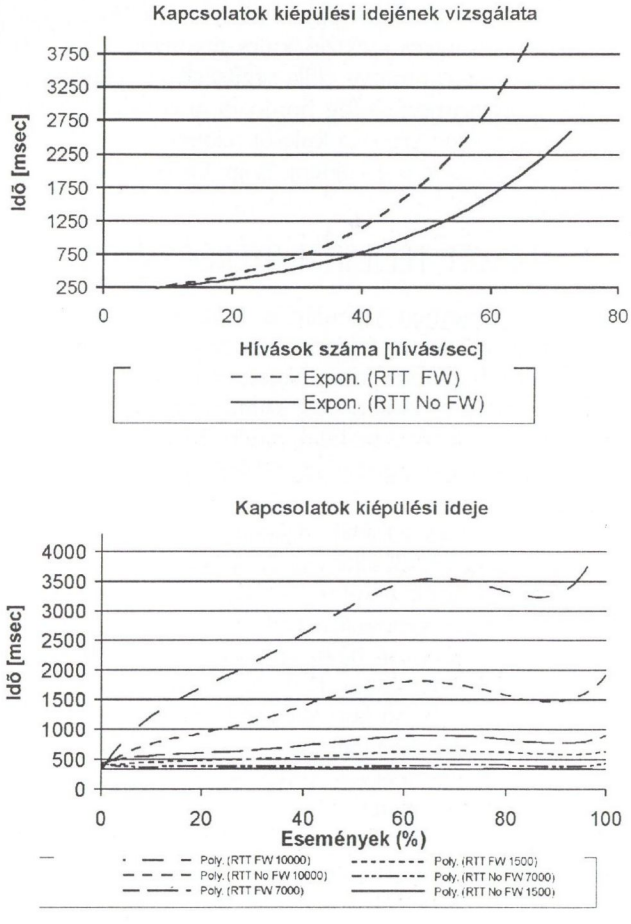
6. ábra. A sorok hosszának az alakulása az események lefolyása függvényében

Megállapíthatjuk, hogy a tűzfalakkal rendelkező hálózat gerinchálózati kapcsolóinak a sorai egészen 7000 hívásig (39 hívás/sec) nem szenvednek különösebben nagy változást. A 10000 hívásos (56 hívás/sec) esetben viszont a sorok terhelése jelentősen megno, de ebben az esetben már a tűzfalak nélküli hálózat is a blokkolási tartományban lesz.

5.2. A csatornák kiépülési idejének (Connection Time) vizsgálata

A módosított jelzésfolyamok a kapcsolatok kiépülési idejébe késleltetést visznek be, ugyanis több jelzési üzenet cserélődik ki a két tűzfal között mint a hagyományos esetben. Ebből az okból kifolyólag, a legrosszabb esetben az is előfordulhat, hogy a kapcsolat nem épül ki, mert a tűzfalak által védett hálózat egy kapcsolójának az időzítője lejár. A protokoll rendszerünk működő képessége vizsgálatának egy fontos kérdése, hogy a jelzések átlépik-e az időhatárt, amely letelte után felbomlik a kapcsolat. Ezt az időhatárt a T303-as és a T310-es [17] időzítők állítják be. A tűzfalnak a bejövő SETUP üzenet és az erre válaszolandó CONNECT üzenet között körülbelül 14 sec áll a rendelkezésére, hogy a másik tűzfallal felvegye a kapcsolatot. Ez az időhatár úgy érhető el, ha a bejövő SETUP üzenetre csak a 4 sec-os T303-as időzítő közvetlen lejárta előtt válaszol egy CALL PROCEEDING üzenettel. Így még marad 10 sec a T310-es időzítő lejártáig.

A szimulátor segítségével megvizsgáltuk, hogy a hálózat kapcsolat kiépítési idejét mennyire befolyásolja a tűzfalak jelenléte. A csatornák kiépülési idejét a tűzfalak nagyjából a kétszeresére növelték, az időhatárt a jelzések egyik esetben sem lépték át. A hívások blokkolt hálózat esetében is 4 sec alatt maradtak.



7. ábra. A kapcsolatok felépítési idejének a vizsgálata

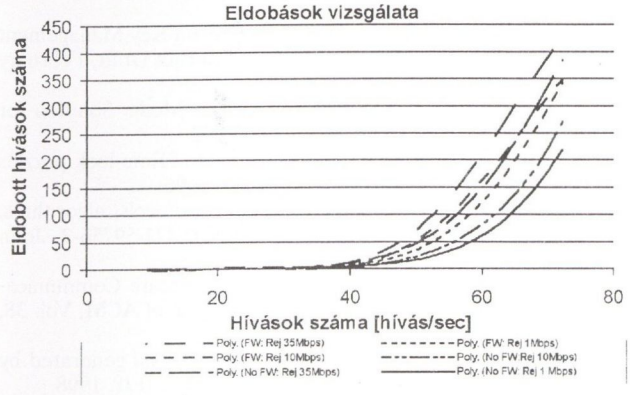
A kapcsolatok kiépülési idejét a 5.3.1-es részben leírt hálózatok és paraméterek használatával vizsgáltuk. Megállapíthatjuk, hogy akárcsak a sorok vizsgálata esetén, itt is a 10000 hívás esetén kezdett a kiépülési idő drasztikusan különbözni a két hálózat között.

5.3. Az eldobott hívások számának vizsgálata

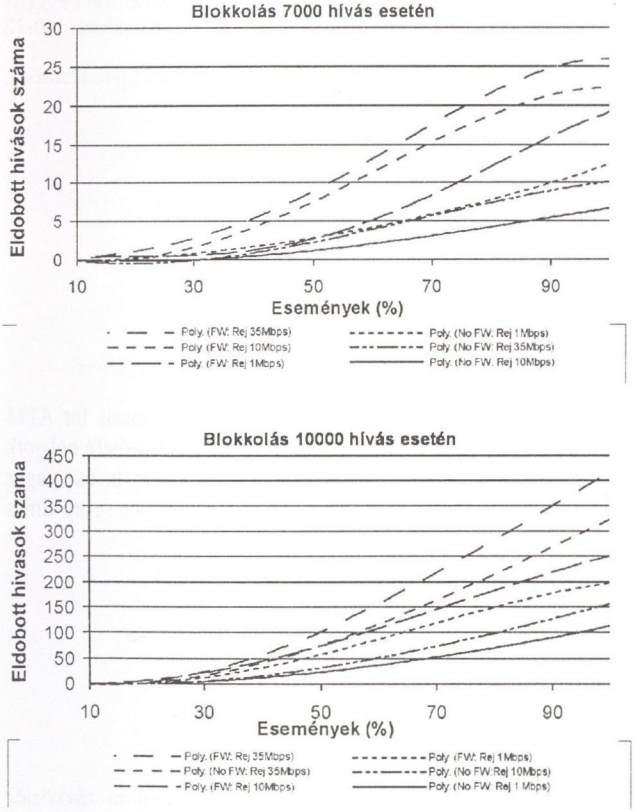
Esetünkben az eldobott hívások a sávszélesség hiány miatt következhetnek be. A sávszélesség hiány bekövetkezését a tűzfalak által bevitt sávszélesség növelés is előidézheti. Megállapíthatjuk, hogy a hálózat blokkolása 45

hívás/sec-nál kezdodik és a hívások eldobása az események számának függvényében exponenciálisan nő (8. ábra), ez megegyezik az 5. és 6. ábrákon tapasztaltakkal.

Annak ellenére, hogy a 35 Mbps-os hívásokból van a legkevesebb ezekbol lesz a legtöbb eldobva a hálózat telítődésénél. Ennek az oka, hogy ezek a hívások igényelnek a legnagyobb sávszélességet és a blokkolás kezdete után a hálózat ezt a kérést már nem tudja kielégíteni.



8. ábra. A hívások eldobásának a vizsgálata



9. ábra. A hívások eldobása különböző jelzés mennyiségek esetén

Megállapíthatjuk, hogy a tűzfalak által bevitt sávszélesség növelés nem terhelte le túlságosan a hálózatot mivel a hívás eldobások megfelelnek az előzoekben meghatározott értékeknek.

Ha a tűzfalak plusz sávszélesség igénye terhelő lett volna akkor az eldobások száma jóval meredekebben nőtt volna mint a 9. ábrán bemutatott esetben.

5.4. A szimulációk általános értékelése

A szimulációk során először a hálózatnak a jelzésfeldolgozási kapacitásával kapcsolatos paramétereit vizsgáltuk meg. A sorok hossza és a csatornák kiépülési ideje a jelzési terhelés mértékétol függ. A szimulációk során először ezeket tanulmányoztuk. Esetünkben a hívások eldobása a sávszélesség hiány és a hívásfelépítésre engedélyezett maximális idő túllépése miatt következhet be. A hívások eldobását a fejezet utolsó részében vizsgáltuk meg.

Megállapíthatjuk, hogy a blokkolás és a sorhossz együtt változik, ugyanis mindkét görbe ugyanabban a pontban kezd el jelentősen növekedni. A két esemény egybeesik, ezért a jelzésfeldolgozás csökkenése már a sávszélesség hiány által létrehozott blokkolási zónában történik. Ebből azt a következtetést vonhatjuk le, hogy az ATM kapcsolókat a tűzfalak által generált többlet jelzési forgalom nem terheli le számottevoen.

A blokkoláshoz közeli állapotban mindkét hálózatban a sorhossznál és a kapcsolatok felépítési idejénél megfigyelhető, hogy a görbe sokkal meredekebben kezd növekedni mint a normális esetben. Ez a növekedés azért következik be, mert a hálózat jelzési üzenet feldolgozási kapacitása kisebb mint a hívások érkezési intenzitása. Ez is azt jelzi, hogy a hálózat túl van terhelve. A hálózat 45 hívás/sec-nál kezd a blokkolási zónába jutni, ez megfelel a mért adatoknak.

Napjaink kereskedelmi kapcsolói véges hosszúságú sorokkal rendelkeznek, sorai hossza átlagosan 20 és 100 közötti jelzést tud tárolni [GDC, Fore]. Ennek alapján egy valós hálózat is blokkolódni fog 45 hívás/sec-on felül. A tűzfalakat tartalmazó hálózat nem terheli le túlságosan a fizikai kapcsolókat sem, mivel 45 hívás/sec-ig nem fog ugrásszerű jelzés mennyiséget generálni.

A szimulációs eredmények összességükben azt mutatják, hogy a tűzfalak által generált jelzési forgalom-többlet a tűzfal nélküli hálózat paraméterei ismeretében könnyen kiszámítható és ellenorizhető. Ily módon a tűzfalak telepítésével nemcsak rugalmas védelmi lehetőségeket nyerünk, hanem a nyilvános szolgáltató képes lesz megtervezni az eredeti szolgáltatásai minoségének változatlan szinten tartásához szükséges beruházások mértékét is.

6. ÖSSZEFOGLALÁS

Az általunk ajánlott protokoll lehetővé teszi egy olyan adatvédelmi rendszer kiépítését, amelyhez nem szükséges a jelenleg használatban lévo hálózati egységek protokolljainak a módosítása. Mivel mi is adatcsatornát használunk a tűzfalak közti kapcsolattartásra, ezért a protokollunk leginkább a Stevenson [14] és az ATM Forum [1] ajánlásaihoz hasonlítható. Az általunk kidolgozott protokoll ezekkel a protokollokkal szemben számos előnnyel rendelkezik.

Lehetővé teszi a tűzfalak közötti automatikus felderítést, jelentősen egyszerűsítve a rendszergazda feladatát a tűzfal konfigurálásánál. A Stevenson-féle protokoll ajánlattal szemben, ahol csak az adatok titkosítása lehetséges, a mi rendszerünk lehetővé teszi a felhasználói adatok integritásvédelmét is. Ennek az a jelentősége, hogy megakadályozza a támadót abban, hogy hamis adatokat csempésszen be a felhasználói adatok közé. Ezenkívül lehetővé válik az adatvédelmi paraméterek újraegyeztetése és a szesszió

kulcsok cseréje, amelyek szintén nem lehetségesek a Stevenson modellnél.

Az ATM Forum segédcsatornát használó módszere egymagában kevesebb szolgáltatást nyújt mint a mi protokollunk. Nem támogatja a felderítő típusú jelzések használatát, ráadásul a felhasználói adatok leblokkolásával jelentős késleltetéseket és adatvesztést okozhat. Ezenkívül az adatvédelmi paraméterek újraegyeztetéséhez és a kulcscserékhez speciális OAM cellákat kell használni, ezek használata viszont a jelenlegi protokollok megváltoztatását igényli. Az ATM Forum az integritásvédelmet csak a végpontok között biztosítja, tehát minden egyes integritásvédelmet óhajtó felhasználó végberendezésének a protokolljait meg kell változtatni.

IRODALOMJEGYZÉK

[1] ATM Forum Security Working Group, (Draft), "Phase I Security Specification", BTD-SECURITY 01.04, September 1997.

[2] Housley R., Ford W., Polk W., Solo D., "Internet Public Key Infrastructure X.509 Certificate and CRL Profile", PKIX Working group, Internet Draft, March 25, 1998.

[3] ATM Forum Technical Committee "Integrated Local Management Interface (ILMI) Specification Version 4.0" af-ilmi-0065.000, September 1996.

[4] Harkins D., Carrel D., "The Internet Key Exchange (IKE)", IPSEC Working Group, Internet Draft, March 1998.

[5] Laurent M., Rolin P., Stoffel L., "Security mechanism within control plane", Contribution ATM Forum/97-0040, February 1997, San Diego, California.

[6] Laurent M., Paul O., Rolin P., "Securing Communications over ATM networks", IFIPSEC'97, Copenhagen, Denmark, May 1997.

[7] Peyravian M., "A Certification Infrastructure for ATM", ATM Forum, 1995.

[8] Peyravian M., "A Framework for Authenticated Key Distribution in ATM Networks", ATM Forum, 1995.

[9] Peyravian M., "ATM security scope and requirements", ATM Forum, 1995.

[10] Karn P., Simpson W. A., "Photuris: Session Key Management Protocol" Network Working Group, Internet Draft, February 1998.

[11] Prycker de M., "Asynchronous Transfer Mode. Solution for Broadband ISDN.", Ellis Horwood, 1992.

[12] Rivest R. L., Shamir A., and Wagner D., "Time-lock puzzles and timed-release Crypto", March 10, 1996.

[13] Schneider B., "Applied cryptography: protocols, algorithms, and source code in C" Volume ISBN 0-471-59756-2, John Wiley & Sons, 1994.

[14] Stevenson D., Hillery N. and Byrd B., "Secure Communications in ATM Networks", Communications of ACM, Vol. 38, No. 2, February 1995, pp. 45-52.

[15] Székely S., Moldován I., Simon Cs., "Overload generated by signalling message flows in ATM networks", IFIP, 1998.

[16] S. Székely, Cs. Simon, G. Szűcs: "Performance Analysis of Switched Virtual Connections in ATM Networks", To be presented at: IFIP WG 6.4 Conference "Sixth IFIP Workshop on Reformance Modelling and Evaluation of ATM Networks", IFIP ATM'98, Ilkley, United Kingdom, 20-22 July 1998

[17] ATM Forum, "ATM User-Network Interface Specification", version 3.1, 1994.

