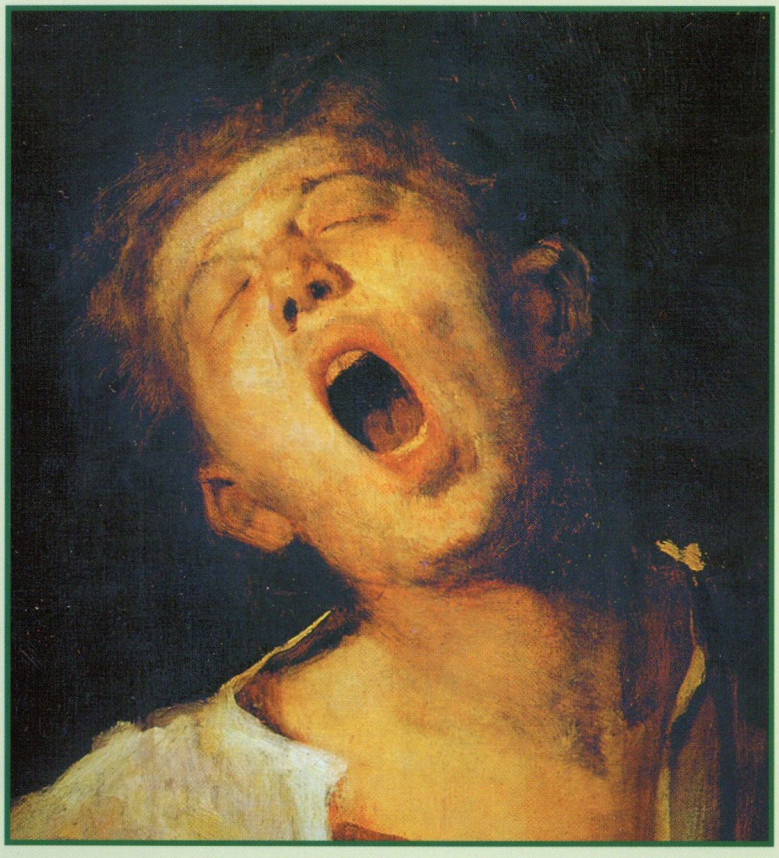
híradástechnika

VOLUME LVIII.

2003/5

Május



A távközlés fejlődése

Elméleti számítások és eredmények

Információs társadalom

A Hírközlési és Informatikai Tudományos Egyesület folyóirata

Tartalom

Címlap: Ne álmosan várjuk, hanem aktívan alakítsuk a jövőt (ELŐSZÓ)

Vonzó távközlési szolgáltatások

(MÁJUS)

Már három-négy éve érezhető, hogy az átviteli kapacitás növekedése lényegesen gyorsabb, mint a felhasználói igények fejlődése. Ez a folyamat párosulva a távközlési verseny megindulásával, csökkenti a távközlési vállalatok profitját. Ugyancsak négy-öt éve várható volt, hogy kipukkadjon az informatikai lufi, ami be is következett, megrázta a tőzsdét és az ezredfordulóra válsághangulat alakult ki. A hirtelen változások hatására számos területen a reménytelenség érzete alakult ki, ami tovább rongálta az infocom terület eredményességét.

Világszerte aktuálissá és divatossá váltak George Gilder tanai. Az általánosan érvényes gazdasági tételt, miszerint, ha egy tömegesen rendelkezésre álló eszköz olcsó beszerzésével és nagy mennyiségű alkalmazásával sikerül egy új, érdekes, vonzó terméket előállítani, akkor az biztosítja a piaci sikert. A kapcsolatos primőr árak pedig a gazdasági eredményességet is. Ennek szellemében az utóbbi években keresték azt a tartalmat, amivel a fényvezetők több terrabit/secundum átviteli kapacitását értékesíteni lehet.

Az ilyen irányú társadalmi felmérések és műszaki fejlesztések mindez ideig nem hoztak átütő eredményt. A távközléssel eddig szoros kapcsolatban lévő távszolgálatok lassú terjedése sem segített az iparág helyzetén. Ezzel párhuzamosan azonban látható, hogy az egészségügy, a biotechnológia, a gépkocsi ipar és az energiaszolgáltatás fejlődésében a jövőben nemcsak az elektronika és az automatika, hanem a távközlés is meghatározó szerepet fog betölteni. Ezek az optimista kilátások csak akkor válnak realitássá, ha a távközlés és informatika, valamint az alkalmazó szakmák közötti határterületeken az érdekelt szakmai képviselők megtalálják az átjárást, az érdekek egyezését és az eszközök alkalmazásának egyszerű megoldását.

Lapunkban is igyekszünk a jövőben kiemelten foglalkozni azokkal a szakterületekkel, melyek elősegíthetik az informatika és távközlés szélesebb körű alkalmazását. Ez természetes kötelességünk, mert az újság neve megegyezik az egyesület régi elnevezésével, ahol nemcsak távközlési szakosztály volt, hanem többek között műsorszóró, informatikai, alkatrész szakosztály is. Ezek is beleérthetők a híradástechnikába, tehát ezeknek a témáknak is kellő súllyal szerepelniük kell.

A kapcsolatok kiépülése érdekében érdemes azokat az elméleti ismereteket bemutatni, melyekre alapozva az új szolgáltatások kiépülhetnek. Jelen számunkban is öt olyan cikk szerepel, mely igyekszik célkitűzésünknek megfelelni. Foglalkozunk például az alkatrészek hűtésének problémájával, protokoll konverzióval, mikroelemek szimulációjával, szűrők zajtényezőinek minimalizálásával. Természetesen a szokásos informatikai témák és beszámolók ezek mellett is megjelennek.

Lehet, hogy kiváló mérnökeink az új területeken esetleg kezdőnek érzik magukat, de biztos vagyok benne, a műegyetemi képzés olyan alapokat adott, hogy ezen ismeretek megszerzése nem okoz nehézséget. Erre építve alakulhatnak ki azok az új szolgáltatások, melyeknél esélyünk lesz a piacon is hasznosítható megoldások kidolgozására.

Reméljük, hogy a tapasztalt, sikeres mérnökök élvezettel tanulmányozzák az új lehetőségeket és az új ismeretanyag megszerzése során szinte megfiatalodnak. Ifjúi lendülettel keresik az új alapokra építhető, vonzó szolgáltatásokat.

Lajtha György

A mobil távközlés kialakulása és jövője

Beszélgetés Sugár Andrással, a Westel vezérigazgatójával

A riportot készítette: NAGY BEATRIX HAVASKA igazgatásszervező
nbh@mailbox.hu

A közel 50%-os piaci részesedéssel rendelkező Westel Mobil Rt. vezérigazgatója több mint 12 éve meghatározó egyénisége a mobil rendszerek telepítésének és üzemeltetésének. Igyekszünk megismerni sikereinek hátterét és jövőképét.

• A mobil szolgáltatások a társadalom közérzetére is hatással vannak. Mivel a történelem ismerete segít a jövő helyes megítélésében ezért kezdjük azzal, hogy milyen volt a kezdet. Mint kiváló külkervállalat-vezető elvállalta egy induló szolgáltatási ág a mobil első kísérleteinek vezetését. Mi késztette erre? Hatással volt-e döntésére Horváth Pál lelkesítő szövege?

Az egész úgy történt, hogy megkerestek. A Transelektro már három éve együtt dolgozott a Magyar Postával különböző távközlési ajánlatok értékelésében. Ezeket én vezettem, tehát ismertük egymást Horváth Palival, aki korábban a hálózatfejlesztési igazgató volt, később aztán a Matáv vezérigazgatója lett. Ekkor kezdtek vezérigazgatót keresni a Westel Rádiótelefon Kft. élére. Sokféle szempont szerint próbálták kiválasztani az ideális jelöltet, de ahogy hallottam nehezen tudták a tulajdonosok (amerikai és magyar) egyeztetni, hogy ki lenne erre a legalkalmasabb. Mivel én megfeleltem az amerikai elvárásoknak, Horváth Pali pedig értékelte a munkámat, így rám esett a választásuk. Később megtudtam, hogy én voltam a 18-dik jelölt, akit megnéztek.

'Ma már senki sem hiszi el, hogy akkoriban a legnagyobb feladat a cég finanszírozásának megszervezése volt. Magyarországon egyik bank sem akart hitelezni, mert nem hittek benne, hogy ez egy perspektivikus üzletág lesz.

• Tehát mások nem bíztak a sikerben?

Tulajdonképpen nem. Gondolom Magyarországon és külföldön is egyaránt a jó bankkapcsolataim hatásos érvként szolgáltak mellettem.

Ehhez el kell mesélnem egy anekdotát: amikor először bejött hozzám az akkori gazdasági igazgató, Fürjes Zsóka, megkérdeztem tőle, hogy állunk. Mondta, hogy van 15 millió dollár kifizetetlen számlánk. Ekkor megkérdeztem: menynyi készpénzünk van? Azt mondta mínusz 7 millió Ft. Akkor tönkrementünk, mondtam. Így is lehet mondani, felelte.

• Hitt abban, hogy ebből egy hosszú távon is sikeres üzletág lesz?

Én abszolút hittem. Láttam a terveket, persze a tervek sokkal szebbek voltak, mint a valóság. Viszont láttam külföldön, hogy ott ezek a mobilszolgáltatások előbb vagy utóbb lábrakapnak és fantasztikus pályát futnak be.

Akkor még persze nem számoltunk milliós előfizetői körrel, de a vezetékes ellátottság is 950 ezer vonal volt, tehát nem egészen 10%. Ebben a környezetben hinnünk kellett abban, hogy a cég egyszer finanszírozható lesz, és országos ellátást tud majd nyújtani. Továbbá hinni kellett abban, hogy el tudjuk indítani a szolgáltatást, ami azért volt különösen nehéz, mert akkor még nagyon drágák voltak a készülékek, ráadásul ezen a magas áron nem tudtunk piacot bővíteni.

A 200 ezer Ft-os telefon nagyon sok problémát okozott az értékesítésben. Nagy élmény volt ezért, amikor 1992 decemberében a Westel Rádiótelefon Kft. elérte a 20 ezres ügyfélszámot. Ezen a fantasztikus ünnepen éreztük először, hogy nem reménytelen az üzlet. Nagyon sok marketing trükköt és kommunikációs üzenetet kellett a piacra dobni a fellendüléshez. Mindezek mellett hittünk a sikerben.

• A konzervatív nézeteket valló postás kollegák mennyire voltak nyitottak az újdonság irányába?

Villamosmérnök vagyok, ezért tudom, hogy milyen keményfejűek a mérnökök. De ha megmutatjuk nekik, hogyan kell működnie egy cégnek, és az eredmények is jönnek, akkor maguk is részesei lesznek a közös igyekezetnek.

Egyik fő feladatunk az volt, hogy az akkor 70%-os műszaki orientáltságú és 30%-os marketing ügyfélorientált cégből egy 70% marketing és 30% műszaki orientáltságú céget csináljunk. Ez sikerült, és azóta is így van. Nálunk a marketing vezeti az egész céget és ezt a filozófiát kellett elfogadtatni. Természetesen engem, ha az elképzelések megvalósítása nem igazol, elsöpört volna a történelem. Ez azonban nem így történt.

Tulajdonképpen belátta mindenki, hogy versenyhelyzet van, ahol a marketing a döntő tudomány a siker felé vezető úton. Most már büszkén mondhatom, hogy több műszaki vezetőmnek is van MBA képzettsége. Így már ők is érdeklődnek a marketing iránt, mert látják, hogy attól az ő tudományuk cseppet sem lesz kevesebb, ha kicsit kitárják az ablakot és kinéznek rajta. Megismerik mit kér az ügyfél, mit kér a piac és miként kell a szolgáltatási portfoliót összeállítani.

Szerencsére, ez egy növekedő vállalat, tehát az átalakulást meg lehetett menet közben szervezni. Nem kellett embereket elküldeni, csak arra kellett figyelni, hogy az újak már más képességeket hozzanak be a cégbe.

• Milyen elvek alapján történt a kollégák kiválasztása?

Tudás, rátermettség, elkötelezettség, állandó áttörési kísérlet, emellett akaraterő, mely segít megvalósíthatatlannak tűnő feladatokat is megvalósítani. Mi kellett mindehhez? Csapatépítő ember vagyok, és mint csapatjátékos dolgozom. A kollégáim addig értékelnek, amíg valami többletet tudok adni az ő gondolkodásukhoz, és ezt el is várják. Ugyanezt kérem én is a munkatársaimtól, így tulajdonképpen egymás gondolatát formáljuk. Ezáltal korszerűbb lesz az egész cég, mind a gondolkodásunk, mind a lehetőségeink bővülnek, és nem utolsó sorban a piacon is sikeresen helytállunk. Mi magyarok meg akartuk mutatni a világnak, ha lehetőséget kapunk, akkor azzal jól fogunk sáfárkodni és behozzuk lemaradásunkat a mobil távközlésben. Ez egy nagyon fontos kérdés volt számunkra.

Jelentős kihívást is jelentett és egy nagy adag magyaros kurázsi is kellett ahhoz, hogy tíz év alatt ezt véghezvigyük. Ehhez persze a cégen belüli egyetértésre is szükség volt és a tulajdonosi támogatást is megkaptuk.

• Észrevehetően óvatos volt a készenléti rendszerek létesítésével kapcsolatban. Ennek üzleti, politikai vagy stratégiai okai voltak?

Megtanultuk, hogy a távközlés nagyon beruházás igényes ágazat. A 70-es években már próbálkoztam egyetlen egységes diszpécser rendszert létrehozni. De már akkor is minden tárcának különböző elképzelése volt a rendszerrel kapcsolatban. Más a honvédségé, a tűzoltóságé, így nem lett volna lehetséges egységes digitális készenléti rendszert kiépíteni. Az igények mindig igen szerteágazóak. Ez persze most is fellelhető...

Gazdaságos lehet-e egy országos szolgáltatás 35 ezer ügyféllel? Meg lehet csinálni, persze ha valaki szán erre elegendő pénzt, de működő üzleti modellt még nem láttam, hiszen ezek a hálózatok nem 35 ezer felhasználó számára készülnek. Ahogy látjuk a mobilok is milliós ügyfélkörrel rendelkeznek, és akkor kezd nyereségesen működni. 35 ezer ügyfélnél csak drágán lehet szolgáltatni.

Én valóban nem vagyok lelkes, de vannak konstrukciók, amiben el tudom képzelni a továbblépés lehetőségét. Ha esetleg a három mobilszolgáltató összefogna és cserébe megkapná a UMTS licencet. Ebben az esetben maga a kezdeti beruházás kvázi kikerülne a modellből, és rögtön csökkenne a pénzügyi teher, amely lehetővé tenné, hogy a szolgáltatás ára olcsóbb legyen.

A másik kérdés, hogy milyen minőségű, milyen feltételrendszerű szolgáltatást kell nyújtanunk. Nem lövünk-e túl az igények oldalán akkor, amikor tudjuk, hogy a mentőautó fél nap alatt megy ki a beteghez, akkor nem nagyon számít, hogy hány másodperc alatt értesítettük.