ATM DATA SECURITY SYSTEMS

A. TÖRÖK, L. FISCHER, CS. SIMON

HIGH SPEED NETWORKS LABORATORY, DEPT. OF TELECOMMUNICATIONS AND TELEMATICS, TECHNICAL UNIVERSITY OF BUDAPEST

This paper describes a proposal for a protocoll system for an ATM firewall. At first we present some of the current proposals for ATM security in the literature and after this we present our method. The method proposed allows data integrity check in the intermediate network components, too. The other advantage of our protocol system is that it makes the configuration of the security proxys easier. In our paper we have validated our model through simulations. We examined the changes in the queue lengths of the switches, the connection setup times and the variations in the number of the rejected calls.

Simon Csaba 1987-ben a Temesvári Műszaki Egyetemen szerzett mérnöki oklevelet a Villamosmérnöki karon. Jelenleg a Budapesti Műszaki Egyetem Távközlési és Telematikai Karán a HSN-Lab keretén belül Ph.D. hallgató. Kutatási tevékenysége során az ATM hálózatok teljesítmény-vizsgálatával, valamint ATM hálózatok multicast és adatvédelmi protokolljainak megvalósításával foglalkozott.

Török Attila jelenleg a Temesvári Műszaki Egyetem távközlési karának ötödik évfolyamos hallgatója. Érdeklődési területei a nagysebességű hálózatok, kriptográfia, programozható hálózatok. A Budapesti Műszaki Egyetemen 1998-ban rendezett TDK konferencián a Hálózatmenedzselés szakon I. helyezést ért el. A közeljövőben szeretne felvételizni doktorandusz hallgatónak a BME-re.

Fischer Lajos jelenleg a Temesvári Műszaki Egyetem távközlési karának ötödik évfolyamos hallgatója. Érdeklődési területei: számítógépes hálózatok, mobil távközlés. A Budapesti Műszaki Egyetemen 1998-ban rendezett TDK konferencián a Hálózatmenedzselés szakon I. helyezést ért el. A diplomadolgozat megvédése után egy távközlési cégnél szeretne elhelyezkedni.

E-LEVÉL FELOLVASÓ

ZAINKÓ CSABA, NÉMETH GÉZA, BOGÁR BALÁZS, SZENDRÉNYI ZSOLT

BUDAPESTI MŰSZAKI EGYETEM
VILLAMOSMÉRNÖKI ÉS INFORMATIKAI KAR, TÁVKÖZLÉS ÉS TELEMATIKA TANSZÉK
1111 BUDAPEST, PÁZMÁNY PÉTER SÉTÁNY 1/D

Az elektronikus levelezőrendszer használata egy jobban napi életünk részévé válik, és egyre fontosabb, hogy rendszeresen nyomon tudjuk kísérni postafiókunk forgalmát. Hálózatra kötött számítógép használata esetén a feladat nem jelent komoly problémát, de ha állandóan mozgásban vagyunk, akkor más megoldásra is szükség van. Ilyen telefonos szolgáltatás például az e-levél felolvasó, amely segítségével bárhonnan, telefonon keresztül meghallgathatjuk, hogy kitől milyen levél érkezett. A leveleinket a rendszer olvasható formába alakítja át, amelyet a tanszéken fejlesztett szöveg-beszéd átalakító felolvas a telefonba. A digitális telefonkészülék nyomógombjai segítségével navigálhatunk a menürendszerben, kiválasztva a felajánlott funkciók közül az épp szükségeset. A tanszéken a felolvasó fejlesztése másfél éves múltra tekint vissza, Bogár Balázs és Szendrényi Zsolt már végzett hallgatókkal együtt készítettük el a demo rendszert, melynek szolgáltatásait a tanszéken található AT&T Definity alközponton keresztül lehet használni. Bogár Balázs a hálózati kapcsolatokat és az adminisztrációs részt, Szendrényi Zsolt a telefonos csatolót fejlesztette, én, Zainkó Csaba pedig a levélfeldolgozást és értelmezést készítettem.

A magyar elektronikus levelek legfőbb problémája, hogy az emberek többsége nem használ ékezetes betűket, mert a levelező rendszere nem ad rá lehetőséget, vagy a régen megszokott angol 26 betűs abc-re szorítkozik. A képernyőt olvasva az emberi agy pótolja a hiányosságokat, de felolvasás esetén a hallott szöveget már nem képes átalakítani, ezt a gépi intelligenciának kell megoldania, ékezetesíteni kell a beérkezett leveleket. Az elektronikus levelek átalakítása során a mondathatárok megállapítása, a levelek szabad stílusa miatt nem egyszerű feladat. A mondatvégi írásjelek nem mindig jelentik a mondat végét, sokszor rövidítéseket jelölnek, vagy internetes címek részét képezik. A levelek értelmezésénél a szöveg nyelvének megállapítására is szükség van, a különböző nyelvű részeket az adott nyelven kell megszólaltatni.

1. BEVEZETÉS

Mai világunkban a kommunikáció és az adatáramlás egyre fontosabb szerepet tölt be az ember mindennapi életében. Régen a papír alapú információáramlás volt a jellemző, de az idő előrehaladtával egyre inkább a papír nélküli, elektronikus adatcsere irányába mozdul el a világ. A személyes találkozások helyett a telefonos konferenciák, videó konferenciák kerülnek előtérbe, míg a hagyományos posta helyett, az elektronikus levelek használata terjed el.

Az elektronikus levelezőrendszer használata egyre jobban napi életünk részévé válik, és egyre fontosabb, hogy rendszeresen nyomon tudjuk kísérni postafiókunk forgalmát. Hálózatra kötött számítógép használata esetén a feladat nem jelent komoly problémát, de ha állandóan mozgásban vagyunk, akkor más megoldásra is szükség van.

Ilyen telefonos szolgáltatás például az e-levél[2] felolvasó, mely segítségével bárhonnan, telefonon keresztül meghallgathatjuk, hogy kitől milyen levél érkezett. A leveleinket a rendszer olvasható formába alakítja át, melyet a tanszéken fejlesztett szöveg–beszéd átalakító felolvas a telefonba. A digitális telefonkészülék nyomógombjai segítségével navigálhatunk a menürendszerben, kiválasztva a felajánlott funkciók közül az épp szükségeset.

A távközlés és a számítástechnika ilyen jellegű összefonódását Integrált Számítógépes Távközlésnek (CTI – Computer Telephony Integration) nevezzük, amely manapság egyre jobban elterjed a világon. A telefonos e-levél felolvasó nemzetközi szinten is még viszonylag gyerekcipőben jár, még nem tisztázódott, hogyan is kell egy ilyen rendszert tökéletesen megvalósítani.

A BME Távközlési és Telematikai tanszéken a felolvasó fejlesztése másfél éves múltra tekint vissza, Bogár Balázs és Szendrényi Zsolt már végzett hallgatókkal és Németh Géza konzulenssel segítségével készítettük el a demo rendszert, melynek szolgáltatásai a tanszéken található AT&T Definity alközponton keresztül érhetők el. Bogár Balázs a hálózati, és adminisztrációs részt, Szendrényi Zsolt a telefonos csatolót fejlesztette, én, Zainkó Csaba pedig a levélfeldolgozást és az értelmezést készítettem el.

A demo használata néhány helyen rámutatott arra is, hogy a kezdeti elképzeléseim nem voltak helytállóak. Ebben a tanulmányban már ezen tapasztalatokat is figyelembe vettem. Mivel a fejlesztés csapatmunkában történt, ezért nemcsak a saját munkámat írtam le, hanem a teljes rendszer megértéséhez, a csapat többi tagjának munkáit is röviden összefoglaltam. Ahol mások munkáit elemzem ott azt külön jelöltem, ilyenek például a következő fejezetek: 4.4., 4.5., 4.6. fejezetek, továbbá vannak olyan fejezetek amelyeknél nem tulajdoníthatók egyikünk önálló fejlesztésének sem, ilyen például az 4.1. fejezet és a 4.2. fejezet.

2. FEJLESZTÉSI CÉLOK

2.1. Mottó

„Az e-levelek telefonon keresztül történő elérése, kiegészítő hardverek nélkül, szöveg–beszéd átalakító segítségével"

Az elektronikus levelek elolvasására az emberek túlnyomó többsége valamilyen levelezőprogramot használ, Novelles környezetben Pmail-t, Unixos környezetben Pine-t, de egyre jobban elterjednek az internetes böngészőkkel egybeépített alkalmazások is. Ezeknek a programoknak közös tulajdonsága az, hogy a számítógép monitorán jele-

[1] A felolvasó fejlesztése projekt keretében folyik, amelynek szűk fejlesztői a fent felsoroltak. Munkájuk eredményeinek egy részét is leírom jelen tanulmányban, hogy a teljes rendszer összefüggéseiben is látható legyen.

[2] Az e-levél az elektronikus levél rövidítése, az angol e-mail magyar megfelelője.

nítik meg a levelek tartalomjegyzékét, vagy a kívánt levél belső tartalmát. A legnagyobb megkötés ilyen esetekben az, hogy csak számítógép mellett ülve lehetséges a használatuk és mivel egy ilyen alkalmazás nagy mennyiségű beállítási paraméterrel rendelkezik, nehezen hordozhatóak egyik gépről a másikra.

Ez a megkötés úgy oldható fel, hogy a leveleket telefonon keresztül érheti el a felhasználó, tehát bárhol a világon a nyilvános telefonhálózatot igénybe véve hozzáférhet a leveleihez. Ezt a megoldást használják sok helyen az internet és a levelek eléréséhez sok helyen, de ehhez költséges hardverekre van szükség, otthoni számítógépre, laptopra, modemre és az ezeket irányító programokra, melyek sok helyen nem biztosítottak.

Nekünk az a célunk, hogy csak a világ minden táján megtalálható egyszerű analóg[3] készülékek segítségével, emberi beszéd segítségével lehessen „elolvasni" azaz meghallgatni a leveleket.

A rendszer teljesen automatizált működésű, nem valós személy végezné a felolvasást, hanem a tanszéken fejlesztett gépi szöveg–beszéd átalakító.

2.2. Felhasználók köre

A fejlesztés indulásakor a cél az volt, hogy a vakok és csökkent látóképességű embereket segítő alkalmazást fejlesszünk, de már a legelső lépések megtételekor világossá vált, hogy ez a rendszer sokkal szélesebb rétegek kiszolgálására is alkalmas lehet. A nyitás nem jelentett hátrányt a vakok igényei szempontjából, mert a felhasználó mindenképpen telefonon érintkezik a rendszerrel, és a telefonkészülék funkcióit korlátozás nélkül képesek használni a vakok.

Ez a rendszer nem a hagyományos e-levél kezelő rendszereket kívánja helyettesíteni, hanem kiegészíteni azokkal a lehetőségekkel, amikkel ezek nem rendelkeznek. Ha valaki csak a munkahelyen tud hozzáférni a leveleihez – mert például otthon nincs számítógépe vagy internetes csatlakozása –, akkor az e-levél felolvasó segítségével az esti órákban, vagy a hétvégén is képes nyomon követni elektronikus postafiókjának forgalmát.

Folyton mozgásban lévő üzletemberek számára akár nélkülözhetetlen is lehet ez a szolgáltatás, hisz ha elutazik, például egy szállodában körülményes lehet internetes csatlakozást találni, ehelyett könnyedén, a minden szobában megtalálható telefonkészülék segítségével meghallgathatja a sürgős leveleit. Autóban utazva, vezetés közben szinte nem is nyílik más mód arra, hogy leveleiről információhoz jusson, fontos üzeneteit meghallgassa.

Ha valaki levelet vár, és nem akarja, vagy nem tudja folyamatosan a számítógépes levelezőrendszerével nyomon követni a beérkező leveleket, akkor telefonon keresztül egyszerűbben és gyorsabban megteheti ezt.

2.3. Elméleti korlátok

A rendszer csak kiegészíteni tudja a hagyományos levélkezelőket, a telefonrendszer és a hallás útján átvitt információk tulajdonsága miatt.

- *Hosszú szövegállományok:* Az ember a látására sokkal nagyobb mértékben hagyatkozik[4], mint a hallására, látás útján sokkal gyorsabban és több információt képes befogadni, mint hallás útján. Több oldalas szöveget nagyon sok ideig tart felolvasni, nincs értelme végigvárni.[5]
- *Kép, programok:* A felolvasás nem alkalmas ilyen jellegű állományok leírására.
- *A rendszer által nem támogatott idegen nyelvű szöveg:* Ha a szöveget nem a saját nyelve szerint olvassák fel, akkor nehezen vagy egyáltalán nem érthető lesz a beszéd.
- *A rendszer által nem támogatott formátumú szöveg:* Egyre növekszik a szövegszerkesztők száma a számítástechnikai piacon, és ezzel együtt a szöveg tárolásánál használt eljárások száma is, továbbá néhány nemzet igen speciális karakterkészletet használ.

2.4. Hasonló alkalmazások a világon

Hasonló magyar nyelven működő szolgáltatásról nem tudok, kutatásaim során nem találkoztam hazánkban ilyen alkalmazással.

Külföldön, főleg angol nyelvterületen már léteznek ilyen alkalmazások, de a számuk még meglehetősen alacsony. Kutatásaim során a „legkiforrottabb" benyomást a PhoneSoft [12] vállalat terméke tette, mely már kereskedelmi forgalomban van és az alapcsomag ára 2990 dollár[6].

Ezek mellett még sok kisebb cég is foglalkozik Amerikában ilyen jellegű szoftverek írásával, de ezek már nem olyan színvonalúak, a Net-savvy [13] e-mail reader-e már jóval kevesebb szolgáltatást nyújtott, csak a legalapvetőbb funkciókat tartalmazta.

Az athéni műszaki egyetemen is foglalkoznak ilyen jellegű rendszer felépítésével, ún. „Speech Agent"-et [9] fejlesztettek, ahol a menü kezelését beszéd felismeréssel oldották meg, és a hangsúlyt a beszéddel végzett irányításra helyezték.

3. RENDSZER FELÉPÍTÉSE

3.1. Működés menete

1. A felhasználó a nyilvános telefonhálózaton keresztül képes elérni a szolgáltatást, a megfelelő számot tárcsázva az alkalmazás a lehető leghamarabb felveszi a telefont. A „megfelelő szám" kifejezés azért fontos, mert egy többcsatornás telefonkezelő kártya használata esetén, előfordulhat, hogy több szolgáltatást is nyújt egyetlen gép, vagy ugyanazt a szolgáltatást, de más formában. Az e-levél felolvasóval kapcsolatban arra gondolok, hogy más-más számon különböző nyelvű rendszer érhető el, tehát már a kezdeti bejelentkező szöveg is a kívánt nyelven szólalna meg (1. ábra).
2. Az üdvözlés és a felhasználó azonosítása után a rendszer már tudja, hogy „kivel áll szemben" és ez alapján változtathatja meg a működésének paramétereit. (Ezekkel a paraméterekkel a későbbiek során még részletesen foglalkozom a 3.3.3. fejezetben.)

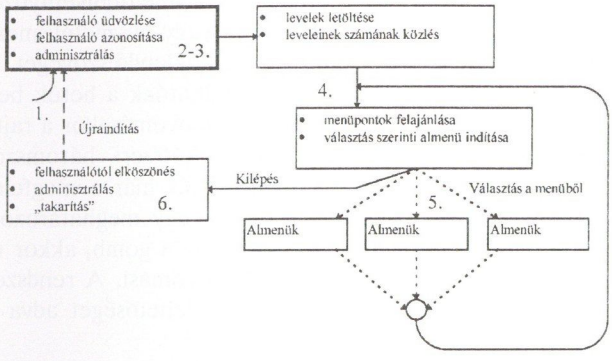
[3] Hagyományos, beszédsávú átvitelt biztosító telefonkészülék.

[4] Átlag ember nem használja ki a hallás adta lehetőségeket. Erre bizonyíték, hogy a vakok az átlag ember számára szinte érthetetlen hadarást is gond nélkül megértik.

[5] Teszteredmény: 2 kbyte-os magyar szöveget (kb. 30 sor), 3,5 perces szintetizált beszéddé alakítja át a felolvasó.

[6] 2990 dollár 1998 októberi árfolyamon kb. 650 eFt-nak felel meg.

3. A rendszer a felhasználó cselekvéseit letárolja, hogy az esetleges visszaélések felderítését segítse.
4. A rendszer letölti a megfelelő leveleket a szerverről és feldolgozza a tartalomjegyzék elkészítéséhez. Ezalatt a felhasználóval közli leveleinek számát, és megkéri, hogy a felsorolt menüből válassza ki a kívánt funkciót.
5. A program mindig felajánlja a lehetséges választási lehetőséget és a rendszer bármely pontján kérhet a felhasználó segítséget a rendszer kezeléséhez. A levelek tartalomjegyzékét, tartalmát meg lehet hallgatni, illetve egyéb szolgáltatásokat igénybe lehet venni (3.2. fejezet).
6. Kilépéskor a rendszer minden olyan felesleges információt, adat- és hang-fájlt töröl, amire már nincs szükség, helytakarékossági és adatvédelmi szempontból.



1. ábra. A működés menete

3.2. Menürendszer és funkciók

A menürendszer a főmenüből és az almenükből áll, illetve ún. rejtett menükből. A főmenük egyes funkciók választása után újabb menükbe juthatunk el, ezek az almenük. Rejtett menüről akkor beszélünk, ha a felhasználónak úgy kell a funkciók közül választania, hogy a lehetőségeket előzetesen nem ajánlja fel a rendszer. Ilyenek lehetnek például a hallgatás közbeni funkciók, amikor egy levél hallgatása közben, nem olvassa fel a rendszer, hogy milyen gomb segítségével mit tudok elérni, mégis például egy sort előre vagy hátra ugorhatok a felolvasásban.

3.2.1. Főmenü

Főmenü az a menü, amellyel a felhasználó az azonosítás után találkozik. A menüben a legalapvetőbb funkciók találhatóak meg, amit szinte minden esetben használhat az ember.

Elérhető funkciók:

- **Tartalomjegyzék:** A felhasználó ezzel a funkcióval a levelek tartalomjegyzékét hallgathatja meg (3.2.2.fejezet).
- **Összes levelek meghallgatása:** Itt a leveleket egymás után, megszakítás nélkül lehet meghallgatni (3.2.4. fejezet).
- **Kijelölt levelek elfaxolása:** Vannak olyan levelek amelyek fontosak lehetnek, vagy túl hosszúak ahhoz, hogy meghallgassuk őket, ilyenkor egy megadott telefonszámra küldi el a rendszer a kiválasztott levél fakszimiléjét.
- **Felhasználó beállításai:** Ebben a menüpontban a felhasználó úgy tudja paraméterezni a meghallgatás menetét, ahogyan a számára a legbarátságosabb, a legkönnyebben használható, és amely a legjobb szövegértést teszi lehetővé. Itt módosíthatja a rendszer igénybevételéhez használt tikos kódot is. Ebben a menüpontban olyan paraméterek módosítására van lehetőség, amit a telefonkészülék gombjai segítségével meg lehet adni, tehát vagy szám információról van szó, vagy valamiféle választási lehetőségekről. Olyan adatokat, melyek neveket, mondatokat, tehát karakteres információkat tartalmaznak, csak nagyon körülményesen lehet megadni.
- **Felhasználó észrevételei:** A felhasználó észrevételeit a rendszer az üzenetrögzítőhöz hasonlóan eltárolja a szolgáltatást fejlesztők és üzemeltetők részére. Az üzenet hosszát korlátozni kell, megakadályozva a rendszer túlterhelését (Tárterülettel való gazdálkodás).
- **Segítség:** Segítségkérés minden esetben lehetséges, tartalmazza az egyes választási lehetőségek hatásainak leírását, mit mire tud használni.
- **Kilépés:** A főmenüből lehetséges kilépni a teljes rendszerből, a program az elköszönés után a vonalat megszakítja, és vár a következő beérkező hívásra.

3.2.2. Tartalomjegyzék menü

Ebben az almenüben a levelek tartalomjegyzéke hallható, a levél feladóját, a tárgyát és a feladás dátumát közli a rendszer. Azt, hogy a felhasználónak milyen sorrendben olvassa be a rendszer a levelek tartalomjegyzékét, az a felhasználó egyéni beállításától függ, alapértelmezett az, hogy a legrégebben érkezett levéltől a legújabb felé halad.

Használható funkciók:

- **Egy tartalomjegyzék bejegyzéssel előre/hátra:** A felhasználó ezzel a lehetőséggel gyorsabban megtalálhatja azt a levelet, amit keres, nem szükséges minden egyes bejegyzést végighallgatnia. Lehetősége van egy-egy bejegyzés átugrására, de akár több, például 5 bejegyzés kihagyására is. Erre akkor lehet szükség, ha ritkán olvassa valaki a leveit, vagy rövid idő alatt sok üzenete érkezik.
- **Mondat újrahallgatása:** Ha az elhangzott mondatot nem, vagy nem pontosan értette, akkor ezzel a funkcióval újra, ismételten meghallgathatja az elhangzott mondat elejétől kezdve.
- **Adott levél teljes tartalmának meghallgatása:** Ha a tartalomjegyzék alapján a felhasználót érdekli a levél belső tartalma is, akkor ezt a funkciót választva az egy levél meghallgatása menübe jut, ahol a rendszer felolvassa a kívánt levelet.
- **Adott levél faxolásra való kijelölése:** A főmenüben található faxolási funkcióhoz szükséges kijelölést végzi, az éppen aktuális levelet bejegyzi az elfaxolandók listájára.
- **A levél törlése:** Lehetőség van a tartalomjegyzékből, illetve a postafiókból a levél törlésére. Ennek a funkciónak a működése sokban függ attól, hogy a felhasználó milyen típusú szerveren tárolja a rendszerét, pontosabban megfogalmazva, milyen protokoll segítségével lehet elérni a leveleit. (A levélletöltési protokollok különbségeiről a 3.4.1. fejezetben olvashat.)
- **Válaszlevél küldése:** A levelekre korlátozott mértékben reagálni lehet. Sok esetben előfordul, hogy az ember nem kíván hosszú válaszlevelet írni, szinte csak az olvasás tényét akarja a levél feladójával közölni. A válaszadás is egy almenü használatával lehetséges (3.2.6. fejezet).

- **Visszalépés a főmenübe:** Ha valaki nem akarja végighallgatni az összes bejegyzést, akkor lehetősége van visszaugrani a főmenübe, amit a rendszer automatikusan is megtesz, ha már az összes tartalomjegyzék bejegyzést felolvasta.
- **Segítségkérés:** A felhasználó bármelyik menüben kérhet segítséget, az aktuálisan elérhető szolgáltatásokról.

3.2.3. Egy levél meghallgatása menü

Egy adott levél meghallgatása úgy kezdődik – hasonlóan a tartalomjegyzék bejegyzésekhez –, hogy a feladó, a feladás időpontja és a levél tárgya hangzik el először, majd az üzenet elejétől a végéig mondatonként olvassa fel a program.

Használható funkciók:

- **Egy mondattal előre/hátra:** Természetesen a teljes levél tartalmát nem kell végighallgatni a felhasználónak, ha a levél végére kíváncsi, ezzel a funkcióval kihagyhat mondatot, illetve visszafelé ugorhat a szövegben.
- **Öt mondattal előre/hátra:** Hosszabb levek esetén szükség lehet a nagyobb mértékű ugrásra is.
- **Mondat megismétlése:** Ha a mondat nem volt tisztán érthető, vagy egy fontos információt újra kíván hallgatni valaki, akkor ezt is megteheti.
- **Válaszlevél küldése:** Ezzel ugyanazt az almenüt lehet elérni, ami a tartalomjegyzék menüben is szerepel, tehát egy rövid válaszlevelet lehet generálni.
- **Adott levél faxolásra való kijelölése:** A levelet itt is kijelölhetjük arra, hogy a tartalmát elfaxolja a főmenüben megadható számra.
- **Vissza az előző szintre:** Ezzel abba a menübe juthatunk vissza ahonnan ebbe a menübe beléptünk.
- **Segítség:** Hasonlóan a többi menühöz, itt is segítséget nyújt a rendszer.
- **Kilépés:** Visszatérés az előző menübe

3.2.4. Összes levél meghallgatása menü

Itt a tartalomjegyzékkel szemben, nem csak a levél legfontosabb jellemzőit ismerhetjük meg, hanem az levelek teljes terjedelmét felolvassa a rendszer.

- **Egy levél előre/hátra:** A levelek hallgatása közben a levelek között ugrálhatunk előre, illetve hátra.

A menürendszer további funkciói megegyeznek az egy levél meghallgatása menü lehetőségeivel.

3.2.5. Fax menü

Ebben a menüben a faxolással kapcsolatos adatokat lehet megadni. A felhasználó által kiválasztott leveleket a megadott paraméterekkel faxolja el a program. Az adatok megadása után a rendszer ellenőrzés céljából visszaolvassa a beállított értékeket és lehetőséget ad azok módosítására.

- **Cél telefonszám változtatása:** Itt lehet megadni azt a telefonszámot, amit a faxolásnál a gép használni fog.
- **Fax minőségének változtatása:** Választani lehet a normál és a finom felbontású faxok között.
- **Fax elküldésének időpontja:** Azonnal vagy késeltetve.
- **Fax küldésnek megerősítése:** Beállított értékek felolvasása után a felhasználó dönt az adatok helyességéről és vagy elküldi a faxot, vagy visszatér a menübe további módosítások megtétele érdekében.
- **Segítség:** Útmutató a faxoláshoz, és a számlázás menetéről.
- **Kilépés:** Visszatérés az előző menübe.

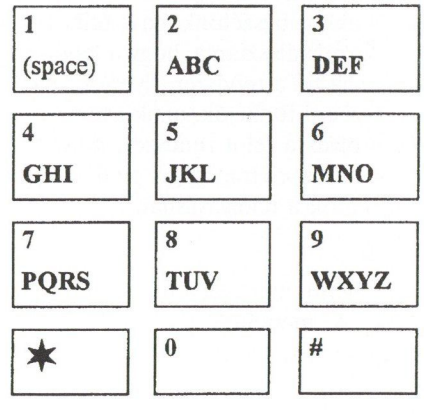
3.2.6. Válaszlevél menü

Itt előre eltárolt tartalmú leveleket lehet elküldeni, melyet a felhasználó a regisztráció során megadott.

Funkciók:

- **Válaszlevél az előre letároltak közül:** A előre megírt sorszámozott válaszlevelek közül ki lehet választani a megfelelőt, és azt a feladó részére elküldeni. Fontos, hogy minden válaszlevél tartalmazza, hogy a levél automatikusan generált, mivel valószínűleg a felhasználó nem tud a megszokott hosszúságú és minőségű levelet írni, ami félreértésekhez vezethet.
- **Válaszlevél írása:** Itt a felhasználó a telefonbillentyűzet segítségével írhatja meg a levelet, vagy beszédfelismerő esetén betűnként adhatja meg a elküldendő szöveget.
  A telefonbillentyűzetek[7] felhasználhatóak a betűk beírásához (2. ábra). A billentyű első lenyomásakor a rajta lévő számot kell értelmezni, de a kétszeri, háromszori vagy négyszeri ismételt megnyomás már a megfelelő betűt jelenti. Természetesen, ha egy meghatározott időn belül nincs megnyomva ugyanaz a gomb, akkor új betűnek kell venni a következő lenyomást. A rendszer minden detektált betűt visszaolvas, lehetőséget adva a javításra.
  Példa: 12 ORA begépelése (2. ábra).

1	2	(space)	O	R	A
1	2	1-1	6-6-6-6	7-7-7-7	2-2



2. ábra. Telefonkészülék-billentyűzet

- **Válaszlevél visszahallgatása:** A megalkotott levél meghallgatása.
- **Válaszlevél küldése:** A megalkotott levél elküldése.
- **Segítség:** Segítség a válaszlevél elkészítéséhez.
- **Kilépés:** Visszatérés az előző menübe.

[7] Néhány nagyobb készülékgyártó (Panasonic, GE, Motorola, Benefon, Ericsson) újabb telefonjait megvizsgáltam, és azokon szerepelnek a számokhoz tartozó betűk, inkább a régebbi készülékeknél merülhetnek fel problémák.