A meglévő hálózatokkal is megoldhatónak látszik a feladat. Egyre inkább érezhető, hogy a Nokia ki fog hozni egy olyan zártláncú megoldást a meglévő GSM hálózaton, mint annak idején az Ericsson – a GSM PRO-val – ami nagyon jól vizsgázott. Az árvízi védelemnél ezzel a rendszerrel 16 készülék tudott egymással kapcsolatot tartani. És nagy szerepe volt a szolgáltatásnak abban, hogy a töltéseket meg lehetett óvni az átszakadástól.

Ebben a kérdésben majd a kormány fog dönteni.

• A 450-es „kis" Westel egy darabig önállóan üzemelt. Ma már nem is hallani róla. Vannak-e még előfizetők a 60-as élő hívószámon, tervez-e ezen a frekvenciasávon és ezen a hívószámon valamilyen új, a közvélemény előtt nem is ismeretes szolgáltatást bevezetni?

Fájdalmas nézni, hogy milyen rövid a 06-60-as cég életciklusa. Hihetetlen mennyit invesztáltunk a hálózatba és 13 év után itt állunk, elhaladt mellettünk a GSM gyorsvonat és elvitte az ügyfeleket. A 06-60 a kiürülés előtt áll. Nagyon örülünk, hogy egyáltalán eddig kitartott.

Nyugat Európában az is világrekordnak számít, hogy rendszerünk egyáltalán még működik, mert ők már rég beszüntették ezeket a szolgáltatásokat. 15-18 ezer ügyféllel ezt már nem lehet gazdaságosan üzemeltetni. Ahhoz, hogy fenntartsuk évek óta pénzt kell belepumpálni. Az előfizetők száma havonta több ezer ügyféllel csökken, de természetesen szívesen látjuk őket a 30-as hálózatban.

• Hogyan látja az újabb generációs rendszerek jövőjét?

Az első generációs rendszerek után a második generáció olcsóbban többlet értéket hozott. Ezek után senki sem magyarázta el, ezért senki sem értette világosan, hogy a második és a harmadik generáció között, mivel digitális rendszerek nincs akkora különbség. A 3. generációs rendszerek adatátviteli sebessége figyelemreméltóan magas, így ezek a rendszerek képzik a mobil Internet infrastruktúráját.

• Lesz-e valaha 4G vagy 5G, és az milyen frekvenciasávban fog működni?

Ezeknél a rendszereknél az egyre nagyobb adatátviteli sebesség a döntő. Többletértéket csak az átviteli sebesség hordoz magában. És ehhez járulhat az egyre gazdagabb tartalom, valamint a legkülönfélébb üzleti alkalmazhatóság.

Mi Magyarországon a második generációs GPRS-szel már elértük azt, hogy egy 40-50 kbit/sec sebességgel tudunk adatokat letölteni. Ezzel elértük, hogy az ügyfél érdeklődni kezdet a WAP iránt, amit mi már rég eltemettünk. Mert a WAP szolgáltatás két évvel ezelőtt is jó volt, csak a sebesség nem volt kielégítő. Amikor a 777 mobil portált bevezettük, egyszerre mindenki föléledt, ezzel a WAP reneszánszát hoztuk létre nagy sikerrel.

• Sok esetben az előfizetők lemondják a fix állomásokat, mert nyaralókban, üdülőhelyeken nem érdemes 12 hónapig alapdíjat fizetni. Ez jelentheti-e azt, hogy a mobilszolgáltatóknak az eddiginél lényegesen nagyobb forgalomra kell felkészülniük?

A tarifaverseny miatt változik az ügyfél szokása, és ez a verseny kiterjed a vezetékes rendszerre, de a mobilra is egyaránt. Olyan verseny ez, ahol igyekszünk egyre jobb ajánlatokat adni. A mobil nagyon kényelmes eszköz de néhány nagysebességű szolgáltatáshoz elengedhetetlen a vezetékes kapcsolat.

• A piacon jelenleg három cég van, melyek közül a Vodafone meglepő tarifapolitikával igyekszik utolérni a két vezető vállalkozást.

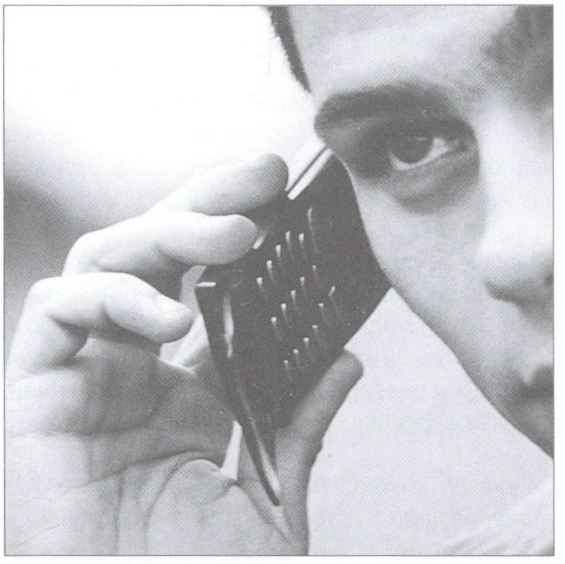
Amikor még csak ketten voltunk a piacon, már akkor is nagy volt a verseny. Ez csak fokozódott a Vodafone belépésével. A múlt évben közel 20%-kal nőtt a piac. Elértük azt a 69-70%-os telítettséget, ami már csak 5%-kal marad el az EU átlagától. Kivéve a Skandináv országokat, ahol a földrajzi és meteorológiai viszonyok miatt a telítettség 80%. Nagyon jó eredményt produkált Magyarország és a mobil valóban kiemelkedően népszerű.

Most következik majd egy fázis, amikor egyre fontosabbá válik az ügyfelek megtartása. Ezért a jövőben a verseny csak fokozódni fog. A Westel mindent megtesz, hogy a minőségstratégiája fenntartásával a leginnovatívabb szolgáltató legyen a piacon, a legkedvezőbb árakkal jelentkezzen, és előnyben legyen a másik két szolgáltatóval szemben. Az április 1-én bejelentett lebeszélhető 50%-os havidíjkedvezménnyel azt hiszem a Westel lepte meg a konkurenciát.

• A felhasználók számának növekedésével és a képátvitel megjelenésével valószínűleg több frekvenciára lesz szükség. Elképzelhető-e hogy a következő években kialakul a pikocellás rendszer, esetleg épületen belüli cellákkal, vagy külön lakópark ellátással?

Az épületen belüli ellátást kell javítani, olyan helyeken, ahol sok a vasbeton, vagy az ablak van bevonva különböző védőrétegekkel. Ez gátolja, árnyékolja az elektromágneses hullámok terjedését. Éppen ezért nekünk az épületen belüli ellátáshoz, annak javításához kell a pikocellákat alkalmazni. Ezt már régóta alkalmazzuk az üzletházakban, családi háznál, és a bevásárlóközpontban is. Ez a minőségbiztosítás egyik szükséges eszköze.

A viszonylag kis kapacitású állomások rendkívül hasznosak bizonyos esetekben. Elsőként bemutattunk a Ferihegyen egy olyan rendszert, ahol a WLAN hálózaton keresztül lehet az Internetre felcsatlakozni. A letöltés sebességét a WLAN hálózattal megoldással tudjuk növelni. A rendszer különösen népszerű lehet a „hot spot" kategóriájú helyeken, ahol sok ember tartózkodik, és sokan kívánják a PC-jüket használni vezeték nélkül.



Hírek

Beata Brestenska szlovák parlamenti képviselő, az Infovek Projekt egyik értelmi szerzője megkezdte az előkészítő munkálatokat annak érdekében, hogy a szlovák országgyűlésben létrejöhessen a „Társadalom informatizálása" elnevezésű parlamenti bizottság. Ez azért is fontos, mert a szlovákok kissé szkeptikusak az IT fejlődése, ezen belül főként a kormányzat és az országgyűlés által támogatott internetfejlesztési kísérletek ügyében. Az Infovek Projekt célja, hogy felkészítse az ország fiatalságát a XXI. századi életre. Az Infovek végrehajtása során valamennyi iskolatípus és szakma számára korszerű tananyagok kidolgozására is sor kerül.

•

A Nemzeti Információs Infrasturktúra Fejlesztési Program (NIIF), a Hungarnet Egyesület és a Magyar Internet Társaság 2003. április 14-17. között tizenkettedik alkalommal rendezte meg a Networkshop konferenciát, amelynek idén a Pécsi Tudományegyetem Pollack Mihály Műszaki Főiskolai Kara adott otthont. A Cisco Systems, teljes IP alapú hangátvitelt valamint vezeték nélküli hálózati hozzáférést biztosított a résztvevőknek. A Networkshop a felsőoktatási hálózati szakemberek évente megrendezett legrangosabb konferenciája, amelyen e rohamosan fejlődő terület technológiájának és alkalmazásainak kutatói, fejlesztői, a gyártók, a szolgáltatók és a felhasználók találkoznak. A rendezvényen közel 500 szakember vett részt, de az előadások egy részét videokonferencia segítségével a felsőoktatási intézmények hallgatói és oktatói is nyomon kísérhették.

•

Az Informatikai Vállalkozások Szövetsége – folytatva az 1997-ben megkezdett, mára már hagyományossá vált kezdeményezést – az idén is jutalmazta az elmúlt év legkiemelkedőbb teljesítményét nyújtó informatikai menedzsereket. A tavalyi évtől kezdődően a díj – a szövetség néhai elnökének tiszteletére – „Gyurós Tibor Díj"-ként kerül az adott év kiválasztottjához. A vezetői kvalitásokat szimbolizáló, vándordíjként funkcionáló karmesterpálcát, valamint az Év Informatikai Menedzsere díjjal együtt járó, fémbe vésett oklevelet ez alkalommal Vityi Péter, a Microsoft Magyarország Kft. ügyvezető igazgatója vehette át. Az „Év Fiatal Informatikai Menedzsere – 2002" kitüntető címet pedig Dr. Czinege László, a Hewlett-Packard Magyarország Kft. Divízió igazgatója nyerte el.

Az infokommunikációs hullám sajátosságai

BŐGEL GYÖRGY
A KFKI Számítástechnikai Rt. stratégiai tanácsadója,
a Közép-Európai Egyetem Üzleti Iskolája tanári karának tagja, a Debreceni Egyetem docense
gbogel@kfki.hu

„...maga az élet ciklikus..." (Bródy András)

Cikkünk a modern információs technológia fejlődését vizsgálja a technikai innovációra épülő cikluselmélet tükrében. Arra a kérdésre keres választ, hogy mennyire felel meg az informatikai csúcstechnológia eddigi története a technikai innovációt középpontba helyező ciklusmodellnek, megtalálhatjuk-e benne a jellegzetes fejlődési szakaszokat, mennyiben hasonlít az IT ciklus a korábbi hullámokra, előidézett-e szélesebb és mélyebb gazdasági és társadalmi „rendszerváltást". Az utóbbi kérdés vizsgálatánál megkülönböztetett figyelmet szentelünk a vállalatvezetésnek. Legfontosabb megállapításunk az, hogy az információs technológia fejlődése valóban hullámot gerjesztett a gazdaságban és a társadalomban, ami sok tekintetben hasonlít a korábbiakra, de egyes pontokon el is tér azoktól. A tanulmány végén kitérünk arra is, hogy ha valóban beszélhetünk informatikai ciklusról, akkor hol tartunk benne most, és milyenek a kilátások. Ezzel kapcsolatban két lehetséges helyzetértelmezést és forgatókönyvet vázolunk fel.

1. Innovációs hullámok a gazdaságban és a társadalomban

A technikai innovációs hullámok általános jellemzői

A jelentősebb technikai innovációk (gondoljunk például a gőzgépre, a vasútra vagy a telefonra) hatóköre messze túllépi a technika és a gazdaság határait. Minden hullámnak van egy *vivő ágazata,* amihez más vezető ágazatok kapcsolódnak: gőzgép például „innovációs nyalábot" alkot a vasúttal, a vasúti berendezésekkel, a gőzmeghajtású gyártóeszközökkel. Ezen ágazatok fejlődése meghatározott *inputokra* (példánknál maradva: vasra és szénre) épül. A kornak megvannak a maga alapvető közlekedési és kommunikációs eszközei (vasút, telegráf, gőzhajó), amelyek az újítások terjedésének sebességét is befolyásolják. A technikai újításokhoz szervezési és vezetési innovációk kapcsolódnak: a vasúttársaságokat nagyrészt már részvénytársasági formában szervezték meg.

Könnyű belátni, hogy az új eljárások és termékek terjedését több tényező befolyásolja, így például a korábbi technológiák érettsége (elektromosság és vasút nélkül nehéz elképzelni az autóipar fellendülését), a nyersanyagforrások bősége és hozzáférhetősége, az energiaellátás, az infrastruktúra, a munkaerő mennyisége és szakértelme, a fogyasztási szokások és a vásárlási hajlandóság, a jogrendszer, az állami szabályozás. Ha mindezek között nem alakul ki valamilyen harmónia, a hullám nem indul el.

Carlota Perez egyik írását [2000] felhasználva nézzük meg, hogyan megy végbe a technikai innovációk által előidézett „rendszerváltás". A venezuelai kutató szerint az események jellegzetes mintát követnek. Az új technológia „berobbanásához" egyes *alapvető inputok* (pl. szén, vas, acél, áram, olaj, mikrocsip) árának radikális csökkenésére van szükség. Ez lehetőséget ad egyes, az olcsó forrásokat nagy tömegben felhasználó iparágak felfutására, ami újabb vállalkozókat vonz az input előállításába és a tömegszerűség révén tovább javítja a gazdaságossági mutatókat.

A mérnökök és a vállalkozók előtt új „tervezési tér" bontakozik ki olcsó és megbízhatóan rendelkezésre álló inputokkal, újfajta eljárásokkal és technikai modellekkel. Megindul az inputokra alapozott termékek terjedése (vasút, elektromos cikkek, autó stb.), ami „begerjeszti" az értékesítésükkel, szervizükkel, használatuk megkönnyítésével foglalkozó, kiegészítő iparágakat, és nyilvánvalóan új infrastruktúrára is szükség lesz.

Az inputokat előállító, az új termékeket „hordozó", a kiegészítő és az infrastrukturális iparágak öngerjesztő összjátéka, *pozitív növekedési spirálja* (ezt az elnevezést Bill Gates egyik könyvéből [1995] vettük át, aki a fiatal informatikai iparágat jellemzi vele), a tanulási görbén való előrehaladás, a tömegtermelés gazdaságossága, az innovátorokat csábító extraprofit lendületbe hozza a gazdaságot. Ezt a folyamatot figyelte meg például a fényvezetőkkel kapcsolatban George Gilder, és vetítette előre az ebből következő új szolgáltatásokat.