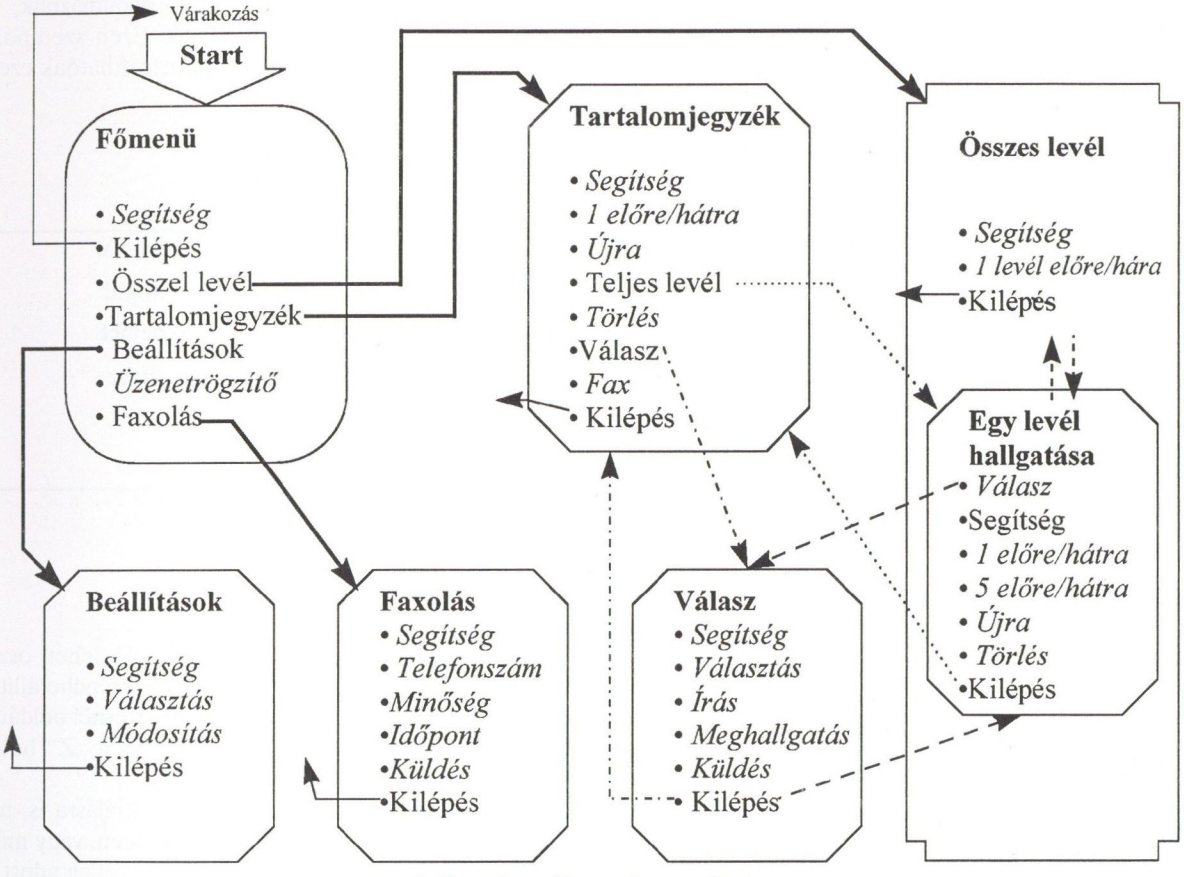
3.2.7. Beállítások menü

A 3.3. fejezetben felsorolt adatok közül azoknak a módosítása van lehetőség, melyeket telefonon keresztül viszonylag könnyen megadhat a felhasználó, ilyen például az új titkos azonosítója.

- **Paraméter választás:** A felhasználó rendelkezik egy listával, melyben fel van tüntetve, hogy melyik paraméter milyen sorszámú. A sorszámot beütve megtudhatja a paraméter aktuális beállítását.
- **Paraméter módosítás:** A kiválasztott paraméter értékének módosítása.
- **Segítség:** Segítség a beállításokhoz, a paraméterek sorszámának listáját felolvassa a rendszer, arra az esetre, ha a felhasználó nem rendelkezne ezzel.
- **Kilépés:** Visszatérés az főmenübe.

3.2.8. Menük összefoglalása

Az 3. ábrán látható a menük viszonya egymáshoz. A lekerekített téglalap a főmenü, a belőle kiinduló vastag vonalak pedig az innen választható almenükre mutat. A téglalapokban a menün belül végrehajtódó funkciók dőltbetűkkel vannak írva, az újabb menüt generálók pedig normál álló betűkkel. A lecsapott sarkú téglalapok az almenük, és a szögletes sarkú pedig egy olyan menü, ami tartalmaz egy másik menüt is.



3. ábra. A menük egymáshoz való viszonya

3.3. Felhasználók nyilvántartása

3.3.1. Regisztráció

Minden felhasználót regisztrálni kell a legelső belépés előtt, a működéshez szükség van a legfontosabb adatokra. Itt nem személyes jellegű adatokról van elsősorban szó, hanem a felhasználó postafiókját kezelő szerverre való belépést lehetővé tévő információkról. A legfontosabb adatok, melyek nélkül a felolvasás nem lehetséges (1. táblázat).

3.3.2. Azonosítás

Minden egyes telefonhívás beérkezése után a felhasználó azonosítására van szükség, mert a rendszer ez alapján képes a megfelelő postafiók tartalmának letöltésére, továbbá így biztosítja a felhasználó leveleinek védelmét.

Azonosító: 4 jegyű 10-es számrendszerbeli szám. Az azonosító minden esetben négyjegyű, tehát a 18-as számú azonosító helyett 0018 létezik csak.

Titkos kód: felépítés teljesen megegyezik az azonosítóéval, szintén egy négyjegyű szám.

Az azonosító és a titkos kód hossza változtatható, igazán megkötést csak a telefonkészülék felülete jelent, mert a digitális készülékeken összesen 12 db olyan nyomógomb található, amelyhez DTMF[8] hangot rendeltek és ezek közül is a „* " és a „#" szimbólumok kitüntettet feladatot szoktak ellátni. Bár a DTMF még rendelkezik az A, B, C, D szimbólumokkal is, de ezek szinte egyetlen telefonon sem találhatóak meg, általában csak speciális eszközök ismerik (pl. modem).

[8] Dual Tone Multiple Frequency: A nyomógombok lenyomása esetén 2 db különböző frekvenciájú hang keletkezik, melyet a vevőoldalon egyértelműen fel lehet ismerni. 2x4 db frekvencián 16 db szimbólumot kódolnak.

1. táblázat

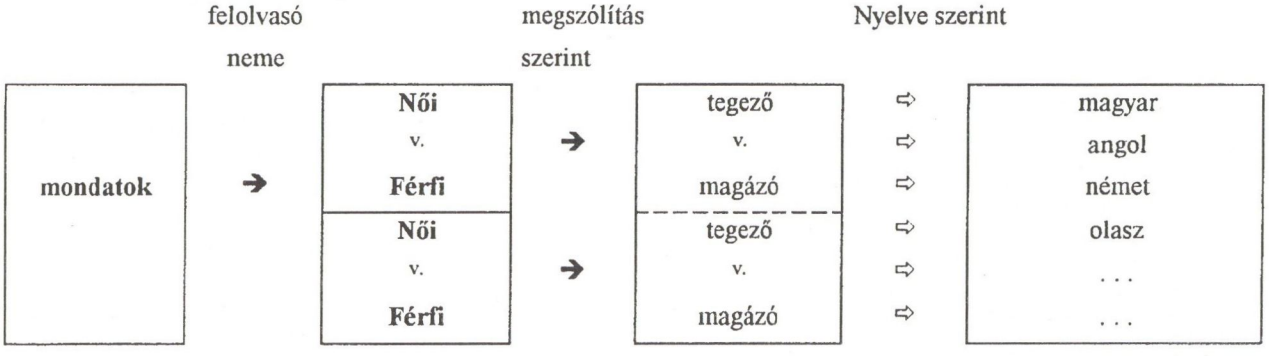
Szükséges információ	Célja	Megjegyzés
Felhasználó neve	azonosítás	
Postafiókját kezelő szerver neve	levelek elérése	
Postafiók elérésének módja	levelek elérése	Unix, Novell, ill. POP IMAP, FTP protokoll
Szerveren használt login neve	levelek elérése	
Login névhez tartozó titkos neve	levelek elérése	Mindenképpen szükséges
Azonosító belépés	felolvasóba	A rendszer generálja regisztrációkor
Azonosítóhoz tartozó titkos kód	felolvasóba belépés	
Renszerben használt neve	érthetőség	Elsőleges nyelv a magyar

3.3.3. Felhasználóhoz tartozó paraméterek

Az ember–gép kapcsolat minőségét lehet javítani, ha az alkalmazás lehetőséget nyújt személyes jellegű beállítások használatára. Vannak olyan paraméterek, amik nem változtathatóak, de ezek mellett sok olyan paraméter található, melyek nem jelentenek lényegi változást az alkalmazásban, de a felhasználó számára kellemesebbé tehető a felolvasó.

Előre felvett üzenetek:

Fontos paraméter a rendszernek, hogy a köszöntő, segítő üzenetek milyen nyelven, milyen stílusban vannak felvéve. Szöveg nyelvén azt értem, hogy a szöveget mely nemzet anyanyelvén olvasták fel, a stíluson pedig azt, hogy a mondatokban magázó vagy tegező formát alkalmaznak, vagy az, hogy női vagy férfi hang hallható. Ezen szempontok szerint tehát a következőképpen csoportosíthatóak ezek az üzenetek (4. ábra).



4. ábra. Mondatok felosztása

Hallgatás közben generált üzenetek:

A szöveg–beszéd átalakító által generált beszédnek a következő paramétereivel lehet variálni. A szintetizálás

- alapfrekvenciája,
- sebessége,
- az artikuláció mértéke.

állítható. Az alapfrekvenciával növelve, a szintetizált szöveg egyre jobban elnőiesedik, de a telefonon keresztül hallgatva csökken az érthetősége. Sebességet növelve csökkenthető a lejátszás ideje, de ez is az érthetőség rovására mehet. Az artikuláció paraméter változtatásával állítható be, hogy a szintetizátor mennyire erősen artikulálja a hangokat, vagy akár ki is lehet kapcsolni.

Menürendszer:

Menürendszer változtatására korlátozott mértékben van lehetőség, hozzáadni a menüpontokhoz nem lehetséges, csak arra van mód, hogy egyes választási lehetőségeket le lehessen tiltani, például ha valaki nem rendelkezik fax készülékkel, nincs szükséges erre a menüpontra tehát a rendszer ne ajánlja fel részére ezt a szolgáltatást.

Tartalomjegyzék és levél meghallgatás:

Tartalomjegyzék hallgatásakor fontos lehet, hogy a leveleket a kívánt sorrendben hallgassa meg az ember.

Rendezési elvek a következőek lehetnek:

- rendezés nélkül (a megérkezés időpontja szerint),
- a feladás időpontja szerint,
- a feladó személye szerint,
- a levél tárgya szerint.

Az előbb felsorolt elveket még kétfelé lehet osztani aszerint, hogy növekvő illetve csökkenő sorrendbe állítsa a program. A feladó személye szerinti rendezésnél például az „A" betűvel kezdődő szerepeljen elől, vagy a „Z" betűvel kezdődő.

Lehetősége van a felhasználónak szelektálásra is, tehát megadhatja, hogy milyen dátumtól kezdődően, vagy milyen tárgyú leveleket kíván csak megtekinteni, esetleg adott tárgyú, vagy adott helyről érkezett leveleket pedig egyáltalán nem kíván meghallgatni. Olyan opciót is választhat a felhasználó a dátum szerinti szelekciónál, hogy csak azokat a leveleket olvassa fel az e-levél felolvasó, melyek az utolsó meghallgatás után érkeztek.

Ezeket a beállítási lehetőségeket természetesen nem csak a tartalomjegyzékre vonatkozik, hanem az összes levél meghallgatása menüben is hasonló szelekció lehetséges.

A rendezésen túl, olyan állítási lehetőségek is vannak, melyek segítségével a tartalomjegyzék mondatát a sajátos igények szerint lehet formálni. Meg lehet határozni a levél feladója, tárgya és a feladás időpontja sorrendjét, esetleg azt, hogy melyiket hagyja ki ezek közül, illetve az egyes információk formátumát. Legjobban a feladás időpontjával lehet variálni, az év, hónap, nap információkat sok fajta képen lehet felolvasni. Például a dátum legyen 1998. november 6.

1998 november 6. „Ezerkilencszázkilencvennyolc november hatodika."
98 november 6. „Kilencvennyolc november hatodika."
98 10 6 „Kilencvennyolc tizedik hó hat."
november 6. „November hat."

Évet csak akkor lehet elhagyni, ha így is egyértelmű az információ, tehát a levél egy évnél fiatalabb. Ez szerencsére szinte minden esetben így van.

Faxolással kapcsolatos beállítások:

- **Kívánt cél megadása:** A cél a telefonszám, melyre a faxot küldeni kell. A faxolással kapcsolatban már felmerül a számlázás kérdése is, mivel ekkor az e-levél felolvasó kezdeményezi a hívást, tehát a telefonszolgáltató az ő részére számlázza ki a hívás költségét. A fizetési konstrukciók rengetegébe nem kívánok belemenni, ez inkább közgazdasági jellegű probléma.
- **Fax minősége:** G3 osztályú faxok[9] lehetőséget kínálnak arra, hogy két fajta felbontásban lehessen képet átvinni [14] (2. táblázat).

2. táblázat.

G3 faxok jellemzői[10]	Függőleges felbontás	Vízszintes felbontás
„normál"	3,85 vonal/mm	8 vonal/mm
„finom"	7,7 vonal/mm	8 vonal/mm

Finom felbontású fax küldése tovább tart de egyenletesebb minőséget, jobb olvashatóságot biztosít. Egy A4-es oldalnyi szöveg átvitele tartalmától függően 40-60 másodperc ideig tart, tehát inkább nagyobb levelek küldése esetén lényeges a felbontás okozta időnövekedés.

- **Fax küldése azonnal vagy később:** Azonnali küldés akkor valósítható meg, ha a felhasználónak külön vonalon van a faxkészüléke, mert ekkor párhuzamosan a hallgatással el lehet küldeni a faxot. Ez előnyös abból a szempontból, hogy ha valami probléma támad, vagy a levél tartalma alapján még más levél is érdekli, akkor azt azonnal meg tudja hallgatni, nem szükséges utólag újra felhívnia a szolgáltatást. Ha a faxkészüléket ugyanarra a vonalra kötve használja a telefonáló, akkor az e-levél felolvasó csak azután kezdi el a fax elküldését, miután a felhasználó letette a telefonkészüléke kagylóját. Itt lehetőség van a késletetés beállítására, ha a felhasználó számára hosszabb időt vesz igénybe a telefonról a fax vételére való átállás.

3.4. Hálózatkezelés

3.4.1. Távoli postafiókok elérésének módjai

Legelterjedtebb a POP és az IMAP protokoll használata, de ezen kívül még más módon is el lehet érni a leveleket, például FTP segítségével [11], [7].

POP (Post Office Protocol): Ez egy régi, de még sok helyen használatos protokoll, melynek az a lényege, hogy a postafiók tartalmáról másolatot lehet készíteni, és ezek után beállítástól függően a szerver gép vagy törli az ottani kópiát, vagy változatlanul hagyja. Hátránya az, hogy több helyről való hozzáférés támogatása minimális, tehát ha az egyik helyre a leveleket már úgy töltötte le, hogy a szerver a leveleket törölte, akkor máshová ez már nem lehetséges. Továbbá az is probléma, hogy letöltéskor a teljes tartalmat le kell hozni, és ez akkor komoly gondot jelenthet, ha a postafiókunkba nagyméretű üzenet érkezett, például egy 2 Mbyte-os audió fájl.

FTP (File Transfer Protocol): Ez egy univerzális protokoll, nem kifejezetten levelek letöltésére alkották meg, hanem ahogy a nevében is benne van fájlok átvitelére használható. Az, hogy mégis erre használható, az azért van, mert az esetek döntő többségében egyetlen fájlban tárolják a teljes postafiókunk tartalmát, és így ezt lemásolva rendelkezésre állnak a leveleink. Hátrányai hasonlóak mint a POP protokollé, itt is le kell minden levelet tölteni tartalmától, méretétől függetlenül.

IMAP (Internet Message Access Protocol): Ez a protokoll három működési módot támogat, a legelső lényegében megegyezik a POP működésével (*offline* üzemmód). *Online* üzemmód esetén a levelek a szerver gépen maradnak, a levélről információk kérdezhetőek le, de nem szükséges a teljes tartalmat letölteni, csak akkor, ha szükségünk van rá. További előnye, hogy a leveleket egyesével is elérhetjük, nem szükséges az összeshez egyszerre hozzányúlnunk. Harmadik működési mód a disconnected, ahol a postafiók tartalmáról első lépésként egy másolat készül a helyi gépre, majd a szerver–gép kapcsolatot bontják. A módosítások után ismét felveszik a kapcsolatot a gépek, és szinkronizálják a tükörmásolatot az eredetivel.

A levelek letöltését a lehető leghamarabb meg kell kezdeni, mert ha FTP-t, POP-ot használunk akkor ez a művelet igen időigényes is lehet. Más esetekben is előfordulhat hosszabb várakozás, ha például a hálózat vagy a szerver számítógép túlterhelt.

3.4.2. Regisztráció és információ

A regisztrációt interneten keresztül érdemes végrehajtani, mert így egyrészt nem igényel emberi beavatkozást, továbbá az adatok helyessége is ellenőrizhető. A rendszer működése szempontjából a postafiók elérhetőségének biztosítása igen lényeges, tehát szükséges, hogy tesztelve legyen ez, az adatok alapján. Ehhez egy olyan gép szükséges, amely web-es szolgáltatást képes nyújtani, tehát egy http-szerver funkciót tud ellátni.

A regisztráció folyamán a beírt adatokat formailag is ellenőrizni kell, tehát az e-levél címnek tartalmazni kell egy darab „@" karaktert és legalább egy darab pontot is. Azért, hogy az első használatkor se legyen gondja a felhasználónak, fontos, hogy a beírt adatok helyességét úgy is ellenőrizze a regisztrációt végző gép, hogy ún. próbaletöltést végez, tehát a beírt adatok alapján a leveleket tartalmazó szerverről megpróbálja letölteni az éppen aktuális leveleket, vagy legalább azt megvizsgálni, hogy az adott szerver létezik, és hogy azon a szerveren olyan nevű felhasználó létezik. Ha sikertelen az ellenőrzés, akkor két eshetőség állhat fent. Vagy a felhasználó adott meg rossz adatokat, vagy pillanatnyilag nem érhető el az a szerver, amin a levelek tárolva vannak. Ilyen esetben az adatok helyesbítése után újra kell próbálkozni, vagy ha a felhasználó nem változtat a beállításokon, akkor valószínűleg csak átmeneti kiesésről van szó.

[9] A G3 csoport tartozó készülékek általában kompatibilisek az alacsonyabb osztályú készülékekkel, de G2-, G1-es csoportú készülékekkel szinte már nem is lehet találkozni.

[10] Gyakorlatilag a 200x100 dpi-s és a 200x200 dpi-s felbontásnak felelnek meg ezek az adatok.

Regisztráció után a felhasználó részére egy levelet kell küldeni, amelyből a használathoz szükséges információkat ismét közli a rendszer.

Levélnek mindenképpen tartalmaznia kell:

- a felhasználó azonosítóját;
- a szolgáltatás telefonszámát;
- a gond esetén hova fordulhat;
- a kezelési útmutató elérési helyét.

A felolvasóhoz tartoznia kell egy részletes, írott kezelési útmutatónak, melyet célszerűen hálózaton elérhető formában kell tárolni, és ennek kézenfekvő megoldása az, hogy a regisztrációt végző gépre html formátumban kell elhelyezni, továbbá biztosítani kell egy egyszerű letöltési lehetőséget (tömörített formátumban a teljes leírás).

3.5. Levél- és szövegfeldolgozó

Ennek a részegységnek az a feladata, hogy a postaládában található karakterfolyamból egy „emberi fogyasztásra" alkalmas szöveget állítson elő.

3.5.1. Az elektronikus levélről röviden

Az elektronikus levél két nagy részre osztható fel, a borítékra és az üzenetre.

A borítékot szokták még fejrésznek „header"-nek nevezni. Itt a hagyományos levélhez hasonlóan azok az információk találhatóak meg, melyek a kézbesítéshez, rendszerezéshez szükségesek. A boríték úgynevezett mezőkből (field-ekből) áll. Minden mező elején a mező neve, kettőspont és a mező tartalma áll. Ezek azért fontosak a számunkra, mert ilyen mezőkben találhatóak azok az információk is, amelyekre szükség van a tartalomjegyzék készítéséhez és a tényleges üzenet értékeléséhez [5].

Legfontosabb mezők:

- **From:** A levél feladójának címe, esetleg a neve.
- **Subject:** A levél tárgya.
- **Date:** A feladás dátuma.

A tartalomjegyzék készítéséhez ezek az információk már elegendőek, de a szöveg értelmezéséhez többre van szükség.

- **Content-Type:** Itt arról kaphatunk információt, hogy a levél tartalma milyen jellegű üzenet, milyen karakterkészletet használ [4], [6].

A boríték végét egyetlen üres sor jelzi, onnan kezdve a levél teste, maga a tényleges üzenet található. Ez az üzenet sokfajta lehet, szövege, grafika, kép, hanganyag, program vagy ezekek tetszőleges kombinációja.

3.5.2. Levél feldolgozása

A levél feldolgozása abból áll, hogy a szerverről letöltött fájlból a levelek tartalmát és az azonosításukhoz szükséges információkat kinyerje. A levél fejlécéből ki kell hámozni azokat az információkat, amelyek a tartalomjegyzék készítéséhez szükségesek. Ezt a következő módon lehet megtenni. (Itt nem a pontos algoritmust írom le, azt a gyakorlati fejtem ki.)

Feladó: A feladót a *From* azonosítójú mezőből lehet megtudni. Ezzel az a legnagyobb probléma, hogy a feladó neve és az email cím együtt szerepelnek ebben a mezőben, de az is előfordulhat, hogy csak az email cím van megadva és ilyenkor nem is ismerhetjük a feladót.

Dátum[11]: A feladás dátuma a Date kulcsszóval jelzett mezőből derül ki. Ez egy szabványos formában megadott dátum, mely másodperc pontosan megadja az elküldés időpontját. Az időpont megállapításánál az időzónákra kell nagy figyelmet fordítani, mert két azonos dátum még nem jelenti ugyanazt az időpontot, ha más időzónából érkezett a levél. A felhasználó számára mindig a helyi idő szerinti dátum érdekes, minden dátumot erre kell átalakítani.

Tárgy: A levél tárgya a *Subject* mezőben található meg, ezen csak minimális konverziót kell végrehajtani. Speciális karaktereket nem lehet használni a levél fejrészében, ez Magyarországon különösen gondot okoz az ékezetes betűk gyakorisága miatt. Ezt úgy oldották meg, hogy a egy kitüntetett karakter segítségével (=) meg lehet adni a kívánt kódkészletet, a kódolási eljárás típusát, és utána a karakterkódjával lehet hivatkozni az adott speciális betűre:

Példa: március $\Longrightarrow$ =?iso-8859-2?Q?m=**E1**rcius?=

Ez egy iso 8859-2 karakterkészlet szerinti kódolás ahol az E1 az „á" betű hexadecimális kódja [3].

Üzenet: A fejrész után található az üzenet test, melynek kódolása a fejrészből derül ki. A *Content-Type* mezőből megállapítható, hogy mi az üzenet típusa és ha szöveg akkor milyen kódolással, milyen karakterkészlettel lett írva.

Néhány lehetséges típus átalakítása:

- **Application:** Alkalmazások (programok) átalakítása nem lehetséges, rövid üzenettel kell helyettesíteni, melyből a felhasználó számára kiderül, hogy milyen nevű, hosszúságú alkalmazást kapott.
- **Audio:** Ha ismert formátumú fájl, akkor a felhasználónak le kell játszani.
- **Image, video:** nem lehetséges az átalakítása.
- **Multipart:** többrészes dokumentum, amit szét kell bontani, tehát külön-külön kell az egyes részeket vizsgálni.
- **Text:** különböző karakterkészlet esetén konverzió szükséges.

3.5.3. Szöveg feldolgozása

Szöveg feldolgozásán azt értem, amikor egy egybefüggő szöveget értelmes mondatokká szedünk szét. Erre azért van szükség, mert a szöveg—beszéd átalakítók mondatokat képesek befogadni, a mondatvégi írásjelekből tudják megállapítani a mondat típusát.

Első lépésben meg kell állapítani a szöveg nyelvét, mely például az egyes nemzetek szavainak előfordulásának vizsgálatával, vagy bizonyos alapvető szabályszerűségek figyelésével lehetséges. Ilyenek lehetnek a „th" kapcsolatok gyakorisága, mely az angol nyelvre utal, vagy az „(" és az „sch" betűk, melyek a németre, és a sok „e" betűs szavak, mely a magyar nyelvű szöveget valószínűsítik. Jellegzetesem nyelvünkben a kettős betűk is (sz, zs, gy, ny, ...), melyek nemigen találhatók meg más nyelvben. Van amikor olyan a levél, hogy a szöveg nem egységes, különböző nyelvű mondatok váltogatják egymást, ilyenkor mondat szinten kell dönteni a nyelvről.

Mondathatárok:

Mondathatárok megállapítása első ránézésre viszonylag egyszerűnek tűnik, de a levelek rövid vizsgálata után is már tisztán látni, hogy ebben a esetben nem lesz könnyű dolga

[11] A dátum itt, nemcsak az évet, hónapot, napot, hanem az órát, percet, másodpercet is jelent.

a programnak, mert a magyar nyelvben léteznek olyan jelek, melyek több funkcióval is bírnak.

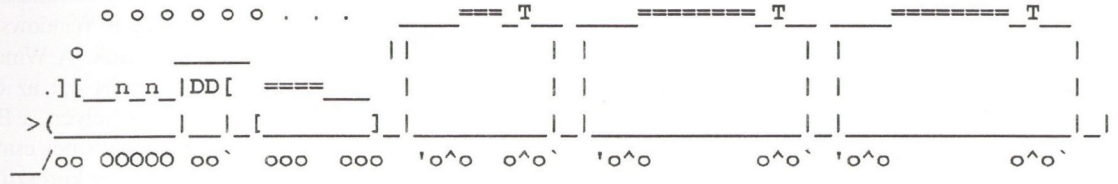
Írásjelek: Mondathatárokat a „ . ! ? ” jelek jelölik, de ezeket nem csak erre a feladatra használjuk, ezért tisztán a pont megléte alapján nem dönthetünk.

Internet címek: Ezekben a címekben több pontot is találhatunk, amelyek félrevezetik az olyan algoritmusokat melyek csak a „ . ” karaktert keresik.

Rövidítések: Rövidítések végén mindig pont szerepel, amit szintén figyelmen kívül kell hagyni a mondathatár keresésénél.

Karakterrajzok: az elektronikus levelekben a levél írója sokszor olyan rajzokat készít, melyek a számítógép szempontjából szövegnek számítanak, de valójában csak a képernyőn megjelenítve tartalmaznak információt. Ezeket felolvasva olyan „zagyvaságot” kapunk, melynek valódi értelmét senki sem tudja felfogni hallás után.

Az előbb felsoroltakat figyelembe véve még mindig gond lehet az, hogy az elektronikus leveleket sokkal lazább stílusban írják a levelezők, mint más irományokat, tehát nem is biztos, hogy a mondat vége jelölve van. Ezt sajnos már igen nehéz észrevenni, mert ehhez már tartalmilag kéne vizsgálni a leveleket, ami még igen bonyolult feladatnak számít manapság.



5. ábra. Kivonat példa [7]

Kivétel szótárak:

Rövidítések vagy idegen szavak felolvasása sokszor nem érthető, ezeket a megfelelő alakjukkal kell helyettesíteni. Ezeket az ún. kivétel szótárban kell tárolni, amelyből minden benne szereplő rövidítéshez, idegen vagy jövevény szóhoz a megfelelő kiejtésű alakot lehet visszakeresni, és utána a felolvasáskor ezzel lehet helyettesíteni. Minden nyelvhez külön kell egy ilyen szótárat készíteni, hiszen az egyes szavak, rövidítések kiejtés más-más a különböző nyelveken.

Ékezetesítés:

Főleg magyar nyelvű elektronikus leveleknél gyakori az, hogy a feladó ékezetek nélkül adja fel a levelét és ezt felolvasva nehezen érthető beszédet kapunk. Ékezetesítést tehát a felolvasás előtt el kell végezni, mert hallás után már nehezen tudja agyunk az átalakítást elvégezni, ellenben azzal, hogyha az írott szöveget olvassuk, akkor az intelligenciánk úgymond „kirakja az ékezeteket” a magánhangzókra.

Ékezetesítés egy részét megoldhatjuk kivétel szótárak segítségével, melyek leginkább a gyakori tulajdonnevekre, keresztnevekre alkalmazhatóak hatékonyan (Tamas ⟶ Tamás). Másik módszer, hogy az adott szó összes ékezetes formáját megvizsgáljuk, és a magyar szövegben való előfordulásuk alapján döntünk. Ez a feladat hasonló a helyesírás ellenőrzés problémájához.

Betűzés:

Olyan magyar szavakat, melyek nem tartalmaznak magánhangzót, nem lehet kiejteni[12]. Ezeket a szavakat úgy lehet csak felolvasni, ha minden egyes betűt egyenként lebetűz a rendszer. Vannak speciális karakterek, amelyeknek nem felel meg hang a magyar nyelvben, ezeket is külön kell lebetűzni. Ide tartoznak azok a karakterek, amik nem betűk vagy számok és nem mondatban szereplő írásjelek. A „ . ” is ide tartozik abban az esetben, amikor nem mondatvéget vagy rövidítést jelöl. Például:

html	→	„há té em el”
kft	→	„ká ef té”

www.bme.hu	→	„vé vé vé pont bé em e pont hu”
10 %	→	„tíz százalék”

A betűzés során felmerül olyan probléma is, hogy az angol „at” (@) jelet, hogyan ejtsük ki magyarul, „at jel”-nek vagy az egyre jobban elterjedő „kukac”[13] kifejezést használjuk.

3.6. Telefonkezelő

A telefonkezelő alrendszer feladatai:

- a gépben található telefonos illesztőkártya menedzselése,
- a kimenő üzenetek lejátszása,
- a felhasználó azonosítása,
- a többi alrendszer értesítése,
- a menüpontokhoz tartozó előre felvett üzenetek lejátszása,
- a felhasználó által a telefonkészüléken megnyomott gomb detektálása,
- a szintetizált szövegek lejátszása,
- a vonal bontása.

Telefonkezelésnél nagyon fontos, hogy a rendszer realtime formában tudjon működni, mert a felhasználó megkívánja, hogy az utasításaira a rendszer azonnal reagáljon. A valós idejű működési módot az is szükségessé teszi, hogy a lejátszott üzenetek nem szakadhatnak meg, hiszen már legkisebb szünetet is észre lehet venni. Továbbá az is szükséges, hogy a felhasználó értesüljön arról, hogy a gombnyo-

[12] Talán erre az egyetlen kivétel az „s” kötőszó, melyet magánhangzó nélkül ejtünk.