Az új termékek és technológiák tervezéséhez, előállításához, elosztásához és használatához új vezetési, oktatási és egyéb rendszerekre, ideológiákra, szabályokra, életstílusra, kultúrára, kormányzásra, politikai rendre van szükség. A rohamosan növekvő, nagy nyereséget zsebre vágó új iparágak és cégek mindent latba vetnek ezek megteremtése érdekében: terjesztenek, propagálnak, lobbiznak, magyaráznak, példát mutatnak, és így tovább.

Mivel a régi rend szükségképpen *ellenáll,* az új harmónia mindenféle csatározások közepette, nem ritkán vérben és verítékben születik meg. A korábbi, lassuló, hanyat-

lásnak induló iparágak és a hozzájuk kapcsolódó rendszerek munkásai, alkalmazottai utcára kerülnek, szakértelmek, képességek értéktelenednek el, társadalmi és politikai feszültségek keletkeznek, összeütközések robbannak ki; utcán, kávéházban, parlamentben heves viták dúlnak mindenféle szabályozási, gazdaságpolitikai, vámügyi és egyéb kormányzási kérdésekről. Az események lefolyását természetesen sajátos *helyi körülmények* (politikai, földrajzi helyzet, történelmi múlt, nyelv, fontos közszereplők egyénisége stb.) is befolyásolják A hullám beindul, kiterjed, „rendszerváltást" idéz elő.

Schumpeter [1980] ezt a folyamatot „kreatív rombolásnak" nevezi, jelezve, hogy valami elpusztul, de egyben valami új is létrejön, az egyik hullám hanyatló szakasza átfed egy másik felemelkedésével.

A technológiák életciklusa

A „rendszerváltást" előidéző technológiák (a fenti leírásból láthatjuk, hogy valójában inkább közös gyökerekből táplálkozó technológia-nyalábokról van szó, amelyekbe beleértjük a hozzájuk kapcsolódó munkaszervezési módokat is) életciklusa a következő tipikus fázisokra bontható.

a) Lappangás. Az új technológia *laboratóriumi fázisban* van. („Laboratórium" alatt adott korokban kolostort, egy kastély dolgozószobáját, pajtát vagy éppenséggel garázst kell érteni.) Megszületnek az első, a házilagos kivitelezés miatt meglehetősen kezdetleges prototípusok. Megtartják az első termékbemutatókat, bejegyeztetik az első szabadalmakat.

Mindenféle alkalmazási kísérleteket végeznek, de a technikatörténeti munkákból (lásd pl. [Greguss 1985]) látható, hogy a feltalálóknak, tudósoknak gyakran fogalmuk sincs arról, hogy mire is lehet majd az újdonságot használni, a közönségről nem is beszélve. Ez a fázis akár egészen sokáig is tarthat, az innováció hatóköre nagyon szűk, az újdonságok alig láthatók.

b) Bizonyítás. Bizonyosságot nyer a *technikai* megvalósíthatóság. Az új technológiák és termékek életképesnek mutatkoznak, méghozzá nemcsak technikai szempontból, hanem *üzletiből* is: sikerül tömeges érdeklődésre számot tartó alkalmazási módokat találni, van kereslet, a befektetések megtérülnek, nyereséget lehet csinálni. Az újdonságoknak híre megy, egyre többen érdeklődnek iránta, vevők és vállalkozók egyaránt. Ez az a pillanat, amikor a nagy gazdasági-társadalmi hullám megindul.

c) Berobbanás. Elkezdődik az inputok, a vivő, hordozó és kiegészítő iparágak fentebb leírt, pozitív fejlődési spirált eredményező összjátéka. Innovátor körökben általános a lelkesedés, a nagy nyereség reménye sokakat csábít, magasba szökken a *gründolási láz*. Egyre több új vállalatot alapítanak. Bródy András felhívja a figyelmet arra, hogy az innováció lökésszerűsége – ez a „lökés" történik meg a *berobbanás* fázisában – nem *oka,* hanem *következménye* a gazdaság ciklikus menetének [Bródy 1983]. Ezzel egyrészt arra utal, hogy közgazdasági szempontból „innováció" alatt nem valaminek a feltalálását, hanem az újdonság tömeges alkalmazásba vételét kell érteni, másrészt jelzi, hogy az „innovációs lökés" más gazdasági tényezők (kamatláb, beruházások) szintén ciklikus mozgásának a függvénye.

d) Növekedés. Az új technológiák és az új termékek közismertek és általánosan elfogadottak, a hétköznapi élet részévé válnak, *domináns rendszert* alkotnak. Rohamosan bővül az alkalmazási lehetőségek köre. Az általános emelkedő trendre, divathullámok, „őrületek" időszaki hullámai rakódnak rá, egyesek az általános és tartós aranykor beköszöntét jövendölik. (Részletesen elemzi a „mániák" természetét Kindleberger [2000].) A társadalomban, a politikában, a vállalatvezetésben, az oktatásban, a kultúrában, a törvényhozásban és szabályozásban mélyreható változások mennek végbe.

e) Lassulás. A domináns technológiák beérnek, a fejlődésük már nem revolúciós, hanem evolúciós jellegű. A hirtelen meggazdagodás kora lezárul, a telítődő piacok, a heves verseny lefelé szorítják a jövedelmezőséget. Egyes források kiapadnak, megdrágulnak. A piacon a túlkínálat jelei mutatkoznak. Nem ritkák a csődök. Ez ismét nehéz időszak, méghozzá leginkább azoknak, akik a megelőző fázis eufóriájához, magas növekedési és jövedelmi számaihoz, az azokkal együtt járó társadalmi státuszhoz és érdeklődéshez szoktak hozzá, és most kicsúszni érzik a lábuk alól a talajt.

Leginkább Grove [1997] *inflexiós pontját* juttatja az eszünkbe: azt a kanyart, ahol radikális lépésekre, strukturális alkalmazkodásra van szükség. A lassulás egyre határozottabban érzékelhető az egész gazdaságban, a társadalom nyugtalan, egyre több a pesszimista előrejelzés. Mindeközben a fű alatt már ott lappanganak az új technológiák, amelyek bizonyítás után „berobbanhatnak" és a maguk képére formálhatják a világot.

f) Érettség. Egy hullám végén „hanyatlásnak" kellene bekövetkeznie, de szándékosan nem használjuk ezt a szót. Vannak esetek, amikor egy technológia a hozzá tartozó termékekkel együtt egyszerűen *eltűnik* a hullám végén. Az sem elképzelhetetlen viszont, hogy valamilyen impulzus hatására *újjáéled,* például azért, mert a termékekhez új felhasználási módot találnak, azok életpályája újraindul. De van még egy lehetőség: a domináns technológia ugyan más lesz, de *együtt lehet élni* vele, bele lehet simulni, fel lehet ülni a szekerére: a nagy vasútépítési kornak vége, de vonatok nélkül elképzelhetetlen lenne az élet.

2. Az autóipari hullám

A technológiai életciklus fázisainak általános ismertetése után lássuk, hogy az utolsó, többé-kevésbé teljes technológiai hullám hogyan ment végbe. E hullám vezértermékе a robbanómotor és az autó volt.

a) Lappangás. Bár a robbanómotort már valamikor a 19. század hatvanas-hetvenes éveiben feltalálták [A technika krónikája 1991], az hosszú évtizedeken át nem gyakorolt különösebb hatást az iparra és a gazdaságra. A robbanómotoros járgányok gyártása Amerikában és Európában egyaránt kis autógyártó műhelyek százaiban folyt. Az autózás a gazdagok szórakozása volt.

b) Bizonyítás. 1908 és 1914 között Henry Ford számos újítást vezetett be a saját autógyárában. (Tegyük hozzá: ehhez sok segítséget kapott egy Galamb József nevű magyar mérnöktől.) Közülük a témánk szempontjából legfontosabbak nem a termék konstrukciójára, hanem gyártásának módjára vonatkoztak. A korábbi egyedi elemeket Ford szabványos, cserélhető alkatrészekkel váltotta fel, amiket célgépekkel állítottak elő. Bebizonyosodott, hogy az autót szabványos termékként stabilizálni lehet, a gyártást tömeges méretekben racionálisan meg lehet szervezni, a sorozatgyártásra sikeres üzleti modellt lehet építeni.

Maga Henry Ford társadalomfilozófusként is fellépett [Ford 1989], elképzelései közül számos meg is valósult, bár azok közé kétes gondolatok is keveredtek [Baldwin 2001]. Ha a vállalkozások tipikus fejlődési fázisait leíró Greiner-modellt [1995] használjuk, azt kell mondanunk, hogy Ford az autógyártást a „kreativitás" fázisából átvitte a „profi irányítás" szakaszába.

c) Berobbanás. A múlt század húszas éveiben a robbanómotor *egyeduralomra* tett szert. A sok száz autógyártó műhely helyét fordi elvek alapján működő gyárak vették át. A szabványosításnak, az új munkaszervezési módszereknek, a szisztematikus racionalizálásnak köszönhetően a munka termelékenysége látványosan növekedett. A benzin mint „alapvető input" stabil minőségű, olcsó, könnyen hozzáférhető termékké vált.

Ford T-modelljéből 1908 és 1927 között összesen 15 millió darabot gyártottak Az ára egyre inkább megfelelt az átlagember pénztárcájának: 1908-ban még 850 dollárt kellett fizetni érte, 1913-ban már csak 600-at, 1916-ban pedig már potom 360 dollárért szerezni lehetett egyet.

d) Növekedés. 1938 és 1980 között a világ autóiparának termelése rohamosan bővült. Egyes kis méretű, egyedi példányokkal foglalkozó, exkluzív műhelyek megmaradtak ugyan, de a prímet már egyértelműen a terjeszkedő *gyáróriások* vitték. Az autóiparral együtt növekedtek a hozzá kapcsolódó hordozó, kiegészítő és infrastrukturális iparágak. Egymást követték a különböző gyártási újítások. Megindult a piac szegmentálódása és ennek nyomán a termékek differenciálódása, amire a General Motors gyorsabban reagált a Fordnál [Chandler 1969].

Az emberi tőkébe történő beruházásokkal foglalkozó Schultz kimutatta, hogy az USA lakosságában az egy főre eső konstans iskolaévek száma 1900 és 1957 között több mint hatszorosára emelkedett, a növekedés erőteljesebben 1929 után indult meg, és a második világháború után újabb lökést kapott [Schultz 1971]. A „tudásbázisú gazdaság" tehát nem a század végén, az informatika hatására kezdett kibontakozni, hanem jóval korábban: az „új hullám" – mint később látni fogjuk – el sem indulhatott volna az új „tudásbázisok" és „tudásszervezetek" nélkül. (Bár valószínűleg annak van igaza, aki szerint a gazdaság mindig is „tudásbázisú" volt.)

e) Lassulás. A múlt század hetvenes éveiben a növekedés lelassult, az amerikai autógyárak profitrátája csökkenni kezdett. Néhány vállalat csődbe ment, megindultak a nagy felvásárlások és összeolvadások, a piac *oligopolisztikussá* vált. A hetvenes és a nyolcvanas évek világszerte a *válságjelenségek* jegyében teltek el.

1973-ban az OPEC országok olajválságot robbantottak ki, ami világosan megmutatta, hogy a világ mennyire függőségi helyzetbe került egy korlátozottan rendelkezésre álló természeti erőforrástól, amelyek közül egyesek a kimerülés határához érkeztek. Az olajválságot általános áremelkedés követte. Egyre több fejlődő ország adósodott el kritikus mértékben. A hatvanas években alacsony volt a munkanélküliségi ráta, a nyolcvanas évek elején a nyugati országokban viszont már 5 és 10% között mozgott.

Bródy András, aki részletesen elemezte a lassulás és az általános rossz hangulat okait, a következőket jósolja a nyolcvanas évek elején: „Ha a beszámolómban kifejtett nézetek és elméletek helytállóak, akkor a következő mintegy húsz évre, tehát az ezredfordulóig a növekedés lassulására, a gazdaság általános stagnálására kell felkészülnünk" ([Bródy 1983] 161. o.). Mélyebb, válságosabb recessziók várhatók – jelzi. Könyvében csak egy-két mondat utal arra, hogy az átlagnál élénkebb mozgás van a mikroelektronikai iparágban.

f) Érettség. A lassulási fázis után az autóipar természetesen nem tűnt el: fejlődésében megjelennek megújulási, belesimulási, együttélési forgatókönyvek. Az iparágat óriásira nőtt cégek uralják, a profitráták alacsonyak, igazán nagy újítás csak ritkán mutatkozik. A súlya nem csökkent, de a következő innovációs hullámot, majd a kilencvenes évek „hosszú fellendülését" már nem ő vezérelte. Az autóipari hullám késői fázisai átfedtek az infokommunikációs hullám kezdetével és felemelkedésével.

3. Az infokommunikációs hullám sajátosságai

Az autóipari hullámot a számítástechnika, az informatika és a távközlés hulláma követte. Történetének első szakasza jól követi a klasszikus mintát, lezártnak azonban még egyáltalán nem tekinthető: a jelen és a közeli jövő tekintetében többféle forgatókönyvben kell gondolkodnunk.

a) Lappangás. A lappangás szakasza az információtechnológiai iparban is meglehetősen hosszúra nyúlt. Ugorjunk nagyokat az időben. Blaise Pascal már 1642-ben megszerkesztett egy számológépet, Charles Babbage pedig 1820 és 1860 között már kifejezetten összetett masinákkal jelentkezett.

A második világháború idején a brit kormány olyan gép kifejlesztésével bízta meg Alan Turinget, a Manchester University matematikusát, amely képes megfejteni a németek Enigma elnevezésű katonai kódját. Már most jegyezzük meg: a fejlett országok államai, felismerve az ügy katonai jelentőségét, kezdettől fogva élénk érdeklődést tanúsítottak az elektronikai, a távközlési majd a számítástechnikai ipar iránt, ami jelentős anyagi támogatásban, nagy állami megrendelésekben is megnyilvánult.

A népszerű történetek ellenére a modern informatika bölcsője nem garázsokban, hanem egyetemi tanszékeken, kutatóhelyeken ringott, úgy is mondhatnánk, hogy az előző hullám idején kialakult, állami és hadiipari támogatást élvező tudásközpontokban. Az ENIAC, EDVAC és UNIVAC gépeket a Pennsylvaniai Egyetemen építették fel. A mai számítógépek alapvető architektúrájának (központi processzor, memóriaeszközök, input-output eszközök) kidolgozása szintén egy egyetemi tudós, Neumann János nevéhez fűződik.