[13] A média se talált más kifejezést az „@” jelre, a TV műsorokban is az elektronikus levél címeknél „kukac”-ot használnak.

mására a felolvasó reagált, tehát anélkül, hogy bármilyen cselekvést elindított volna a telefonkezelő, a felhasználó számára jeleznie kell, hogy „megértettem" az utasítást. Ezt úgy lehet elérni, hogy az aktuálisan lejátszott szöveget meg kell szakítani, és egy „köszönöm" üzenetet felolvasni, vagy egy rövid füttyel jelezni.

3.7. Felügyelet és vezérlés

A szolgáltatás üzemeltetőjének biztosítani kell, hogy bármikor lehetősége legyen a teljes folyamat áttekintésére. Biztosítani kell egy olyan konzolt, mely segítségével bármely vonal állapotát meg tudja vizsgálni, bele tud hallgatni, továbbá amivel a rendszer paramétereit tudja állítani.

A rendszer minden cselekvését rögzíteni, naplózni kell. Itt nem a levelek, a kimenő üzenetek tartalmára gondolok, hanem arra, hogy ki, mikor hívta fel a rendszert, sikeres volt-e a leveleinek letöltése, a felhasználó milyen menüket használt, és volt-e a rendszerben hiba. Olyan események bekövetkezésének a naplózására van szükség, melyek a fejlesztéshez, hibakereséshez nyújtanak segítséget.

Szükség van egy vezérlő rendszerre, ami koordinálja az egyes alrendszerek működését, indítja a szöveg, levél feldolgozását, a szöveg–beszéd átalakítót, a levélletöltőt és elküldi az adatokat a naplózó programnak. Ezt elosztottan is meg lehet oldani, amikor mindenki tudja, hogy az egyes események bekövetkezésekor kit kell indítani vagy értesíteni.

3.8. Szöveg-beszéd átalakító

Szöveg–beszéd átalakítónak az a feladata, hogy egy mondatot úgy átalakítson beszéddé, hogy az emberi fül számára kellemes legyen, tehát minél jobban hasonlítson a természetes beszédre. A beszédszintetizálás nagy számításigénnyel jár, ezért a programok ütemezésénél ezt figyelembe kell venni, továbbá az átalakítás időigényes volta miatt, a beszédet előre le kell generálni, mivel a felhasználó nem lenne hajlandó végigvárni az átalakítást, ha a program csak akkor kezdené el a működését, amikor már szükség lenne a kész hangfájlra.

4. MEGVALÓSÍTOTT RENDSZER

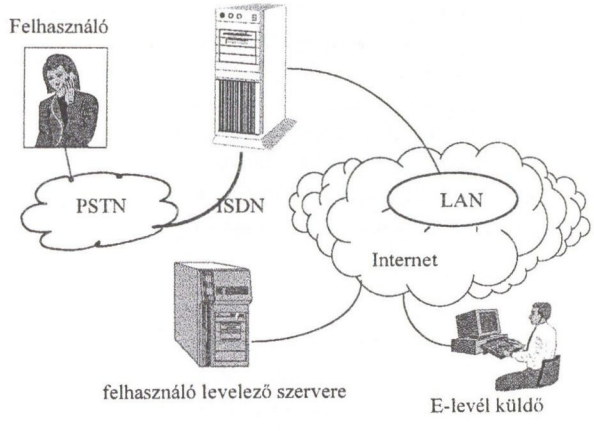
A rendszer megvalósításának a kezdetén világossá vált számunkra, hogy az összes funkciót, maximálisan nem tudjuk megvalósítani, mivel a fejlesztő csapatunk 3 főből[14] állt, és a rendelkezésre álló idő fél év volt. Elsődleges célnak azt tűztük ki, hogy egy olyan demo rendszert készítsünk el, mely az alapvető feladatokat képes végrehajtani, továbbá alkalmas arra, hogy külső felhasználók segítségével teszteltessük a rendszert. Erre azért van nagy szükség, mivel hazákban nincs még hasonló szolgáltatás, nem állnak rendelkezésre felhasználói tapasztalatok.

A demo megvalósítása során arra törekedtünk, hogy úgy alakítsuk ki az egyes alrendszereket, hogy alkalmasak legyenek a későbbi továbbfejlesztésre, lehetőség legyen újabb funkciók beillesztésére, a régiek lecserélésére. Ezt úgy kívántuk elérni, hogy a funkcionálisan különálló részeket külön programba implementáltuk, és minél jobban paraméterezhető alkalmazások készítésére törekedtünk.

[14] Bogár Balázs és Szendrenyi Zsolt már végzett hallgatók, akik diplomattervként foglalkoztak a fejlesztéssel és jómagam, aki mint önnálló laboros fejlesztettem az e-levél felolvasót.

4.1. Fizikai felépítés

Fejlesztési célnak tűztük ki azt is, hogy a teljes rendszer egyetlen PC legyen egvalósítva, úgy véltük, hogy a mai nagyteljesítményű számítógépek mellett egyetlen gép akár 4 telefonáló egyidejű kiszolgálására is alkalmas lehet. Operációs rendszerként egy olyanra volt szükségünk, ami alkalmas a programok párhuzamos futtatására, a programok közötti kommunikációra, megfelelő védelmet tud biztosítani a felhasználói adatok védelmére és ezek mellett még alkalmas arra, hogy hálózatba kötve, http szerver funkciót lásson el. A kiválasztott fejlesztő rendszerünk 32 bites Windows-os platformon fut, így a Windows 95-os és NT változata között kellett választanunk. A Windows NT-t sokkal megbízhatóbbnak ítéltük, ezért ezt az operációs rendszert telepítettük fel. A fejlesztés helyén, a Beszédkutatási Laboratóriumban adott volt a telefonos csatoló típusa, egy Dialogic kártya. Helyi hálózaton keresztül lehetőség volt az internet elérésére, tehát a web-es szolgáltatást meg lehetett oldani.



6. ábra. A rendszer struktúrája

4.2. Fejlesztési környezet

A kiválasztott hardver és szoftver környezet:

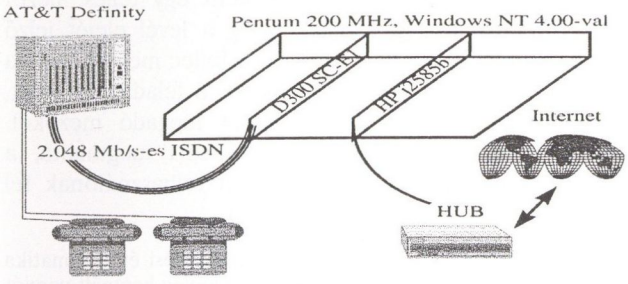
- Pentium 200 MHz MMX, 64 Mbyte memória, 2 Gbyte winchester;
- Dialogic D300SC-E1 telefonos illesztőkártya;
- HP LAN adapter J2585B típusú 100 Mb/s hálózati csatoló;
- MS Windows NT Workstation 4.0 – A PC operációs rendszere;
- MS Visual C++ 5.00 – Objektum-orientált fejlesztőrendszer;
- VOS 5.3 Development System – Telefonok kezelését végző fejlesztői rendszer;
- AT&T Definitiy telefonalközpont;
- 2 db analóg készülék, tesztelési célokra.

A PC-ben található Dialogic telefonos illesztőkártya egy 2 Mb/s-os ún. primer ISDN csatlakozáson keresztül állt összeköttetésben az egyetemi kísérleti telefonhálózat kapcsolóközpontjával, továbbá ugyanerre a telefonközpontra kötött analóg készülékek segítették a tesztelést.

A VOS fejlesztőrendszer a telefonos illesztőegység kezelésére alkalmas, az alapvető feladatok implementálását jól támogatja.

Helyi 100 Mb-es hálózat sávszélessége elegendően nagy ahhoz, hogy ezen a http szolgáltatás és a levelek letöltése egyidejűleg, gond nélkül megvalósítható legyen.

Kísérleti rendszerünk felépítése hasonlít a Dialogic ajánlásához, a megvalósítása a 7. ábrán látható [10].



7. ábra. Kísérleti rendszerünk

4.3. Alrendszerek együttműködése

Az egyes programok a rendszeren belül vagy fájlokon keresztül kommunikálnak, vagy üzeneteket küldenek egymásnak. Az üzenetek azért előnyösek mert rendkívül gyorsak, de viszont csak kevés adatot lehet átadni egyszerre.

Az egyes részek vezérlését nem központilag valósítottuk meg, hanem elosztva, egy esemény bekövetkezése esetén az adott alrendszer értesíti azokat programokat, melyeknek az esemény hatására cselekedniük kell.

A kapcsolatban álló programok közötti üzenetek felépítését a mellékletben található ábrán követhetjük nyomon.

4.4. Telefonkezelő[15]

4.4.1. Telefonos infrastruktúra kialakítása

Szendrényi Zsolt, Kovács Pál segítségével készítette el a telefonos rendszer felépítést, elvégezték a telefonközpont átprogramozását, mely lehetővé tette a Dialogic kártya használatát, továbbá felkonfigurálta az vezérlőt az ISDN protokoll használatához.

4.4.2. Sok-email-es telefonkezelő program

Ez az alkalmazás a következő feladatokat látja el [2]:

- a hívások fogadását, illetve bontását végzi el csatornánként;
- fenntartja a kapcsolatot a felhasználó és a rendszer egyéb elemei között;
- elvégzi a felhasználó azonosítását, a jelszó ellenőrzését;
- előre felvett szövegek lejátszásával menüket biztosít a felhasználónak;
- figyeli a megnyomott gombokat a menükben, és ettől függően végrehajtja az adott
- menüponthoz tartozó utasításokat;
- jelez a többi programnak a további teendőket illetően;
- lejátssza az adott hangfájlokat.

A program nyugalmi állapotban hívásra vár. A hívás megérkezése után, üdvözlő szöveget játszik le, és ellenőrzi a felhasználó azonosítóját. Ha az azonosítás sikeres, akkor elindítja az e-levél felolvasás folyamatát. A telefonáló a levelek meghallgatása után leteszi a kagylót, és a program elvégzi a kapcsolat bontását.

4.5. Hálózatkezelés[16]

4.5.1. EmailFTP

Ez a program FTP protokoll segítségével letölti a leveleket a felhasználó szerveréről, mely jelenleg Unixos vagy Novelles lehet. A program alaphelyzetben a telefonkezelő üzenetére vár, melyből megtudja, hogy hányas számú felhasználó jelentkezett be. Ekkor az illetőhöz tartozó – a regisztrációnál létrehozott – adatfájlból kiolvassa a levelek letöltéséhez szükséges adatokat (szerver neve, login név, jelszó, a leveleket tartalmazó könyvtár stb.). Ezek után a felhasználó nevében belép a szerverre, és egy előre meghatározott könyvtárba letölti a levelek nyers szövegét tartalmazó fáj(loka)t. Ha ez megtörtént akkor egy üzenetet küld a szöveg- és levélfeldolgozást irányító programnak, és ismét várakozó állapotba kerül [1].

4.5.2. GenWave

A GenWave végzi a mondatok hangfájllá alakítását. A MultMail által küldött üzenetekben megkapja, hogy melyik levél hányadik mondatát kell legeneráltatni, és milyen nevű wav-fájlt kell, hogy kapjunk. Ezután kiolvassa az adott mondatatot a MailToText által készített szövegből, beleírja egy ideiglenes fájlba, majd meghívja a Hun4w32 beszédszintetizátor programot a megfelelő paraméterekkel, amelyik legyártja a kívánt beszédet [1].

4.5.3. Consol

A rendszeradminisztrátor munkáját megkönnyítő felügyeleti és konfigurációs feladatokat lát el ez a program. Megjeleníti a képernyőn az egyes telefoncsatornákon végbemenő folyamatokat, mutatja a felhasználó által nyomott gombokat, illetve azt, hogy az egyes vonalakon éppen hányas számú és milyen hosszú hangfájl lejátszása történik. Lehetővé teszi, hogy a rendszergazda a számítógép hangszóróján meghallgathasson egy tetszőleges csatornán elhangzó wave-okat. Ez a funkció természetesen csak tesztelési célokat szolgál, nem a felhasználó üzeneteinek a lehallgatását. A Consol programból lehet végrehajtani a rendszerelemek konfigurációját, és innen is sor kerülhet egy felhasználó regisztrációjára, törlésére. A program segítségével az egyéb programok által készített nyomkövető adatbázisokból statisztikákat készíthetünk, mely alapján a felhasználók szokásait megismerve, fejleszthető tovább a rendszer [1].

4.5.4. Internetes regisztráció

A regisztráció a gépen található honlapról lehetséges, mely során a felhasználótól a szükséges információkat bekéri. A regisztráció csak a tanszék gépeiről lehetséges, hisz a kísérleti telefonhálózatot is csak innen lehet elérni, nincs értelme, hogy bárki bárhonnan bejelentkezhessen. A kapott információkat egy PERL nyelven írt program ellenőrzi, és egy próbaletöltést végez. Ha sikeres volt

[15] A megvalósítás részletes leírása az [1]-gyel jelölt diplomatervben található, itt csak annyit írok le a megvalósításból, amiből kiderül, hogy ezen a téren meddig jutottunk el.

[16] A megvalósítás részletes leírása az [2]-vel jelölt diplomatervben található, itt csak annyit írok le a megvalósításból amiből kiderül, hogy ezen a téren meddig jutottunk el.

a teszt akkor a felhasználó számára kiadja a rendszer használatához szükséges azonosítót [1].

4.6. Szöveg–beszéd átalakító

4.6.1. Hun4w32[17]

Ez a szöveg—beszéd átalakítást végző szintetizátor program. A Beszédkutatási Laborban kifejlesztett MULTIVOX beszédszintetizátorok legújabb 4.0 verziójának 32 bites változata. A parancssorból indítható konzolalkalmazásként működő program bemenete egy ISO 8859-2 karakterkészlettel írt szövegfájl, a kimenete egy wav-fájl. Az előállított beszéd hangerejét, sebességét, és a hangmagasságát egy konfigurációs fájlban lehet megadni [1].

4.7. Levélelemzés

4.7.1. Mail to Mail converter

A programnak az a feladata, hogy a letöltött levelek nyers formátumából a leveleket külön fájlokba szabdalja úgy, hogy közben az alapvető konverziókat elvégezze (fejrész értelmezése, karaktertábla egységesítése, időzónák konvertálása stb.). A FTP megoldás miatt egy olyan fájlt kap a program, melyben a leveleket egymástól egyetlen „from" szóval kezdődő sor választja el.