Az információtechnikai innovációs hullám nem indulhatott volna el az államot (pénz és megrendelés), az egyetemeket (tudás) és a vállalati kutató-fejlesztő részlegeket (tudás és üzleti érdek) összekötő újfajta, igen erős hálózat nélkül üzleti célokra teljesen alkalmatlannak látszottak. Az ötvenes évekig ez volt a véleménye az IBM vezetőinek is: piackutatóik azt jelezték, hogy legfeljebb néhány gépet lehetne eladni. Ugorjunk egy picit előre az időben: ugyanígy „lappangott" az Internet is, amely már a hatvanas években is létezett ARPANET néven, a Pentagon által támogatott egyetemi fejlesztésű és használatú hálózatként.

b) Bizonyítás. A számítógépek gyártásának technológiáját sikerült egyre jobban stabilizálni. A gépek kapacitása gyorsan növekedett: az 1946-os ENIAC másodpercenként még csak 45 aritmetikai műveletet tudott elvégezni, az 1965-ben megjelent IBM 360/75-ös viszont már közel másfél milliót. Az ötvenes évek elején az IBM meglepetéssel tapasztalta, hogy 650-es modelljéből 1.800 darab kelt el, pedig a piackutatók csak néhány tucatra jósoltak keresletet. A cég mozgásba lendült és nagygépeivel szép nyereségre tett szert. A gazdaságban a gépeket először üzleti célokra alkalmazták, később viszont egyre gyakoribbak lettek a termelésirányítási, folyamatszabályozási megoldások.

Az IBM a nagygépekre koncentrált. Az első minigéppel a Digital Equipment Corporation rukkolt elő 1963-ban, amit később mikrogépek követtek. Ezek már sokféle dologra voltak alkalmasak, így például megkönnyítették a gyártási folyamatok automatizálását, alapot adva a teljesen automatizált üzem víziójához. A gépekhez speciális szoftvereket és perifériákat készítettek.

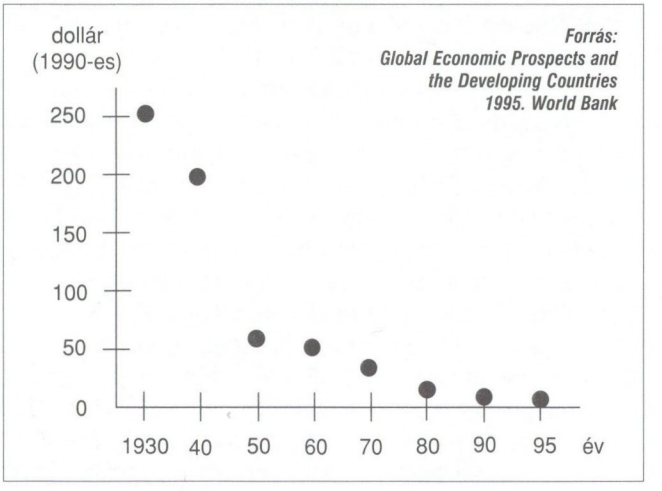
Bebizonyosodott tehát, hogy a szárnyát bontogató informatikai ipar képes életképes termékeket produkálni, amelyek iránt valódi és számottevő üzleti kereslet mutatkozik. A számítógépeket egyre több vállalat vásárolta meg, de a megjelenésük nem kérdőjelezte meg a fordi munka- és vállalatszervezési módszereket, sőt, inkább megerősítette azokat, a centralizált-bürokratizált struktúrákkal együtt. A piacot a nagygépek uralták, amelyeket általában egy külön funkcionális egység (az „elektronikus adatfeldolgozási osztály") használt olyan standard célokra, mint például a bérszámfejtés vagy a számlázás. „Rendszerváltásról" tehát még nincs szó, az igazából csak az Intel mikroprocesszorát használó asztali gépek megjelenésekor kezdődik el.

c) Berobbanás. A nagygépek viszonylag jól belesimultak a fordi értékhálókba és struktúrákba. Legfőbb gyártójuk, az IBM csekély érdeklődést mutatott a kisgépek iránt. Az utóbbiak piacát új vállalkozók lepték el, mint például az Atari, az Apple, a Commodore, a Radio Shack, akik a gépeikhez sokféle szoftvert és perifériát is kínáltak. Az olcsó gépekkel tömegek kezdtek el játszani és dolgozni. Az informatika kitört a vállalati adatközpontokból, egyetemekről és katonai bázisokból és megjelent az emberek mindennapi életében.

Az IBM, késedelmének veszélyeit felismerve, a nyolcvanas évek elején kifejlesztette a maga asztali gépét, standard, a piacon bárki által beszerezhető alkatrészeket, valamint a Microsoft operációs rendszerét és szoftvereit felhasználva. Míg az előző bekezdésben említett új vállalkozások többnyire elvéreztek, a PC gyorsan és sikeresen megindult a piac felső szegmensei felé.

Megvolt tehát a *vezértermék,* ami egy rohamosan csökkenő árú *forrás,* a mikrocsipek felhasználásával állítottak elő. Az utóbbiak kapacitása, Gordon Moore törvényének megfelelően exponenciálisan növekedett. Megjelentek, illetve felzárkóztak a *hordozó, kiegészítő* és *infrastrukturális* iparágak, megkezdődött a távközlés digitalizálása, a számítástechnikával való konvergenciája. A távközlési díjak a hetvenes években már jóval alacsonyabbak voltak a korábbiaknál (1. ábra).

A sikeres innovátorok nagy nyereségre tettek szert, a szektor sok, ma is ismert vezető személyisége ekkor alapozta meg gazdagságát. Az infokommunikációs ipar a hetvenes évek nyomot hangulatában, a lassulás időszakában pozitív jelzéseket adott a világnak: ide gyertek, itt az arany!



1. ábra Egy háromperces New York - London telefonhívás tarifája

d) Növekedés. Az információtechnológiai ipar fénykorának a múlt század kilencvenes évei tekinthetők. Az Egyesült Államokban 1950-ben tizenöt számítógép volt, '55-ben ezer, '65-ben harmincezer, '75-ben százezer, '85-ben pedig már több, mint egymillió. Az ezredfordulón az addig eladott asztali gépek száma meghaladta az egymilliárdot, az Internet felhasználóké pedig a félmilliárdot. Ezekből a számokból látható, hogy a felszállási pont, a „take-off point", amikor a növekedési görbe hirtelen meredekbe vált át, a nyolcvanas évek elejére tehető.

A lendületes növekedéshez még valamire szükség volt. Az informatikai ipar kezdetben *vertikális* struktúrában épült fel: az olyan cégek, mint az IBM, a DEC vagy a Wang mindent maguk állítottak elő a csipektől kezdve a különböző perifériákig, miközben a termékeik nem voltak kompatibilisek egymással. Ezek a „silók" gátolták a fejlődést és a növekedést. Andrew Grove, az Intel magyar származású főnöke egyik könyvében [Grove 1997] leírja, hogyan, milyen feszültségek és problémák közepette alakult át az informatikai ipar vertikálisból *horizontálissá,* miképpen kapott új lendületet az iparág a szakosodástól és az általános kompatibilitástól.

A kilencvenes évtized a töretlen és gyors növekedés jegyében telt el. Ha a statisztikákat nézünk, meredekebb görbéket látunk, mint, az autóipari hullám azonos fázisában. Ennek több oka is van, amelyek mintegy hozzáadódnak a fázis tipikus, fentebb leírt lefutásához. Fontos szerepet játszik a növekedésben a *hálózati jelenség,* ami jól megfigyelhető az infokommunikációs szektorban, ha úgy tetszik, az információ gazdaságtanának fontos törvényei közé tartozik [Shapiro-Varian 1999]. Az évtized során a szektor újabb és újabb technikai innovációs lökéseket kapott, a kilencvenes évek közepén például a könnyen használható böngésző valósággal „berobbantotta" az Internetet [Bőgel 1999].

A gazdaság nemzetközivé, globálissá válása már az előző hullám idején megindult, az újban pedig a vezető iparágak bővülésénél egyre kevésbé kellett földrajzi korlátokkal számolni, ráadásul az információs termékek jó része a kiépített hálózatokon könnyen továbbítható. A növekedést sarkalta az infokommunikációs szektor tipikusnak mondható költségszerkezete is: a kutatásba, fejlesztésbe, hálózatépítésbe fektetett hatalmas összegek megtérülésére csak gyors mennyiségi felfutás esetén van remény. Ne feledkezzünk meg a média szerepéről sem, amelynek rendkívül fontos szerepe volt a közvélemény formálásában [Samuelson 2002].

A világ egyes régióiban technikai, történelmi, politikai és egyéb adottságok miatt a növekedés eltérő méretű volt. A világgazdaság motorja minden bizonnyal az Egyesült Államok volt, ahol a kilencvenes évek második felében világosan kimutathatóan az infokommunikációs szektor volt a látványos növekedés (1. táblázat) forrása.

Az információs szektorba rengeteg tőke áramlott, a vállalatok beruházásaiban és a lakosság kiadásaiban egyre nagyobb szerepet kaptak az információtechnikai eszközök és szolgáltatások, hardvert, szoftvert és távközlést egyaránt ideértve. Kialakult az „infokommunikációs nagyipar", az áru- és tőkepiacon domináns pozíciót szereztek a nagy számítógép- és szoftvergyárak, Internet szolgáltatók és távközlési cégek.

	1991-1995	1995-2000
A GDP évi átlagos növekedése (%)	3,0	4,3
A termelékenység évi átlagos növekedése (%)	1,7	2,8
Átlagos munkanélküliségi ráta (%)	6,6	4,8
Évi átlagos infláció (%)	3,3	2,3

Forrás: US Department of Commerce, 2001. március

1. táblázat Az Egyesült Államok gazdasági adatai

A következő kérdés az, hogy a „szabályszerűen" (bár egyedi színekkel) kibontakozó információtechnológiai innovációs hullám hozott e magával „rendszerváltást", és ha igen, milyen természetűt. A tisztánlátást nehezíti a kilencvenes évtized második felében kibontakozó *Internet-mánia* és a vele együtt járó tőzsdei „léggömb", annak minden kapcsolódó jelenségével és tünetével. Ebben az időszakban a „normális" fejlődésbe irracionális elemek vegyültek – bár, mint korában láttuk, ez nem ritkaság ebben a szakaszban, az alkalmi irracionalitás a dolgok normális menetéhez tartozik.

A számítástechnikai, távközlési és főleg az internetes cégek piaci értékelése elszakadt a realitásoktól. A sajtó megtelt a „megvilágosodás" jegyében született, szeizmikus változásokat jövendölő, látványos jövőképeket felvázoló cikkekkel, azt az érzetet keltve az olvasóban, hogy ha nem siet azonnal valamilyen újdonságot megvásárolni, ha nem szervezi át azonnal az alapoktól kezdve a vállalatát, ha nem száll be most rögtön az elektronikus üzletbe, ha nem veszi meg valamelyik frissen alakult internetes cég nyomdából éppen kikerült részvényeit, akkor menthetetlenül lemarad a versenyben. Egyes cégek és személyiségek körül valóságos hőskultusz alakult ki.

A józanabb hangok [pl. Mandel 2000] elvesztek az általános lelkesedésben. Az okokat és a következményeket már többen elemezték: az események nagyjából úgy futottak le, ahogy azt korábbi idők hasonló jelenségeit vizsgálva Galbraith [1997] és Kindleberger [2000] leírták. A „dotcom mánia" (a 2000. év technikai problémája miatt előrehozott beruházásokkal tetézve) mindenesetre egy „púpot" tett a statisztikai görbékre és elhomályosította az illúziók, a mítoszok és a realitások közötti határvonalat.

Tegyük fel ismét a kérdést: hozott-e „rendszerváltást" az információtechnológiai innovációs hullám? A válaszunk az, hogy *igen,* de a változások tartalma, iránya és lezártsága tekintetében sok a bizonytalanság: rendszerbeli változások kétségtelenül történtek és történtek, de nehéz megmondani, hogy közülük melyek lesznek tartósak és mélyek, és melyek bizonyulnak átmenetinek vagy kifejezetten illuzórikusnak.

4. Változások a vállalatokban

Vegyük először a *vállalatokat,* és nézzük meg, a technológiai innovációk hatására történtek-e változások a fordi vállalatmodellben. Könnyen megállapíthatjuk, hogy az infokommunikációs szektorban kétségtelenül születtek új

vagy újszerű *üzleti modellek,* olyanok, mint például „portál", „elektronikus piactér", „kereslet-aggregátor", „tartalomszolgáltató" [Weill-Vitale 2001].

Témánk szempontjából azonban nem ezek az igazán érdekesek, hanem a munkamegosztásban és a koordinációban bekövetkezett változások. Ha áttekintjük a vonatkozó szakirodalmat (lásd például [Kocsis-Szabó 2000]; [Drucker 2002]; [Ranadivé 1999]; [The Economist 2002]), nagyjából a következő képet kapjuk az *elektronizált* (sokféle informatikai eszközt és alkalmazást használó), *integrált* (informatikai alkalmazásait folyamatok, projektek mentén integráló), *kiterjesztett* (partnereivel elektronikus eszközökkel összekötött) és *valós idejű* (késedelem nélküli, „real time" rendszereket működtető) vállalat „ideáltípusáról":

a) Szervezeti rendszere hálózatos jellegű: különböző munkacsoportok közvetlenül kommunikálnak és kooperálnak egymással.

b) A vállalat maga is egy vagy több hálózat részeként működik A vezetés figyelme ennek következtében kifelé irányul, a külső kapcsolatok, szövetségi rendszerek, partneri hálózatok építése az egyik legfontosabb vezetői feladattá válik.

c) A vállalat elektronikus értékesítési csatornái a világ bármely pontjáról elérhetők, erőforrásait onnan szerzi be, ahol az számára a legkedvezőbb.

d) Az önellátás nem erény: csak azokat a funkciókat építi ki amelyeket hatékonyabban, olcsóbban tud ellátni másoknál, vagy amelyek valamilyen ellenőrzési vagy biztonsági megfontolásból különlegesen fontosak.

e) A működés rugalmas, a szerepek gyakran átrendeződnek, a csoportok, funkciók, döntési szintek közötti határvonalak nem élesek.

A döntési rendszer decentralizált, amit többféle tényező tesz szükségessé, illetve lehetségessé: a szükséges információk bárhová könnyen, gyorsan és hiánytalanul eljuttathatók, az operatív szinten jól képzett szakértők dolgoznak, az ellenőrzés hatékony és gyors. A szervezet lapos, kevés vezetési szint van, a középvezetők hagyományos továbbító-összesítő-jelentéstevő munkáját informatikai alkalmazások helyettesítik. A vezetői szerepek közül háttérbe szorul a menedzseri, és egyre fontosabbá válik a felkészítői, támogatói (angol szakkifejezéssel: *coach*) szerepkör.

A tervezés alapvetően nem „felülről lefelé", hanem „alulról felfelé" irányuló folyamat.

a) A termelésre növekvő mértékben jellemző a tömeges testreszabás: a rugalmas rendszerek jól megválasztott komponensekből sokféle változatot tudnak felépíteni, az ügyfél igényeihez igazodva.

b) A „fizikai" eszközök (épület, gép, nyersanyag stb.) mellett egyre növekszik az információ és a tudás jelentősége: a többféle összetevőből álló „intellektuális tőke" a vállalati vagyon fontos részeként jelenik meg.

c) Az alkalmazottaknak a szervezeten belül nincs állandó, stabil helye: gyakran átcsoportosítják őket, különböző, változó összetételű csapatokban dolgoznak. Elektronikus eszközeikkel bárhol, bármikor rácsatlakozhatnak a vállalat hálózatára, megkaphatják a szükséges információkat és munkához láthatnak.

d) Készleteit tekintve a vállalat nem hetekben vagy hónapokban, hanem órákban és percekben gondolkodik: a készletek nagysága minimális, a beszerzés just-in-time rendszerű.