A feldolgozás menete:

A kapott üzenet alapján megnyitja fájlt. A program soronként olvassa be az input fájlt, illetve ha a levél fejlécét olvassa be, akkor egy sorként egy teljes mezőt olvas. Addig olvassa a sorokat amíg a levél elejét jelző from sort nem találja meg. Ezután a fejléc mezőit olvassa be és keresi a levét tárgyát, feladóját, a feladás dátumát, a dokumentum típusát és kódolását megadó mezőket. Amikor a fejléc végét jelentő üres sort megtalálta, a fejlécnek azon információit, melyet a felhasználónak fel kell olvasni, letárolja a kimeneti fájlba.

[17] Text-to-speech fejlesztés a BME Távközlési és Telematika tanszéken nagy múltra tekint vissza, és a jelenleg használt verziót Olaszi Péter alakította át a felolvasó igényei szerint.

a bemeneti fájl tartalma (xxxxmail)

.
.
From — Mon Sep 29 22:49:00 1997 **Itt kezdődik a levél**
Received: from localhost (vete@localhost [127.0.0.1])
by goliat.eik.bme.hu (8.8.7/8.8.7) with SMTP id NAA13363;
Mon, 29 Sep 1997 13:09:00 +0200 (MET DST)
Date: Mon, 29 Sep 1997 13:08:59 +0200 (MET DST) **Lényeges információ**
From: VESZELKA Tamas <vete@eik.bme.hu> **Lényeges információ**
To: Schuszter Miklos <schuszi@goliat.eik.bme.hu>,
ZAINKO Csaba <zai@goliat.eik.bme.hu>
Subject: sor **Lényeges információ** Message-ID: <Pine.GSO.3.96.970929130303.12234A-100000@goliat.eik.bme.hu>
MIME-Version: 1.0
Content-Type: TEXT/PLAIN; charset=US-ASCII **Lényeges információ**
X-UIDL: 2e679626849f9de2a471a49655091422
Status: RO
X-Status:
X-Mozilla-Status: 0001
Content-Length: 56

Fejléc vége, a test kezdete

Sziasztok,
Holnap talalkozunk!

Udv Tamas

From — **Itt kezdődik a következő levél, és vége van az előzőnek**
.
.

A fejléc információjából kiderül a karakterkészlet, és a kódolás fajtája. A levél testét majdnem változtatás nélkül kiírja a kimeneti fájlba, csak az esetleges karakterkonverziókat végzi el.

A kimeneti fájl: (xxxx_002.txt)

A harmadik levelet VESZELKA Tamas ku:ltte[18], szeptember huszonkilencedike'n, 13 o'ra 8 kor, melynek ta'rgya sor.
Sziasztok,
Holnap talalkozunk!

Udv Tamas

Miután a program az összes levélen végigment, legyárt egy report fájlt melyben az szerepel hogy hány levele van a felhasználónak. Ez lesz az a mondat amit a rendszer először felolvas a felhasználónak a leveli meghallgatása előtt.
report fájl: xxxx_999.mml

HUxxxA levelinek sza'ma, 24.
DExxxDie Anzahl der neuen Briefe, 24.

A HU betűk jelentik azt, hogy a mondat magyarul van, a DE pedig azt, hogy azt a mondatot német nyelven kell majd felolvasni. A kétbetűs nyelvjelzés után található három darab „x"-nek nincs funkciója, későbbi fejlesztések részére tartalékolt terület. A nyelvek jelölését az ISO 3166 nemzetközi szabványok alapján jelöli [8].

[18] A példában szereplő „kültte" (ku:ltte) nem helyesírási hiba, hanem így a kiejtés szerint írva, a felolvasás minősége javul.

4.7.2. Mail to Text converter

Működése:
Ez a program, az előző program által generált text fájlok feldolgozását végzi.

A program feladatai:
- mondathatárok megtalálása,
- nem felolvasható karakterek kiszűrése, átalakítása,
- magánhangzót nem tartalmazó szavak lebetűzése,
- ékezet nélküli levelek érthetőségének javítása ékezetesítéssel,
- kivételkezelés, idegen szavak átalakítása.

A mondat karakterenként olvassa be az input fájt és lépésről lépésre elemzi.

Elemzés során használt állapotok:
- a konverter mondatban van-e,
- a konverter szóban van-e,
- a konverter szünetben van-e,
- az aktuális karakter szám, betű, újsor, írásjel, nyomtatható vagy üres karakter-e,
- a következő karakter szám, betű, újsor, írásjel, nyomtatható vagy üres karakter-e.

Elemzés során használt szabályok:

Főszabályok:
- Mondat eleje: eddig nem mondatban volt, és szám vagy betű jött.
- Szó eleje: eddig nem szóban volt, és szám vagy betű jött.
- Szóban marad: szóban volt és betű vagy szám jött.
- Szó vége: szóban volt és nem betű és nem szám jött.
- Szünet eleje: eddig nem szóban volt és nem betű és nem szám jött. Szünetben marad: szünetben volt és nem betű és nem szám jött.
- Szünet vége: szünetben volt és betű vagy szám jött.
- Mondat vége: mondatban volt és írásjel jött.

Kivételek:
- Ha a fájl végére ért, akkor a szónak, szünetnek, és a mondatnak is vége van.
- Nincs vége a szónak, ha egyébként szó vége lenne, de a következő karakter nem szünet, nem írásjel, de nyomtatatható karakter.
- Nem kezdődik a szünet, ha egyébként szünet eleje lenne, de a szó az előbbi kivétel miatt nem fejeződött be.
- Nincs vége a mondatnak, ha egyébként vége lenne, de a 2. kivétel miatt a szó folytatódik még.

Cselekvések:
- Mondat elején:
  A mondat nyelvét jelző kétbetűs azonosító és a tartalék beírása a kimeneti fájlba; pl: Huxxx.
- Szó elején és közben: Egy átmeneti tárolóban a szó karaktereinek letárolása.
- Szó végén:
  A teljes szó elemzése, majd az átalakított verzió tárolása.
- Szünet elején:
  Egy darab üres karakter írása a kimeneti fájlba.
- Szünet közben és végén:
  Semmit sem szükséges tenni.
- Mondat végén:
  Írásjel és egy újsor kiírása.

Teljes szó elemzése:
Állapotok:
- az épp vizsgált karakter betű, szám vagy egyéb,
- a részszóban volt-e már magánhangzó.

Szabályok:
- Legelőször a teljes szó keresése a kivételszótárban. Ha szerepel benne, akkor kilépés az elemzésből, ha nem folytatása.
- Ha betű a karakter akkor a részszó eltárolása.
- Részszó vége van ha nem betű karakter jött.
- Ha nem betű, vagy vége a teljes szónak, akkor a részszó elemzése következik.
- A részszó szerepel-e a kivételszótárban? Ha igen, akkor a válasz behelyettesítése a részszó helyére, egyébként az részszó elemzés folytatása.
- Ha nem volt magánhangzó a részszóban, akkor a részszó helyettesítése a betűzött formájával.
- Ha az előzőek nem voltak sikeresek, a részszót változatlanul vissza kell írni.

Kivételek:
- Betű típusú egy karakter, ha betű vagy egy magánhangzó utáni repülő ékezet.
- Ha betű a részszó utáni karakter, akkor annak is kiírása. Csak szó végén fordul elő.
- s betűt tartalmazó részszót nem szabad lebetűzni.
- Számokat változatlan formába kell visszaírni.

Példa:
szó:
http://www.hszk.bme.hu/ s6147zai/help.html
_____-okkal jelölt részek a részszavak.

Átalakított: há té té pé kettőspont per per wéwéwé pont há esz ká pont hu per tilde 6147 zai per help pont há té em el

Tehát a program az előzőekben leírt szabályrendszer alapján karakterről karakterre végigvizsgálja a szöveget. A kivételeket a magyar mondatokhoz az irregularhu.txt-ből veszi, mely a következő formátumban van letárolva:
[_]<keresett szó>[_] <helyettesítési alak>

A keresett szó előtti, illetve mögötti alulvonás karakterek azt határozzák meg, hogy a szó abban az irányban folytatódhat-e vagy nem. Ha az alulvonás szerepel akkor csak olyan esetben illeszti a program, ha ott van a szónak a határa. A helyettesítési alak bármilyen karaktersorozat lehet, a karaktersorozat a sor végéig tart. Jelenlegi állapotában a kivételszótár tartalmaz néhány idegen szó megfelelő ejtését, keresztnevek ékezet nélküli alakját és a hozzá tartozó ékezetes formát, hónapok rövidítését, továbbá néhány egyértelmű ékezetesítést, rövidítést.
Példa: _bye_ báj
_email ímél
...

A program használja még a spellhu.txt is, ami az egyes betűk betűzését és a speciális karakterek kimondását tartalmazza:
@ kukac
< nagyobbjel
> kisebbjel
...

4.7.3. Multmail interpreter

Ez a program végzi a teljes vezérlését a szövegfeldolgozó résznek, a működést vezérlő fájlban leírt utasítások szerint.

Az interpreter tulajdonságai:
- Elméletileg tetszőleges számú felhasználót ki tud szolgálni.

- Minden felhasználóhoz külön interpretálja a forrást, más is lehet az egyes felhasználóknál.
- Egész változók tárolásának, számításának támogatása.
- Címkék definiálásának lehetősége, ugró utasítások.
- Tömbök használatának lehetősége.
- Windows Message-k fogadása, küldése.
- Függvényhívások, verem megvalósítás.
- Kisebb, egyenlő, nagyobb feltételek vizsgálata.
- VOS-sal való közvetlen kommunikációra alkalmas utasítások.
- Felfüggesztés (sleep utasítás, alkalmas a felhasználó fájlnak felfüggesztésére, ami a processzorterhelést csökkenti)
- A pillanatnyi utasítástól függetlenül reagálni képes a lenyomott gombokra.

4.7.4. Remove mails and files

Ez a program szolgál a rendszer használata közben keletkező fájlok törlésére. A programot 2 alkalommal hívja meg a multmail egy felhasználó kiszolgálása közben. Első alkalommal a felhasználó bejelentkezésekor, ilyenkor az esetleges rendszerösszeomlásokból[19] visszamaradt szemetet törli. Miután a felhasználó letette a telefonkagylót, a program az összes generált ffájlt törli a logfájlokon kívül. Erre a helytakarékosság, és a felhasználó személyes adatainak védelme miatt van szükség.

5. TOVÁBBFEJLESZTÉS

Elsődleges cél, hogy egy olyan minőségű, és megbízhatóságú rendszert készítsünk amely alkalmas arra, hogy egyetemi szolgáltatásként beindítsuk az egyetemi telefonhálózaton.

5.1. Szolgáltatások bővítése, javítása

A rendszer alapszolgáltatásainak bővítése elengedhetetlen, hisz a mostani rendszer célja csak az volt, hogy kezdeti tapasztalatokat lehessen szerezni az ilyen jellegű szolgáltatás legalapvetőbb fejlesztési, üzemeltetési problémáiról, illetve tesztelni lehessen a sebesség, minőség paramétereket.

5.1.1. Vezérlés

A nyomógombos vezérlés sok ember számára nehézséget okoz, idegenkedést vált ki belőle, mert úgy érzi, nem ő irányítja a rendszert, hanem fordítva. Felhasználó felület készítésekor fontos szempont, hogy a rendszer használójában az az érzés alakuljon, ki hogy egyedül csak tőle függ, hogy mi történik, minden esetben ő legyen a vezérlő. Ez sajnos sok esetben nem valósítható meg, de törekedni kell arra, hogy legalább az érzet hasonló legyen. Ezt azzal is elő lehet segíteni a jelen alkalmazásnál, hogy a nyomógombok helyett emberi szóval, beszédutasításokkal lehessen irányítani, választani a menüpontokból.

A szóbeli vezérlés esetén el kell dönteni, hogy a minden egyes felhasználó betanítsa a rendszert, tehát az egyes funkciókhoz, a saját szavait definiáljuk, vagy egy egységes, mindenki által elfogadott jelrendszert használjunk. Ezt a megoldást használják a National Technical University of Athens fejlesztői is, a rádiós körökben használt ABC[20] szavakkal vezérlik a rendszert. A – Alpha, B – Bravo, C – Charlie, ..., Y – Yankee, Z – Zulu [9].

Ezekek az elnevezések már jól kialakultak angol nyelvterületen, de magyarban nincsen ilyen elfogadott és egyértelműen elkülöníthető betűzési mód. Úgy gondolom, hogy ezt a témakört sokkal részletesebben kell elemezni, de ennek a tanulmánynak nem célja ez, mást állítottam a fókuszba.

5.1.1. Szöveg érthetőségének javítása

- *Új típusú szöveg–beszéd átalakító rendszer integrálása:* A Beszédkutatási Laboratóriumban tovább folytatódik a nagy hagyományokkal rendelkező beszéd–szöveg átalakítók fejlesztése, és várhatóan még ebben az évben egy új alapokon nyugvó rendszer készül el, melynek hangzása sokkal közelebb áll az emberi beszédhez.
- *Ékezetesítés megvalósítása nyelvi elemzés alapján:* Helyesírás ellenőrzőkhöz hasonló elven megoldani az ékezetesítést, tehát nemcsak a szóalakot kell nézni, hanem a mondatban elfoglalt helyét is vizsgálni kell a szónak, és az alapján dönteni a megfelelő alakról.
- *Idegen nyelvű menürendszer lehetősége:* A rendszer jelenleg is kész fogadni más nyelvű elemeket is, de a hanganyagok, szöveganyagokat még meg kell alkotni.
- *Felhasználófüggő menürendszer, és beállítások:* A felhasználónak jelenleg csak az alapvető paramétereket állíthatja, de a szöveg, menü típusából nem választhat.
- *Új, régi, olvasott, nem olvasott, válaszolt típusú levelek szétválasztása:* A rendszer jelenlegi állapotában nem vizsgálja a levelek státuszát, minden levelet egyformának tekint, nem tesz különbséget olvasottság alapján, továbbá nem ad lehetőséget levelek törlésére.

5.2. Rendszer javítása

Funkciók szétválasztása

A programok hordozhatósága megkívánja, hogy a felületek minél szabványosabbak legyenek. Itt nem elsősorban a felhasználói felületre gondolok[21], hanem a programok nyújtotta interfészek egységesítésére. Az eddig megalkotott rendszer önmagában működik, nem integrálható semmilyen komplex rendszerbe.

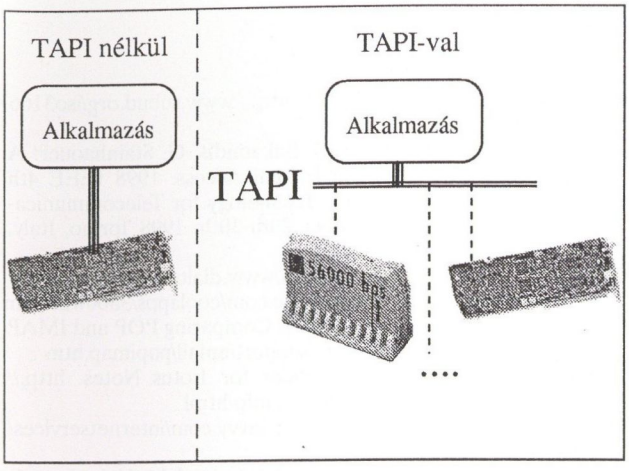
TAPI (Telephony Application Programming Interface):

Ez egy olyan egységes szolgáltatásokkal rendelkező interfész, mely használatával lehetővé válna, hogy a telefonkezelő hardver típusától függetlenül használható lenne a rendszer, tehát az egycsatornás Voice modemet és a 30 csatornás ISDN kártyát ugyanúgy a TAPI biztosította felületen keresztül érné el. Ezzel a megoldással nagyban javulna a rendszer hordozhatósága, hisz a kártya típusa nem lenne „bedrótozva" a programba.