Az könnyen belátható, hogy ez a modell erősen különbözik a huszadik században kialakult centralizálódásra és bürokratizálódásra hajlamos, az irányítást és a végrehajtást szétválasztó, horizontálisan funkciókból, vertikálisan irányítási szintekből álló vállalattípustól. (Ha a régebbi szakirodalomban kutakodunk, leginkább talán a Mintzberg [1979] által leírt, akkoriban különlegességnek számító „adhokráciához" hasonlít, aminek a technológiai fejlődés következtében „eljött az ideje".). Mintákként leginkább a Toyotát, a Cisco-t és a Dellt szokás emlegetni: az elsőt a tömeges testre szabás és az „elektronizált lean management" úttörője, a második 1997-ben önmagában adta az USA elektronikus kereskedelmi forgalmának egyharmadát, a harmadik pedig a közvetítőket kikapcsoló, a veszteségeket minimalizáló elektronikus üzleti modell megtestesítője.

A kérdés csak az, hogy a valóságos vállalatok mennyire közelítik meg a leírt ideáltípust. E tekintetben a kép igen vegyes. Nem kizárható, hogy a típus olyan vonzási pont, amit a vállalatok egyre inkább megközelítenek, csak nehezen és keservesen tudják hozzá igazítani rugalmatlan kultúrájukat, de az is lehet, hogy a fejlődés más irányt vesz majd. Az informatikában a *teljes centralizálás* és a *teljes decentralizálás* lehetősége egyaránt benne rejlik.

5. Társadalmi, politikai, intézményi változások

Az információs technológia fejlődésének társadalmi következményeit tárgyaló munkák [lásd pl. Dyson 1998] visszatérő, vitathatatlan fontosságú témái az alábbiak:

a) Közösségek. A modern távközlési eszközök hozzájárulhatnak újfajta, határok nélküli közösségek rugalmas szerveződéséhez, miközben elősegíthetik mások bomlását. Az utóbbi folyamat lappangó, mélységét, irányait nehéz kiszámítani, és súlyos veszélyeket rejt magában. A technológia a tartalom szempontjából semleges. A modernizálás, áramvonalasítás, állandó „reengineering" (radikális újraszervezés) miatt szétbomló munkahelyi közösségek kapcsolatkereső „társas lény" embere a modern kommunikációs eszközök segítésével gyorsan beszervezhető másfajta közösségekbe: hobbikörökbe, szektákba, pártokba, mozgalmakba stb.

Tapasztalatokból és beszámolókból arra lehet következtetni, hogy számos informatikai, vagy internetes közösség sajátos kulturális jegyeket, rétegződési mintákat mutat [Lessard-Baldwin 2000], amelyek különböző (családi, munkahelyi stb.) csatornákon keresztül átterjedhetnek más területekre is.

b) Kormányzás és politika, az állam szerepe. Heves viták dúlnak arról, hogy az államnak kell-e, szabad-e beleavatkoznia az elektronikus gazdaság és az azt megalapozó infokommunikációs szektor fejlődésébe, és ha igen, hogyan. Az állami kiadásoknak a GDP-hez viszonyított aránya szinte mindenütt növekedett.

Az „információs társadalom" korszaka viszont más nézetekkel köszönt be a hetvenes években. Az elmúlt évszázad utolsó két évtizedében az vált uralkodó elképzeléssé, hogy az állam szerepét vissza kell szorítani, az adók és az állami kiadások mértékét csökkenteni kell. Az állami tulajdon és a központi tervezés rendszerét érdekes módon nemcsak konzervatív és neo-liberális politikai csoportok vetették el, hanem a szocialista és szociáldemokrata pártok is, a szabad versenyt állítva azok helyébe. A dereguláció, a piacok liberalizálása, a magántulajdon megerősítése minden bizonnyal fontos szerepet játszott az új technológia terjedésében. (Gondoljunk csak a távközlési szektorra.)

Maga az Internet a dereguláció, az állam nélküli szerveződés szimbólumává vált. Csak nagyon halvány elképzeléseink vannak arról, hogy milyen lesz a társadalmi, politikai és kulturális élet az „információs társadalom" korszakában. Az államokat mindenesetre sokféle – gazdaságpolitikusi, beruházói, adószedői, szabályozói, felhasználói (elektronikus kormányzás, „elektronikus demokrácia") stb. – szerepkörben mutatnak élénk érdeklődést az elektronikus kereskedelem és az infokommunikációs szektor iránt. Egyes országokban az utóbbi képviselői sikeresen és meggyőzően lobbiztak az államnál, az Egyesült Államokban például Al Gore alelnök határozottan támogatta az információs „szupersztrádák" építésének programját, de az Európai Uniónak és számos országnak is van „e-stratégiája". Az utóbbiakhoz egyes elmaradottabb országok – például India [Bőgel 2001] – nagy reményeket fűznek.

c) Oktatás. Az elmúlt években bebizonyosodott, hogy az információtechnológiai újdonságok terjedésének felgyorsulására csak akkor lehet számítani, ha az egyik legfontosabb input, a technológia használatára, fejlesztésére képes szakemberek tömege is rendelkezésre áll, ehhez pedig jelentős átalakulások kellenek az oktatás tartalmában és módszereiben. Világosan látszik, hogy az elektronikus rendszerek terjedésének, a fejlett elektronikus szolgáltatások tömeges igénybevételének fontos feltétele a megfelelő „számítógépes műveltséggel" rendelkező emberek számának növekedése. Az elektronizálás szemmel láthatóan az oktatási módszereket is elérte: a szaporodó internetes kurzusok az e-világ sajátos, és fölöttébb ígéretes termékeinek tekinthetők, az Internet használata a házi feladatok megoldásánál mindennapos dolognak számít. A képzettség általános szintje emelkedett, az Egyesült Államokban például a felnőttek több mint fele rendelkezik valamilyen felsőfokú végzettséggel.

d) Szegénység és munkanélküliség. Az Egyesült Államokban, ahol a kilencvenes években leggyorsabban fejlődött az információtechnológiai szektor, a korábbi időszakhoz képest, az évtized elejének leépítési hullámát követően, számottevő mértékben csökkent a munkanélküliség (lásd az 1. táblázatot). Közvetlenül a tőzsdei léggömb kipukkanása előtt a foglalkoztatás gyakorlatilag teljesnek volt tekinthető, sőt, egyes munkakörökben kifejezett hiány mutatkozott. A hullám vezető iparágai tehát felszívták a rendelkezésre álló munkaerőt.

Érdemes belenézni a részletekbe is, hiszen megállapítható például, hogy az alkalmi létszámleépítések nem a kékgallérosokat fenyegették igazán, hanem sokkal inkább azokat, akiknek a munkája jól algoritmizálható – tehát számítógépesíthető – volt, függetlenül a szükséges tudás színvonalától. A jövedelmi statisztikákon az is jól látszik, hogy a bérolló egyre jobban kinyílt a jól képzett informatikai, távközlési szakemberek javára, bár ezen a csoporton belül igen nagy volt a differenciálódás [Lessard-Baldwin 2000].

Más országokban ezek az összefüggések kevésbé voltak markánsak. Az mindenesetre látszik, hogy az USA-ban a hatékonyság növekedésének nyertesei nem a befektetők voltak, hanem az alkalmazottak; a recesszió beköszöntével – korábbi hasonló eseményekkel ellentétben – egyebek mellett ezért nem csökkent számottevően a lakossági fogyasztás.

e) Szellemi tulajdon védelme. Az információtechnikai hullám egyik legérdekesebb jogi kérdéséről van szó. A szellemi termékek – kéziratok, zeneszámok, szoftverek stb. – másolásának és továbbításának költségei összezsugorodtak, a továbbítási, terjesztési hálózatok nagyrészt ellenőrizetlenek. A feszültség jelei jól megfigyelhetők például a hanghordozók piacán, ahol a hagyományos termékeket és terjesztési csatornákat egyre súlyosabb csapások érik. A probléma a levegőben lebeg, jogi, kulturális és üzleti következményei egyelőre beláthatatlanok.

f) Biztonság. Ezt a kérdést nemcsak a modern technológiával közvetlenül és különféle áttételeken keresztül egyaránt kapcsolatba hozható New York-i terrortámadás hozta előtérbe. (A terrorista akcióknak egyebek között a tömegkommunikációs lehetőségek adnak „értelmet", amelyek hatalmas tömegek számára teszik láthatóvá, szinte átélhetővé az eseményeket, biztosítják az elkövetők számára fontos tömeges lélektani hatást. A terrorista csoportok tagjai az Interneten keresztül és mobiltelefonon üzennek egymásnak, honlapokra teszik fel a közleményeiket, elektronikus csatornákon mozgatják a pénzt.)

Az utóbbi néhány évben látványosan elszaporodott a számítógépes „fehérgalléros" bűnözés, ami szemlátomást felkészületlenül érte a jogrendszert. Egyes államok már annyira függőségi helyzetbe kerültek a saját technológiai rendszereiktől, hogy komolyan fel kell készülniük egy „számítógépes támadásra".

g) Kultúra. Az információs technológia (számítógép, televízió, Internet, digitális játékok stb.) hatása látványos és egyértelmű. A fejlődésben pozitív és negatív tendenciák egyaránt jelentkeznek, néha kifejezetten szélsőséges formákban is. Új művészeti ágak születnek (pl. számítógépes grafika), a számítógépesítés virtuális világot

teremt körülöttünk. Kitágultak a publikációs és promóciós lehetőségek, a „megmutatkozás" egyre könnyebbé válik, ugyanakkor egyre nehezebb elválasztani az értékest az értéktelentől. Jól megfigyelhető jelenség (elég csak a sok tévécsatornára gondolni) a szellemi tartalom hígulása. Az angol nyelv térhódítása megállíthatatlannak látszik, ami domináns pozíciót biztosít az angolszász országok kultúrájának.

Mindezekből a kiragadott jelenségekből is jól látható, hogy az információs technológiai hullám alaposan megmozgatta a gazdaság és a társadalom számos szeletét, valóban beindultak fontos és alapvető változási folyamatok, a „rendszerváltás" azonban még korántsem teljes és az irányai is kiszámíthatatlanok.

6. Lassulás és érettség (?)

A fejezetcímben a két utolsó fázis összevonásával és a végére tett kérdőjellel azt igyekszünk érzékeltetni, hogy a következőkben inkább csak találgatunk: a kép nem tiszta, ellentmondásos, a pontosabb elemzéshez hiányoznak a történelmi távlatok. Kétségtelen tény, hogy az új évezred legelején a fejlett országokban a lassulás és a recesszió jelei mutatkoznak, azt azonban aligha lehet egyértelműen megmondani, hogy az események vajon a technológiai hullámok fentebb leírt menetét követik-e, vagy valami másról van szó.

Tudjuk jól, hogy a korábbi nagy hullámokban is voltak kisebbek, 1950 és 1972 között például négy „gyors" és öt „lassú" szakasz volt. Az is kétségtelen, hogy a mostani lassulásban fontos szerepet játszik az infokommunikációs szektor (elég ránézni vállalati jelentésekre és a tőzsdei statisztikákra), azt azonban nem tudjuk, hogy a problémái mennyire tartósak.

A következőkben – állásfoglalás nélkül, nem kizárva egyéb magyarázatokat és jövendöléseket sem – a jelenlegi helyzet két markáns értelmezési lehetőségét foglaljuk össze.

A) Forgatókönyv: benne vagyunk az információtechnológiai hullám lassulási és érettségi fázisában, a világ eseményei ezt jelzik, a további menetük az 1. fejezet megfelelő részeiben leírtakhoz fog igazodni. A revolúciós technikai változások kora lezárult, egyes nagy hévvel beharangozott újdonságok hűvös fogadtatásra találtak. Véget ért a kétszámjegyű növekedés korszaka, a vezető szektoron csődhullám söpört végig, rengeteg cég megszűnt, mindennaposak a felvásárlások és az összeolvadások.

Az iparág konszolidálódik, rövidesen néhány nagy cég fogja uralni az oligopolisztikus piacot. A távközlési és informatikai cégek rengeteg embert elbocsátottak, munkaerő iránt kereslet legfeljebb néhány speciális területen mutatkozik.

A szektor vállalatainál a korábbi töredékére csökkent a nyereséghányad, különösen az értéklánc alsó szegmenseiben, ahol a termékek egyre inkább differenciálatlan tömegcikkekké válnak. A hullám vezértermékén, az asztali számítógépeken már csak a legnagyobb, legáramvonalasabb, a termelésüket olcsó ázsiai országokba telepítő cégek tudnak valami hasznot csinálni, a kereslet alakulásában pedig visszaesések mutatkoznak. A mobiltelefonok piaca telítődik, már itt is jól láthatók a forgalom csökkenésének jelei. A vállalatok jó része túl van a nagy informatikai beruházásokon, a jövőben már korántsem fog annyit költeni számítógépesítésre, mint eddig: a csökkenés jól látszik a statisztikákon.

A visszaesés sokukat váratlanul érte (a Nokia értékesítésének növekedése 2000-ben még megközelítette a 60%-ot, 2001-ben viszont már tíz százalék alatt maradt.) döntéseik az aranykorhoz igazodtak, amivel súlyos hibákat követtek el. Volt, aki megúszta a készletei ideiglenes felhalmozódásával (lásd pl. Cisco), mások viszont elképesztő mértékben eladósodtak, mint például a távközlési szektor krémje (2. táblázat).

Vállalat	Adósság/piaci érték (%)
France Telecom	152
Deutsche Telekom	101
Nippon Telephone	68
AT&T	59
Sprint PCS	58
British Telecom	53

Forrás: Newsweek, 2002. június 10., 52. oldal

2. táblázat Távközlési cégek eladósodottsága (2002. június)

A hullámhoz tartozó „rendszerváltás" megkezdődött, de messzire már nem fog jutni. Az elkövetkező időszakban a lassabban mozgó, rugalmatlanabb elemek (jog, kultúra stb.) felzárkóznak a technológiához, de az impulzusok gyengülnek, nagy fordulatokra már nem lehet számítani.

Az információtechnológiai szektort persze nem kell különösebben félteni: a jelek arra vallanak, hogy sikeresen együtt fog élni a következő innovációs hullámmal. Lehet, hogy most az egészségügy és a biotechnológia hulláma következik, vagy esetleg az energia kerül a középpontba, egy biztos: az új hullám cégeinek nagy szüksége lesz informatikára.

A szektor érzi ezt a belesimulási tendenciát, ezért jelzik egyre többen, hogy a szakértőinek „vertikális", adott szektorokhoz, iparágakhoz kapcsolódó tudásra van szükségük. A információtechnológiai cégek feleslegessé vált munkaereje a „régi gazdaság" vállalataihoz áramlik át, aminek kedvező hatása lesz az utóbbiakra A talpon maradó nagy informatikai cégek amolyan közszolgáltató vállalatok lesznek, akik nélkül nem lehet élni, de nem körülöttük forog a világ.

B) Forgatókönyv: a fejlődés kétségtelenül lassul, de az információtechnológiai hullám még a növekedési fázisban van és jó darabig abban is marad. A jelenlegi problémákat a nagy trendre rárakódott „púp", az internetes láz okozza, ami egyébként betöltötte a maga pozitív szerepét: rengeteg tőkét és tehetséget vonzott a szektorba, sok ötletet próbáltak ki, számtalan virág szökkent szárba, gyorsan épült az infrastruktúra.

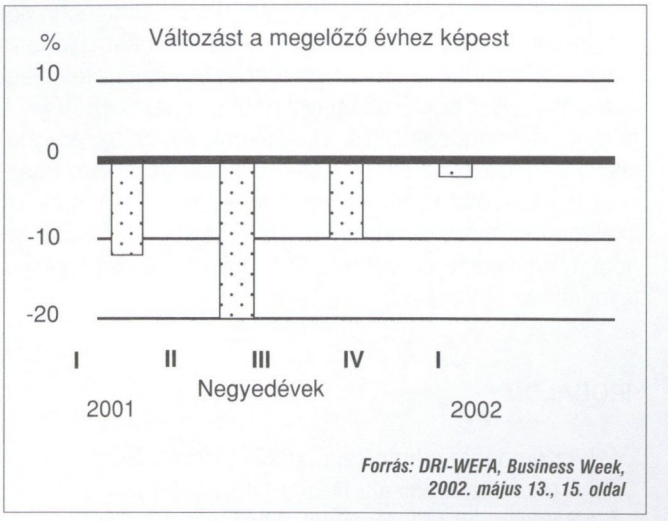
A mánia véget ért, a 2000. év problémájának utórezgései elcsendesednek, a visszaesés átmeneti, a vezérszektor rövidesen visszazökken a normális kerékvágásba. A növekedési görbék már nem lesznek exponenciálisak, de még hosszú ideig meredeken emelkednek majd. Kétségtelen, hogy megjelentek olyan új, feltörekvő innovációs területek, mint például a genetika és a nanotechnológia, de ezek nem indítanak új hullámot, hanem inkább a mostani további emelkedését segítik, meghosszabbítják a növekedési szakaszt.

A technikai innováció tartalékai még egyáltalán nem merültek ki. Moore törvénye a chipek kapacitásának növekedéséről még hosszú ideig érvényben lesz. Az Internet felhasználóinak száma töretlenül növekszik, elég ránézni például a friss európai statisztikákra. A mobil technológiák terjedését jelenleg gátolja ugyan a távközlési cégek eladósodása és a tartalom hiánya, de ezek átmeneti jelenségek, hamarosan jönnek a forradalmi változások. A „real time" világnak még legfeljebb a küszöbénél járunk. A képzettségi szint általános emelkedése, a generációk cserélődése némi késéssel ugyan, de meghozza azt a fejlesztői és felhasználó tömeget, amely élni tud az új technológiákkal, ki tudja használni az abban rejlő potenciált.

Határozott optimizmusra adnak alapot a termelékenységi adatok. Ez a rendkívül fontos mutató [Bródy 1983] az Egyesült Államokban a kilencvenes években évente átlagosan fél százalékkal többel növekedett, mint a megelőző tíz évben. 1995 ás 2000 között a növekedése átlagosan 2,5% volt, 2000-ben 3,3%, 2001. negyedik negyedévében 5,2%. A termelékenység még akkor is növekedett, amikor az output csökkent, és ilyen az elmúlt fél évszázad recesszióiban nem fordult elő.

Ezek az emelkedő számok azt jelzik, hogy az információs technológia most kezd igazán hatást gyakorolni a vállalatokra, most mutatja meg igazán, hogy mire képes. Ha a tőzsdei trendekről lehámozzuk az „internetes púpot" láthatjuk, hogy az informatikával megerősített szektorok (pl. pénzügyi szolgáltatások, egészségügy) eredményei 1995 és 2002 között igen szépen növekedtek [Mandel 2002]. Az informatikai cégeknek persze nem árt megtanulniuk, hogy tartós sikerük titka a hatékonyság növelése ügyfeleiknél.

Az emelkedő termelékenység pozitív üzenetet küld a világnak: költsetek információs technológiára, mert megéri! A lehetőségek óriásiak: az informatika hazájában, az Egyesült Államokban a vállalatoknak még csak 60%-a vezetett be internetes üzleti megoldásokat, és ezek nagy részének a telepítése sincs még befejezve, más országokban pedig még szélesebbek a távlatok. Az elektronikus kereskedelem egyelőre pici töredékét adja a világ forgalmának. Lehet, hogy a heves verseny miatt a vállalatok nem tudják realizálni a hatékonyság növeléséből származó többletértéket, azt mégis érzik, hogy az információs technológia nélkül végzetesen lemaradhatnak. Az informatikára fordított kiadások valóban csökkentek, de a görbék ismét felfelé kapaszkodnak (2. ábra). A rugalmatlan vállalati struktúrák nehezen bár, de megváltoznak, és akkor minden új lendületet kap.



2. ábra Informatikai berendezések vásárlására fordított beruházások nagyságának változása (USA)

Mivel a technológiai innováció folytatódik, a „rendszerváltás" sem áll le. A munkaerővel kapcsolatos vállalati költségek arányának növekedése (az USA-ban ez a szám 2002-ben rekordszintre, 87%-ra emelkedett) azt jelzi, hogy a legfontosabb erőforrás valóban az emberi tudás lett. Az oktatás, a kultúra, a társadalmi élet fejlődése követni fogja a technológiáét, az információs társadalommal kapcsolatos jövendölések nem utópisztikusak.

A világ információs vérkeringésébe bekapcsolódó elmaradott országok új esélyt kapnak a felzárkózásra: világosan látható, hogy például az „ázsiai tigrisek" ismét felgyorsult fejlődésében milyen nagy szerepe van az információs technológiának.

Összefoglalás

Az információs technológia eddigi története viszonylag jól illeszkedik az innovációs ciklusok e cikk elején leírt modelljéhez.

A korábbi hullámokra jellemző sajátosságokat a *berobbanás* és a *növekedés* fázisában is jól megfigyelhettük, de mellettük felbukkantak újfajta vonások is. Látható például, hogy

- a növekedési görbék a hálózati hatásoknak, a modern tömegkommunikációnak és egyéb tényezőknek köszönhetően igen meredekek, a technológiai újdonságok elfogadása gyorsabb, mint a korábbi hullámokban;
- a hullám szinte kezdettől fogva globális;
- a növekedés korlátjai nem anyagi jellegűek: a legfontosabb erőforrás a tudás, ami adott időszakokban szintén korlátozottan áll rendelkezésre, de egyébként más természetű, mint az anyagi jellegű források;
- a berobbanás és a növekedés fázisában, más hullámokhoz hasonlóan, irracionális elemek, mániák és divatok is megjelennek, az általuk okozott „kiegészítő hullám" több tényező összjátéka következtében igen meredeken emelkedett föl és süllyedt le.

Nyugodtan mondhatjuk, hogy az információs technológia „rendszerváltást" idézett elő, ez a folyamat azonban még nem zárult le, kimenetelei többesélyesek. A jelenlegi lassulási jelenségek többféle módon értelmezhetők. A helyzetértelmezésektől és az ezekből levezetett prognózisoktól függően az információs technológiai ciklus hosszával kapcsolatos várakozásaink eltérőek lehetnek. A szektornak mindenesetre igen jó esélyei vannak arra, hogy a következő ciklusba „belesimuljon", együtt éljen és fejlődjön az új vezető iparágakkal.

IRODALOM

[1] Az emberiség krónikája (1990) Officina Nova
[2] A technika krónikája (1991) Officina Nova
[3] Baldwin, N. (2001): Henry Ford and the Jews. Public Affairs
[4] Beevor, A. (2002): The Fall of Berlin. Viking Press
[5] Benedek Zoltán (2002): Nyakkendős bányászok. CEO, április és június
[6] Berend T. Iván (1982): Válságos évtizedek. Gondolat Könyvkiadó
[7] Bőgel György (1999): Miért a Netscape? Vezetéstudomány, szeptember
[8] Bőgel György (2001): Buddha mosolyog. Az indiai szoftveripar sikereiről. CEO, október
[9] Bródy András (1983): Lassuló idő. Közgazdasági és Jogi Könyvkiadó
[10] Chandler, A. (1969): Strategy and Strucure. MIT Press
[11] Christensen, C. (1997): The Innovator's Dilemma. Harvard Business School Press
[12] Christensen, C. (1999): Innovation and the General Manager. Irwin/McGraw-Hill
[13] Dertouzos et al. szerk. (1989): Made in America. MIT Press
[14] Drucker, P. (2002): Managing in the Next Society. St. Martin's Press
[15] Dyson, E. (1998): Release 2.1. Broadway Books
[16] Freeman, C. – Louca, F. (2002): As Time Goes by. Oxford University Press
[17] Ford H. (1989): Today and Tomorrow. Productivity Pr
[18] Galbraith, J. (1997): The Great Crash 1929. Mariner Books
[19] Galbraith, J. (1978): The New Industrial State. Houghton Mifflin
[20] Gates, B. (1995): The Road Ahead. Viking
[21] Goldenberg, B. (2002): CRM Automation. Prentice Hall
[22] Greiner, L. (1995): Evolution and Revolution as Organizations Grow. Harvard Business Review, február
[23] Greguss Ferenc (1985): Élhetetlen feltalálók, halhatatlan találmányok. Móra Könyvkiadó
[24] Grove, A. (1997): Only the Paranoid Survive. Harper Collins Business
[25] Heizer, J. – Render, B. (2001): Operations Management. Prentice Hall
[26] Kerekes Tibor (2002): Biztonságos (?) hálózatok. Alma Mater, Budapesti Műszaki és gazdaságtudományi Egyetem, augusztus
[27] Kindleberger, C. (2000): Manias, Panics, and Crashes. John Wiley & Sons
[28] Kocsis Éva – Szabó Katalin (2000): A posztmodern vállalat. Oktatási Minisztérium
[29] Kuhn, T. (1996): The Structure of Scientific Revolutions. University of Chicago Press
[30] B. – Baldwin, S. (2000): NetSlaves. McGraw-Hill
[31] Lowry Miller, K. (2002): The Giants Stumble. Newsweek, július 8.
[32] Mandel, M. (2000): The Coming Internet Depression. Basic Books
[33] Mandel, M. (2002): The Boon behind the Bubble. Business Week, 2002. július 15.
[34] Michaels, E. – Handfield-Jones, H. – Axelrod, B. (2001): The War for Talent. Harvard Business School Press
[35] Mintzberg, H. (1979): The Structuring of Organizations. Prentice-Hall
[36] Ono, T. (1988): Toyota Production System. Productivity Pr
[37] Perez, C. (2000): Technological Revolutions, Paradigm Shifts and Socio-Institutional Change. In E. Reinert szerk.: Evolutionary Economics and Income Equality. Aldershot: Edward Elgar
[38] Ranadivé, V. (1999): The Power of Now. Osborne McGraw-Hill
[39] Samuelson, R. (2002): The Media's Heavy Hand. Newsweek, július 1.
[40] Schein, E. (1997): Organizational Culture and Leadership. Jossey-Bass
[41] Schultz, T. (1971): Beruházás az emberi tőkébe. Közgazdasági és Jogi Könyvkiadó
[42] Schumpeter, A. (1980): A gazdasági fejlődés elmélete. Közgazdasági és Jogi Könyvkiadó
[43] Shapiro, C. – Varian, H. (1999): Information Rules. Harvard Business School Press
[44] Polónyi István – Tímár János (2001): Tudásgyár vagy papírgyár? Új Mandátum
[45] Weill, P. – Vitale, M. (2001): Place to Space. Harvard Business School

A cikk első, bővebb változata a Debreceni Egyetem Közgazdaságtudományi Karának *Competitio* c. házi folyóiratában jelent meg.

RC polifázisú szűrők zajtényezőjének minimalizálása

DR. LADVÁNSZKY JÁNOS, DR. GERHARD SCHULTES

austriamicrosystems AG
Janos.Ladvanszky@austriamicrosystems.com

Bebizonyítjuk, hogy az RC polifázisú szűrők oldalsáv-elnyomása független a generátor- és terhelő impedanciáktól. Ez a tulajdonság tetszőleges számú fokozat és a fokozatok közötti tetszőleges elhangolás esetén érvényes. Következésképpen a zajtényező minimalizálása az oldalsáv-elnyomás beállításától függetlenül végezhető el. Passzív kétkapuk zajtényezőjére két kifejezést adunk meg, és az egyik felhasználásával a polifázisú szűrők zajtényezőjét minimalizáljuk. A zajtényező erősen függ a generátor ellenállásától és kapacitásától. Megadjuk az n fokozatú polifázisú szűrők zajtényezőjének alsó korlátját. 25 dB-nél kisebb oldalsáv-elnyomású, két fokozatú polifázisú szűrő esetén a zajtényező minimumát 10,18 dB-nek találtuk.

I. Bevezetés

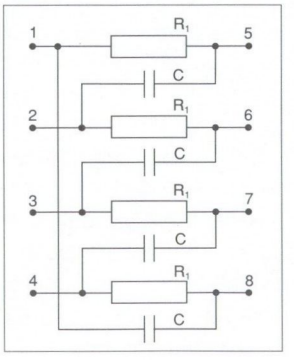
Távközlési rendszerekben széles körben alkalmaznak RC polifázisú szűrőket (PFSZ) [1]. Tipikus felhasználási területük a modulálásnál és demodulálásnál van az egy oldalsávos (SSB) jelek rendszerében. Egyszerűségük miatt igen népszerűek az alkalmazás-orientált integrált áramkörökben.

A PFSZ zaját kvalitatívan vizsgálták [2]-ben, ahol a különböző fokozatok ellenállásainak viszonyát tárgyalják a zajtényező minimalizálása céljából. A PFSZ-ről szóló úttörő cikk [3], a struktúra származtatását és az oldalsáv-kioltás jelenségét részletesen tárgyalja. Egy vevőkészülékben a PFSZ a keverő fokozatot követi, ezért a PFSZ hozzájárulása a rendszer teljes zajához jelentős lehet. Emiatt fontos a PFSZ zajának minimalizálása. Ennek ellenére nem ismeretes olyan publikáció, amely a PFSZ minimális zajtényezőhöz tartozó lezárásait megadná.

Ebben a cikkben megmutatjuk, hogy egy RC PFSZ oldalsáv-elnyomása független a generátor- és terhelő impedanciáktól, teljesen általános feltételek mellett. Ennek a tulajdonságnak következtében a zajtényezőt az oldalsáv-elnyomástól függetlenül lehet minimalizálni. Passzív kétkapuk zajtényezőjére két kifejezést adunk meg, és az egyiket esetünkre alkalmazzuk. Megmutatjuk, hogy az RC PFSZ zajtényezője erősen függ a generátor ellenállásától és kapacitásától. Példaként két fokozatú, 25dB-nél kisebb oldalsáv-elnyomásra tervezett RC PFSZ zajtényezőjét minimalizáljuk.