[19] Rendszerösszeomlást okozhat például a hálózati tápfeszültség váratlan kimaradása okozhat.

[20] A polgári és katonai repülésben is ezt a betűzési formát használják.

[21] Az alkalmazás sajátos jellege miatt nemigen lehet ezen a téren szabványosítani.



8. ábra. TAPI alkalmazása

API (Application Programming): Az önálló programot úgy lehet továbbfejleszteni, hogy más alkalmazásokba be lehessen illeszteni, és nem csak teljes rendszerként működjön. Az egész rendszert úgy kell átalakítani, hogy egységes felületet nyújtson a fejlesztő felé, ezt például API felület biztosításával lehet megvalósítani. Például a levélfeldolgozó egyetlen API függvényként szerepeljen, vagy az egész felolvasó egy e_level_felolvaso() függvényként hívható legyen.

Levélletöltés kiterjesztése

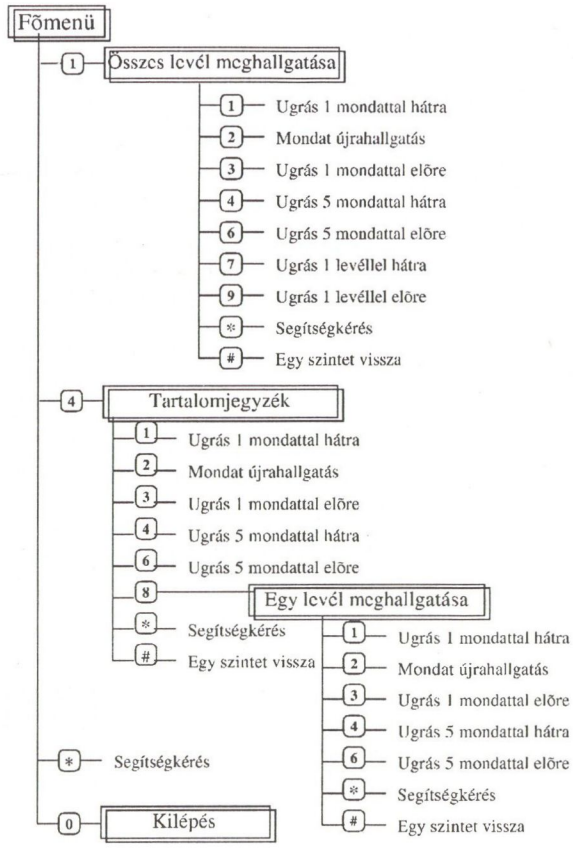
Jelenleg csak az igen „fapados" FTP-vel működik a letöltés, ezt lecserélve az IMAP és a POP protokollt használva javítható a rendszer színvonala. IMAP használata esetén lehetőség lenne a levelek szelektált letöltésére is, ami a rendszer teljesítménynövekedéséhez vezetne, hisz nem kéne csak azokat a leveleket letölteni, amire ténylegesen szükség van.

6. ÖSSZEFOGLALÁS

A felépített elméleti alapok megvalósíthatóaknak bizonyultak, erre szerintem jó bizonyíték a létrehozott demo alkalmazás. Teljes mértékkel tisztában vagyok azzal, hogy az elkészített rendszer nem tökéletes, vannak hiányosságai, de összességében véve egy alapfokú szolgáltatást nyújtó, de megbízható rendszert sikerült elkészíteni. Üzleti alkalmazás színvonalát még nem érte el, de nem is ez volt a célunk, hanem az, hogy egy olyan működő szolgáltatást készítsünk, melyen az alapvető problémákat meg lehet ismerni, a felhasználók szokásait elemezni lehet, és ezzel összefüggésben továbbfejleszteni.

7. DEMO

Információ: http://leszped.ttt.bme.hu
Élő demo (tel.): 463-18-62



9. ábra. TTT – Beszédtechnológiai Laboratórium kísérleti telefonos e-levél felolvasó szolgáltatás menürendszere

8. TARTALOMJEGYZÉK

7. Demo

IRODALOMJEGYZÉK

[1] Szendrényi Zsolt: Telefonos e-levél felolvasó rendszer DSP és hálózati alrendszereinek fejlesztése. BME-TTT 1998. május 22. Diplomaterv 70-75, 82. o.

[2] Bogár Balázs: Telefonos e-levél felolvasó rendszer WinNT alrendszereinek fejlesztése. BME-TTT 1998. május 22. Diplomaterv 31-32. o.

[3] Pásztor Miklós: Magyar ékezetes karakterek az elektronikus levelezésben. http://www.iff.hu/documents/ekezet.html

[4] MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies. ftp://ftp.kfki.hu/documents/rfc/rfc1521.txt

[5] Standard for the format of ARPA Internet text messages. ftp://ftp.kfki.hu/documents/rfc/rfc822.txt

[6] MIME (Multipurpose Internet Mail Extensions) Part Two: Message Header Extensions for Non-ASCII Text. ftp://ftp.kfki.hu/documents/rfc/rfc1522.txt

[7] Koltay Tibor – Szaniszló István: Kapcsolattartás e-mail útján az Interneten. http://www.iff.hu/documents/e-mail.html

[8] Country Codes from ISO 3166. http://www.subud.org/iso3166-countrycodes.html

[9] S. Raptis, C. Malliopoulos, S. Bakamidis, G. Stainhaouer: A Speech Agent for Remote E-Mail Access. 1998 IEEE 4th Workshop Interactive Voice Technology for Telecommunications Applications, September 29th-30th, 1998 Torino, Italy, 151-154. o.

[10] Dialogic – Talking Email. http://www.dialogic.com/coolapps/3261web.htm; http://www.dialogic.com/coolapps/3300web.htm

[11] Shore, Net Services and Support: Comparing POP and IMAP. http://www.shore.net/services/support/email/popimap.htm

[12] PhoneSoft MailCall Mail Reader for Lotus Notes. http://www.phonesoft.com/mailcall/mc_info.html

[13] Net-savvy: Mail Call. http://net-savvy.com/internetservices/emailreader.html

[14] Balogh, Berkes, Kovács: A számítógépes távközlési telematikai szolgálatai. LSI 1988. 157-186. o.

E-MAIL READER

CS. ZAINKÓ, G. NÉMETH, B. BOGÁR, ZS. SZENDRÉNYI

DEPT. OF TELECOMMUNICATIONS AND TELEMATICS
TECHNICAL UNIVERSITY OF BUDAPEST
H-1111 BUDAPEST, PÁZMÁNY PÉTER SÉTÁNY 1/D

Recently email using is become an important point of our life. If you have a computer with internet in the office, there is no problem, but when you are out of the office or travelling, you need a portable computer or laptop, a modem and an internet connection. Instead of these expensive equipment you should call an e-mail reader and you will know your all new mails.

You can listen your mails whenever and whereever you want through telephone with e-mail reader. The service is convert the mail to readable form and read by text-to-speech. The menu system of the e-mail reader is controlled by touch-tone telephone.

This reader has been developing for one and a half year at Department of Telecommunication and Telematics (Technical University of Budapest). There is a experimental development system and a demonstration system. A experimental e-mail reader is connected to the department's education telecom network through a Lucent Definity PABX. The other reader connected to PSTN with a four channel analog telephone interface (Dialogic D/41E). The call number is (+36 1) 463 18 62.

The main problem of Hungarian electronic mails is a lot of people don't use accentuated letters, because some system of users doesn't have those, or the typing is faster without accent. If you read this kind of mail, your intelligence of brain replace a wrong letter by correct form, but can't do it when you are listening to text. Therefore there is a text preprocessor which is convert mails to an accentuated form.

The processing of mails is difficult, because e-mail is 'sluggish' and punctuation marks have different meaning. There are abbreviations, internet links and other expression which contains points but that don't mark the end of the sentence.

Hungarians receive e-mails in a number of languages (for example Hungarian, English, German, etc.), so have to detect the language of the mail, sentence or perhaps every word.

Zainkó Csaba a Budapesti Műszaki Egyetem Villamosmérnöki és Informatikai karán tanul 1994 óta, jelenleg végzős hallgató a Műszaki informatika szakon. 2 éve Üzleti távközlés szakirányra specializálódott és főleg CTI-os alkalmazásokkal foglalkozik. 1998 évi Tudományos diákkonferencián I. helyezést ért el az e-mail felolvasóval.

TÁJÉKOZTATÓ A SZERZŐK RÉSZÉRE

A publikálandó cikket a főszerkesztőnek kell küldeni: Simonyi Ernő, 1061 Budapest, Paulay E. u. 56. II. 4/A; tel./fax: 341 6421, 325 9058, E-mail: sese@mail.matav.hu. Csak magyar vagy angol nyelvű kéziratokat fogadunk el.

A kéziratokat kettes sortávolsággal gépelt oldalakon kérjük beküldeni. Egy megjelent újságoldal kb. 6500 szövegkaraternek, kb. 2 gépelt oldalnak felel meg. A szerkesztői munka megkönnyítése érdekében köszönettel vesszük, ha a szöveg, ábrák, illetve táblázatok MS-WORD 2.0 vagy 6.0, TEX, illetve LATEX nyelvű fájljait is mellékelik.

A cikk címe után a szerző(k) neve és munkahelyi címe következzen. A cím lehetőleg tartalmazza a szerző telefonszámát, faxszámát és E-mail címét is. A szerző(k)nek mellékelniük kell egy rövid, 400-600 gépelt karakteres szakmai szöveges önéletrajzot, és egy jó minőségű fekete-fehér fényképet is. Az életrajz és a kézirat nyelve azonos legyen.

A kéziratot a cikk egy rövid összefoglalójának kell megelőznie. Örömmel vennénk magyar nyelvű összefoglaló angol fordításának, illetve angol nyelvű összefoglaló magyar fordításának csatolását.

A kézirat szöveges részének tartalmaznia kell a cikk szövegét a szükséges egyenletekkel és formulákkal együtt. A szöveges rész címrendűség szerint számozott fejezetekből és alfejezetekből épüljön fel. Az egyenleteket és formulákat a szövegben való hivatkozásokkal összhangban sorszámozni kell. A cikk szöveges részében meg kell jelölni az illusztrációk helyét. A cikk tartalmazhat sorszámozott lábjegyzetekre és szakirodalomra történő hivatkozásokat is.

A sorszámozott lábjegyzeteket külön lapon kérjük. A lábjegyzetek sorszámozása összhangban kell, hogy legyen a szövegben való hivatkozásokkal. Az irodalmi hivatkozásokat kérjük szögletes zárójelben [] feltüntetni mind a szövegben, mind pedig az irodalomjegyzékben.

Az ábrák (vagy egyéb illusztrációk) fekete-fehér, nyomdakész (camera-ready) eredetijét laponként kell mellékelni, egy lapon egy ábrát, az ábrához tartozó sorszámmal és ábraaláírással — összhangban a szövegben levő hivatkozással. Az ábrák megrajzolását vagy újra rajzolását nem tudjuk biztosítani. Köszönettel vesszük, ha az ábrákat tartalmazó, BMP, TIF, PCX, EPS, JPG vagy WMF típusú fájlokat is mellékelni tudják. Az ábrákon szereplő szövegrészek, egyenletek, formulák stb. nyelve egyezzen meg a cikkével, továbbá lényeges, hogy mérete és minősége lehetővé tegye a szükség szerinti kicsinyítést (min. 8,5 cm-ig).

INFORMATION FOR AUTHORS

Contributions should be submitted to the editor in chief: Ernő Simonyi, Paulay E. u. 56. II. 4/A, H-1061 Budapest, Hungary; voice/fax: (361) 341 6421, (361) 325 9058, e-mail: sese@mail.matav.hu. Contributions can be written either in Hungarian or in English. We are sorry, but we cannot accept manuscripts in other languages.

Contributions should be submitted in double spaced typed pages. One page in the journal consists of about 6500 text characters, i.e. approximately 2 typed pages. In order to help editorial work, MS-WORD 2.0 or 6.0, TEX, LATEX files containing the paper, tables and figures are particularly appreciated.

The title should be followed by the author's name (names) and affiliation (institution, address, phone and/or fax number, e-mail address). Each author should provide a short (400-600 characters) technical biography and a black-and-white photograph of good quality. The language of the biography and the paper should be the same.

Contributions should be preceded by an abstract, a short summary of the paper including the title. Hungarian translations of English abstracts, or English translations of Hungarian abstracts are welcome.

The text part of a contribution may contain the text together with the necessary equations or formulas. The part text should be subdivided into hierarchically numbered sections and subsections. Equations and formulas have to be numbered in the same way as they are referred to in the text. The location of the illustrations should be indicated in the manuscript. The text part may also refer to numbered footnotes and references.

Separate pages must contain the footnotes with the same numbering as used in the text. The reference section containing the numbered references must be at the end of the paper. Both, in the text and in the reference list the reference numbers should be in rectangular brackets [].

Black and white and camera ready originals of figures (or other illustrations) should be attached separately together with the numbered figure captions, one figure per one page. We cannot provide drafting or art service. Optionally, BMP, TIF, PCX, EPS, JPG or WMF files types about the figures or tables are appreciated. Text, equations, formulas etc. belonging to the figures or tables should be of the same language as the manuscript. It is important to attach sharp and good quality illustrations which make possible reducing to 8.5 cm, as a minimum size, if necessary.

MATÁV

Oktatási Igazgatóság

Amit érdemes csinálni,
azt érdemes jól csinálni !

Szeretne többet tudni:
a video- és hangtechnikáról,
a digitális jelzéstechnikáról,
az ATM-ről, az SDH-ról,
a mikrohullámú technikáról ?

Forduljon hozzánk !

A híradástechnikai ismeretek köre napjainkban rohamosan bővül. A MATÁV Oktatási Igazgatósága elébe megy a gyors technikai fejlődésnek, célja megalakulásától fogva a távközléssel, az elektronikával összefüggő, ahhoz szorosan kapcsolódó ismeretek fejlesztése. Üzleti filozófiájának része, hogy olyan képzést nyújtson, mely azonnal hasznosítható gyakorlati ismereteket ad.

A MATÁV szakemberei évek óta nagy gyakorlattal, a legújabb eredményekre építve vezetik be az érdeklődőket a híradástechnika világába.

A MATÁV Oktatási Igazgatósága piaci működéséből adódóan továbbra is megőrzi nyitottságát, megtartja sokszínűségét a különböző képzésfajták, képzési szintek és formák tekintetében, tág választási lehetőséget kínálva ügyfelei részére.

QUALITY ASSURED FIRM
ISO 9001
SGS

Részletes felvilágosítás: 431-1629