II. RC polifázisú transzfer függvényei

Az egy fokozatú RC PFSZ az *1. ábrán* látható 8 pólusú struktúra [3].

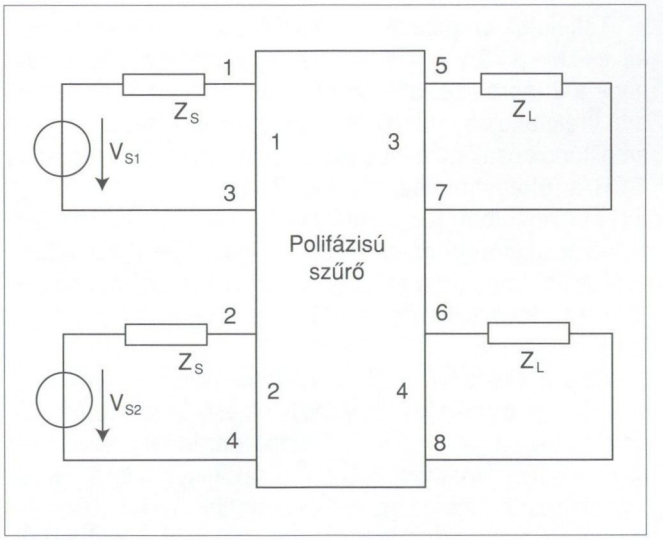


1. ábra. Egy fokozatú RC PFSZ

Az 1. ábrán minden ellenállás és kapacitás egyforma. Több fokozat esetén az 5-6-7-8 pólusok rendre a következő fokozat 1-2-3-4 pólusához vannak kapcsolva. A különböző fokozatok ellenállásai és kapacitásai nem szükségképpen egyformák.

Ebben a cikkben az általánosság csorbítása nélkül azt az esetet vizsgáljuk, melyben minden kapacitás egyforma és csak az egymást követő fokozatok ellenállásai különbözhetnek egymástól.

A bemeneti és kimeneti kapuk a *2. ábrán* látható módon vannak konfigurálva, a pólusok zárójelben: 1 (1,3), 2 (2,4), 3 (5,7) és 4 (6,8). Így első feladatunk a feszültség transzfer függvények meghatározása az 1. kapuról a 3. és 4. kapura (a többi a szimmetriából adódik).



2. ábra FSZ gerjesztése és lezárásai

A feszültség transzfer függvények általános alakja nem ismert tetszőleges fokozatszám esetén. Néhány oktávnál nem nagyobb sávban, 30 dB-nél nem kisebb oldalsáv elnyomás esetén egy vagy két fokozat elegendő, ezért a feszültség transzfer függvényeket egy- és két fokozatú szűrők esetén adjuk meg:

$$G_{V31,1} = \frac{Z_L}{j\omega CR_1Z_L + 2R_1 + Z_L} \quad (1)$$

$$G_{V41,1} = -j\omega CR_1 \frac{Z_L}{j\omega CR_1Z_L + 2R_1 + Z_L} \quad (2)$$

$$G_{V31,2} = Z_L \frac{1+\omega^2R_1R_2C^2}{D} \quad (3)$$

$$G_{V41,2} = -Z_L \frac{j\omega C(R_1+R_2)}{D} \quad (4)$$

$$D = 2R_1 + 2R_2 + Z_L + j\omega C(4R_1R_2 + 3R_1Z_L + R_2Z_L) - \omega^2C^2R_1R_2Z_L \quad (5)$$

ahol (1)-(2) az egy, a többi egyenlet a két fokozatú PFSZ kifejezéseit adja meg, ω a körfrekvencia, és Z_L a terhelő impedancia. R_1 és R_2 jelöli rendre az első és a második fokozat ellenállás-értékeit.

A feszültség transzfer függvények hányadosa

$$\frac{G_{V41,1}}{G_{V31,1}} = -j\,\omega\,C\,R_1 \quad (6)$$

$$\frac{G_{V41,2}}{G_{V31,2}} = \frac{-j\,\omega\,C\,(R_1+R_2)}{1+\omega^2\,C^2R_1\,R_2} \quad (7)$$

rendre egy és két fokozat esetén. Ezt a hányadost az amplitúdók és a fázisok együttfutásának hibáját kifejező m és φ tényezővel is felírhatjuk:

$$\frac{G_{V41}}{G_{V31}} = m\,e^{j\left(\frac{\pi}{2}+\varphi\right)} \quad (7a)$$

ahol m és φ valós mennyiségek, $m \geq 0$.

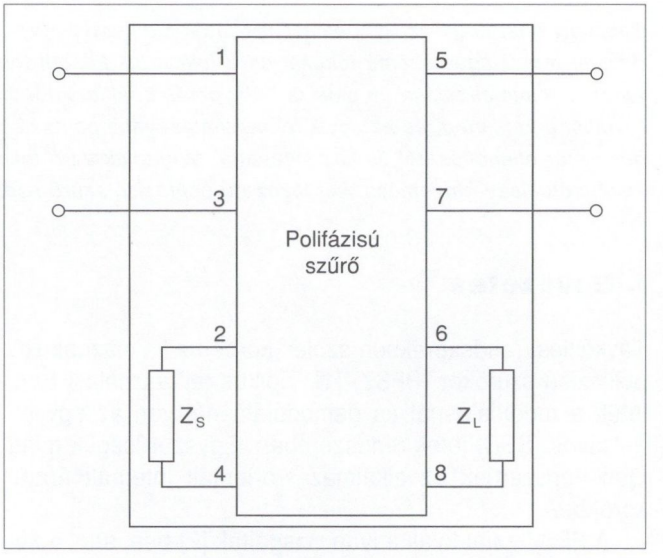
Tökéletes amplitúdó- ill. fázis-együttfutás esetén m=1 és $\varphi = \pm k\pi$ (k=0,1,...). A (6)-(7a) egyenletekből láthatjuk, hogy a 2. ábra szerinti konfiguráció esetén a fázisok minden frekvencián $\pi/2$-vel különböznek egymástól, és az amplitúdók csak bizonyos fekvencián egyeznek meg, $\omega_1 = 1/CR_1$ a (6) egyenletben és $\omega C\,(R_1+R_2) / (1+\omega^2C^2R_1R_2) = 1$ a (7) egyenletben (ez utóbbi a $\omega_1 = 1 / CR_1$ és $\omega_2 = 1 / CR_2$ frekvenciákat adja meg). A (6)-(7a) egyenletről azt is leolvashatjuk, hogy *az amplitúdó- és fázis-együttfutás hibáját kifejező tényezők függetlenek a generátor- és a terhelő impedanciáktól.*

Az egy oldalsávú moduláció fontos jellemzője az oldalsáv-elnyomás, amely szinuszos jelek esetén az oldalsávok amplitúdóinak hányadosa a kimeneten. Ideális keverőket és összeadót feltételezve, az oldalsáv-elnyomást az alkalmazott szűrő jellemzőjének tekinthetjük. A függelékben megmutatjuk, hogy az oldalsáv-elnyomás a fentebb definiált, az amplitúdó- és a fázis-együttfutás hibáját jellemző paraméterekkel fejezhető ki. Következésképpen *az oldalsáv-elnyomás szintén nem függ a generátor- és a terhelő impedanciáktól.* Ez a tulajdonság fontos lesz majd a zajtényező minimalizálásakor.

Az oldalsáv-elnyomás függ a generátor- és a terhelő impedanciák közti különbségtől, ezért ügyelni kell a lezárások szimmetriájára a realizált áramkör esetén.

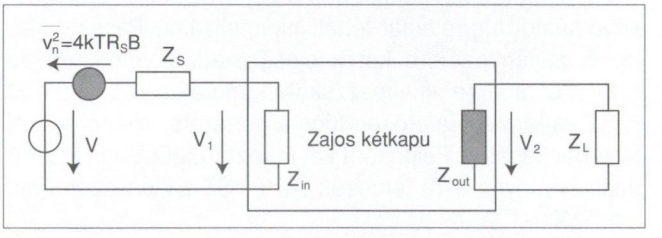
III. Passzív áramkörök zajtényezője

Ebben a fejezetben passzív áramkörök zajtényezőjére adunk meg kifejezéseket, és az egyiket a PFSZ zajtényezőjének minimalizálására használjuk fel. A PFSZ és a lezáró impedanciák szimmetriája következtében elegendő a zajtényező vizsgálata egy bemenet és egy kimenet esetén, a másik bemenetet és kimenetet megfelelően lezárva *(3. ábra)*. Ezért passzív kétkapuk zajtényezőjét fogjuk meghatározni.



3. ábra A kétkapu, melynek zajtényezőjét meghatározzuk. Z_S és Z_L a külső lezárásokkal egyezik meg.

Feltételezzük, hogy a vizsgált kétkapu impedancia-mátrixa létezik. A reciprocitás következtében az impedancia-mátrix modell frekvenciánként három komplex mennyiséggel írható le. A zaj modellezéséhez három másik komplex modell-paramétert alkalmazunk, biztosítva, hogy ezek és az előző három paraméter egyértelműen átszámítható legyen egymásba. A *4. ábra* szerinti modell teljesíti ezt a követelményt, tehát azonos lezárások esetén *modellünk az impedancia-mátrix modellel ekvivalens.*



4. ábra Jelölések a zajtényező számításához. Feltételezzük, hogy Z_S és Z_{out} termeli a zajt. A kétkaput Z_{in}, Z_{out} és V_2 és V_1 közti összefüggés modellezi

Feltételezzük, hogy a 4. ábrán látható áramkör hőmérsékleti egyensúlyban van, tehát minden zajforrás hőmérséklete T. A kétkaput az aktuális lezárások mellett mérhető be- és kimeneti impedancia és a terhelt feszültségerősítés modellezi. A kétkapun belüli hőmérsékleti zajt Z_{out} termeli. A kétkaput zajos generátor gerjeszti és zajmentes terhelő impedancia terheli.

A zajtényező definíciója az alábbi:

$$F = \frac{SNR_{in}}{SNR_{out}} \tag{8}$$

ahol a jel-zaj viszonyok kifejezése a következő:

$$SNR_{in} = \frac{P_{s\,in}}{P_{n\,in}},\quad SNR_{out} = \frac{P_{s\,out}}{P_{n\,out}} \tag{9}$$

és a jelet s és a zajt n indexszel jelöltük.

A bemeneti jelteljesítény, ha V_1 amplitúdójú szinuszos jelet tételezünk fel, a következő:

$$P_{s\,in} = \frac{1}{2}\frac{|V_1|^2}{R_{in}} \tag{10}$$

A bemeneti zajteljesítmény Z_S-ből származik:

$$P_{n_i\,in} = \frac{1}{R_{in}}\left(\left|\sqrt{4kTR_s B}\,\frac{Z_{in}}{Z_s + Z_{in}}\right|^2\right) = \frac{4kTB}{R_{in}}\,\frac{R_s|Z_{in}|^2}{|Z_s + Z_{in}|^2} \tag{11}$$

A (11) egyenletben k a Bolzmann-állandó (≈1.3807*10^{-23} Joule/°K), T a zajhőmérséklet és B a zaj-sávszélesség.

A jelteljesítmény a kimeneten:

$$P_{s\,out} = \frac{1}{2}\frac{|V_2|^2}{R_L} \tag{12}$$

Végül a kimeneti zajteljesítmény:

$$P_{n\,out} = \frac{1}{R_L}\left(\left|\sqrt{4kTR_{out}}B\frac{Z_L}{Z_{out} + Z_L}\right|^2\right) = \frac{4kTB}{R_L}\,\frac{R_{out}|Z_L|^2}{|Z_{out} + Z_L|^2} \tag{13}$$

A fenti egyenletekből a zajtényezőre a következő kifejezést kapjuk:

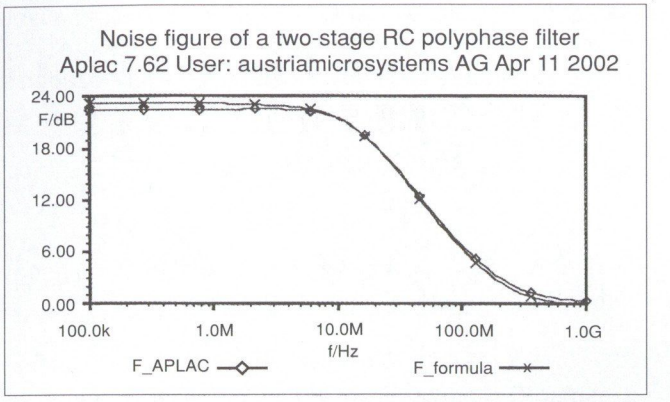
$$F = \frac{1}{|G_V|^2}\,\frac{|Z_s + Z_{in}|^2}{R_s|Z_{in}|^2}\,\frac{R_{out}|Z_L|^2}{|Z_{out} + Z_L|^2} \tag{14}$$

A (14) egyenletben $G_V = V_2 / V_1$ a terhelt feszültségerősítés. (14)-ből látjuk, hogy ha $|Z_S| << |Z_{in}|$ és $|Z_L| >> |Z_{out}|$, akkor az egyenlet a következőre egyszerűsödik:

$$F = \frac{1}{|G_V|^2}\,\frac{R_{out}}{R_s} \tag{15}$$

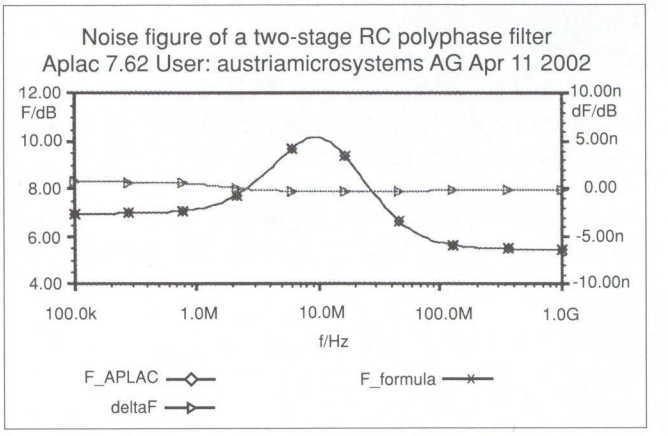
A (15) formula gyors becslésre alkalmas a rendszertervezésben.

Az *5. ábrán* összehasonlítjuk az APLAC [4] programmal és a (15) egyenlettel kiszámított zajtényezőt.



5. ábra A (15) egyenlettel és áramkör-analízis programmal meghatározott zajtényezők összehasonlítása. RS-t úgy állítottuk be, hogy az egyenlet feltételei teljesüljenek

A *6. ábrán* a programmal és a (14) egyenlettel kiszámított zajtényezőt hasonlítjuk össze abban az esetben, amikor a (15) egyenlet feltételei nem teljesülnek. Az egyezés mindkét esetben kielégítő.



6. ábra A (14) egyenlettel és áramkör-analízis programmal meghatározott zajtényezők összehasonlítása. A (15) egyenlet feltételei nem teljesülnek (zajillesztés)

IV. Polifázisú szűrő zajtényezőjének minimalizálása

Ebben a fejezetben a (14) kifejezést alkalmazzuk a PFSZ zajtényezőjének minimalizálására. A zaj-minimumot Z_S függvényében keressük. Az ezután következő lépés a következő fokozat (összegző) zajtényezőjének minimalizálása lehet, Z_L változtatásával. Ezekben a lépésekben az oldalsáv-elnyomásnak Z_S-től és Z_L-től való függetlenségét használjuk ki.

Nézzük először az egy fokozatú szűrőt. $G_{V,1}$, Z_{in} és Z_{out} analitikus kifejezései a következők:

$$G_{V,1} = \frac{Z_L}{j\omega CR_1Z_L + Z_L + 2R_1} \tag{16}$$

$$Z_{in,1} = \frac{j\omega CR_1Z_L + Z_L + 2R_1}{j\omega CZ_L + j\omega CR_1 + 1} \tag{17}$$

$$Z_{out,1} = \frac{j\omega CR_1Z_s + Z_s + 2R_1}{j\omega CZ_s + j\omega CR_1 + 1} \tag{18}$$

Ha ezeket a kifejezéseket (14)-be helyettesítjük, a következő kifejezést kapjuk a zajtényezőre $\omega_1 = 1 / CR_1$ frekvencián (a 6. ábrán látjuk, hogy a zajtényező a sávközépen a legnagyobb, ezért ezt minimalizáljuk):

$$F_1 = \frac{R_S^2 + 2R_S R_1 + X_S^2 - 2X_S R_1 + 2R_1^2}{R_1 R_S} \qquad (19)$$

ahol $Z_S = R_S + jX_S$. A zajtényező Z_L-től független, ahogy vártuk. A zajtényező minimumának helye

$$Z_S = R_1 + jR_1 \qquad (20)$$

Azonban IC realizáció esetén induktív lezárás nem megengedett. $X_S = 0$ esetén a zajtényező minimumának helye

$$R_S = \sqrt{2R_1} \qquad (21)$$

A zajtényező minimumának értéke

$$\min(F_1) = 2 + 2\sqrt{2} \qquad (22)$$

amely 6,838 dB-lel egyenlő.

Ezen a ponton észrevehetjük, hogy *a zajtényező minimalizálása különbözik a teljesítmény-illesztéstől.* Ugyanis a (17) egyenletből az következik, hogy a teljesítmény-illesztés a bemeneten Z_L-től függ. Azonban a zajtényező minimalizálása független Z_L-től, ahogy láttuk.

Folytassuk most a két fokozatú szűrővel. Behelyettesítve (14)-be $G_{V,2}$, $Z_{in,2}$ és $Z_{out,2}$ értékét, a zajtényező $\omega_C = 1/C\sqrt{R_1 R_2}$ sávközépi frekvencián

$$F_2 = \frac{1}{4}\frac{2R_S^2(R_1 + 3R_2) + R_S(R_1^2 + 14R_1R_2 + R_2^2) + 4R_1R_2(3R_1 + R_2)}{R_S R_1 R_2}$$

(23) ahol az összes lezárás rezisztív. A zajtényező a terheléstől független, mint az előbb. A zajtényező minimumának helye

$$R_S = \sqrt{\frac{2R_1R_2(3R_1 + R_2)}{R_1 + 3R_2}} \qquad (24)$$

Megjegyezzük, hogy $R_1 = R_2$ esetén (24) (21)-re egyszerűsödik. A zajtényező minimuma

$$\min(F_2) = 4 + 4\sqrt{2} \qquad (25)$$

amely 9,85 dB-lel egyenlő. Ez a két fokozatú PFSZ zajtényezőjének alsó határa.

(22) és (25) összehasonlításával könnyen meg lehet találni az n fokozatú szűrő minimális zajtényezőjét:

$$\boxed{\min(F_n) = 2^n\left(1 + \sqrt{2}\right)} \qquad (26)$$

Ez a zajtényező tapasztalható tökéletes amplitúdóegyezés esetén, ha a különböző fokozatok ellenállásai megegyeznek. A (26) egyenlet érvényességét számítógépes szimulációval ellenőriztük n = 1, 2...5 esetén, sikerrel.

V. Példa: Széthangolt, két fokozatú polifázisú szűrő optimális zajtényezője

Példaként széthangolt, két fokozatú PFSZ zajtényezőjét minimalizáljuk. A tervezés bemenő adata a kapacitás értéke, C = 8 pF (a rendelkezésre álló szilíciumfelület alapján határoztuk meg), a sávközépi frekvencia f_c =10 MHz, és ezen a frekvencián az oldalsáv-elnyomás értéke, S_{max}= 25 dB. A következő egyenleteket kell megoldani R_1-re és R_2-re:

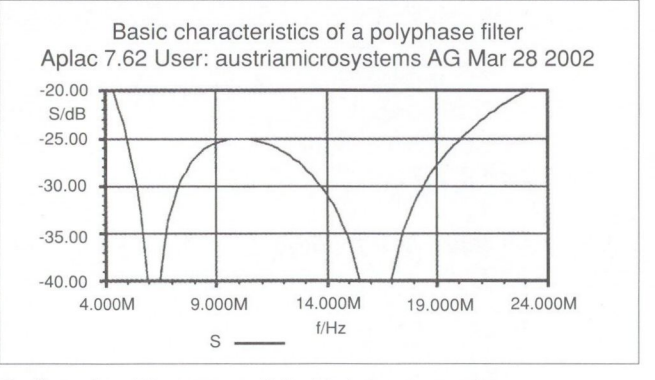
$$f_C = \frac{1}{2\pi C\sqrt{R_1R_2}} \qquad (27)$$

$$S_{max} = 20\ \log\left(\frac{R_1 + R_2 - 2\sqrt{R_1R_2}}{R_1 + R_2 + 2\sqrt{R_1R_2}}\right) \qquad (28)$$

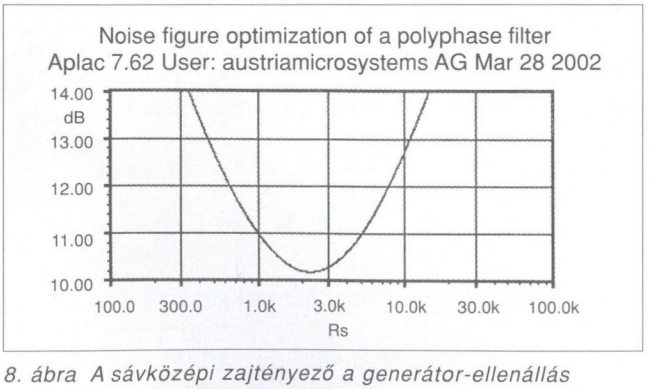
ahol (28) a (7), (35) egyenletekből és S lokális maximumának feltételéből következik.

A (27)-(28) egyenleteknek két pár megoldása van, egyikük R_1 = 1,227 kΩ, R_2 = 3,226 kΩ. A (24)-(23) egyenleteket alkalmazva a zajillesztésre, a minimális zajtényezőhöz tartozó generátor-ellenállás R_S = 2,239 kΩ, és a zajtényező F_2 = 10,18 dB. Ennek a szűrőnek az oldalsáv-elnyomása látható a *7. ábrán* a frekvencia függvényében. A sávközépi zajtényezőt tüntettük fel a *8. és 9. ábrán* a generátor ellenállásának, illetve kapacitásának függvényében.

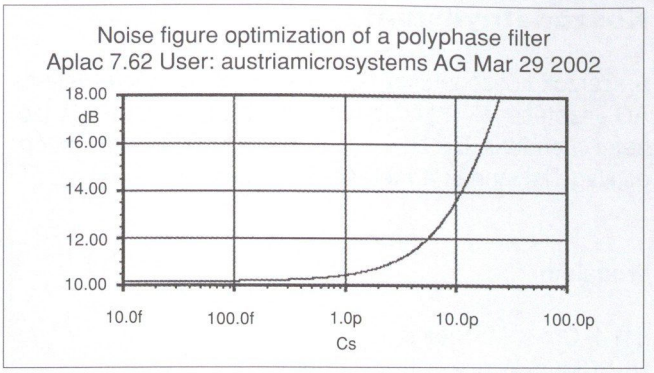
Megmutatható, hogy a sávszélesség f_c és S_{max} függvénye. Ezért a kapacitás értéke mint bemeneti változó nem helyettesíthető egy, a sávszélességre felírt egyenlettel, bár ez kívánatos lenne.



7. ábra A zajillesztett szűrő oldalsáv-elnyomása



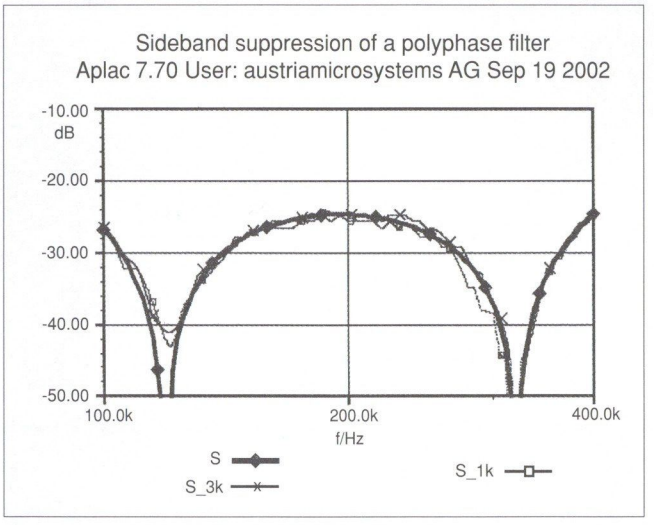
8. ábra A sávközépi zajtényező a generátor-ellenállás függvényében, ha a generátor kapacitása zéró



9. ábra A sávközépi zajtényező a generátor kapacitásának függvényében. A generátor ellenállását zéró kapacitás mellett zajminimumra állítottuk be

VI. Mérések

Kísérletileg igazoljuk a PFSZ elméleti oldalsáv-elnyomás görbéjét, és azt az állítást, hogy az oldalsáv-elnyomás független a generátor ellenállásától *(10. ábra)*.



10. ábra Két fokozatú PFSZ elméleti (S) és mért (S_1k, S_3k) oldalsáv-elnyomása

A 10. ábrán látható görbéket megvalósított, két fokozatú PFSZ-n mértük, melynek elemértékei $R_1 = 490\ \Omega$, $R_2 = 1291\ \Omega$ és $C = 1000$ pF.

Az 1. pólust műveleti erősítő kimenetével sorbakapcsolt R_S ellenálláson keresztül gerjesztettük. A 3. pólust leföldeltük. A 2. és 4. pólust R_S értékű ellenállással zártuk le. A kimeneteket szimmetrikusan zártuk le, műveleti erősítőkkel. Minden műveleti erősítő LM 318-as típusú volt.

A feszültségerősítéseket HP 3575 A Gain-Phase Meterrel mértük. A feszültségerősítésekből az oldalsáv-elnyomást a (35) egyenlettel (lásd a függelékben) határoztuk meg.

Ahogy az ábrán látható, R_S=1 kΩ és R_S=3 kΩ értékeket alkalmaztunk. Az elméleti és a mért értékek egyezése jó, demonstrálja azt a tényt is, hogy az oldalsáv-elnyomás valóban független a generátor ellenállásától.

Ezzel cikkünk fő állításának alapját kísérletileg igazoltuk is.

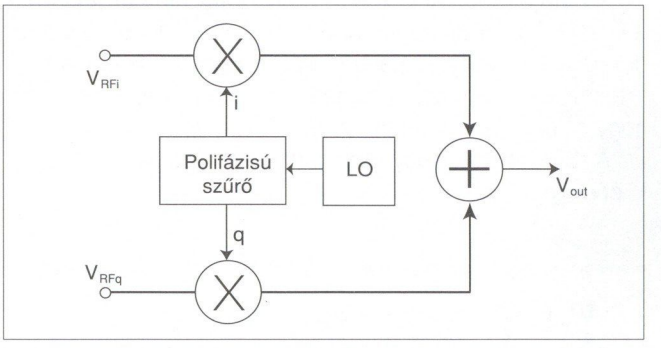
VII. Következtetések

Az RC PFSZ zajtényezőjének minimalizálásával kapcsolatos néhány eredményt közöltünk. Megadtuk a feszültség transzfer függvényeket, és a passzív kétkapuk zajtényezőjére közöltünk két kifejezést. Megmutattuk, hogy az oldalsáv-elnyomás független a lezáró impedanciáktól, ezért a zajtényezőt az oldalsáv elnyomás megváltozása nélkül lehet minimalizálni.

Eredményeinket két fokozatú, széthangolt PFSZ tervezésében és zajillesztésében alkalmaztuk és kísérletileg igazoltuk az oldalsáv-elnyomásnak a generátor-ellenállástól való függetlenségét. Az oldalsáv-elnyomás lezárás-függetlenségét egy- és két fokozat esetére bizonyítottuk be. Azonban ez a tulajdonság tetszőleges számú fokozat esetén is érvényes.

VIII. Függelék: Az oldalsáv-elnyomás

A vizsgált PFSZ-t egy oldalsávos modulációnál és demodulációnál alkalmazzák. Az amplitúdók és a fázisok együttfutásának hiánya véges oldalsáv-elnyomáshoz vezet. A következőkben ezt az összefüggést vezetjük le egy oldalsávos modulátor esetén *(11. ábra)*.



11. ábra Egy oldalsávos modulátor

Feltételezzük, hogy a v_{RFi} és v_{RFq} bemeneti jelek amplitúdó- és fázis együttfutása tökéletes:

$$v_{RFi} = V_{RF}\cos(\omega_{RF}t) \tag{29}$$

$$v_{RFq} = V_{RF}\cos\left(\omega_{RF}t + \frac{\pi}{2}\right) \tag{30}$$

Az amplitúdó- és a fázis-együttfutás hibáját a helyi oszcillátor PFSZ-n átjutott jelében vesszük figyelembe (az ábrán i-vel és q-val jelölt pontokon):

$$v_{LOi} = V_{LOi}\cos(\omega_{LO}t) \tag{31}$$

$$v_{LOq} = V_{LOq}\cos\left(\omega_{LO}t + \frac{\pi}{2} + \varphi\right) \tag{32}$$

ahol V_{LOi} különbözhet V_{Loq}-tól, és φ különbözhet zérustól. Ezek a különbségek írják le az említett hibát. Az általánosság csorbítása nélkül $V_{RF} = 1$ V-ot tételezünk fel.

A modulátor kimeneti feszültségét a következő alakban tételezzük fel:

$$v_{out} = V_U \cos\left[(\omega_{RF} + \omega_{LO})t - \varphi_U\right] + V_L \cos\left[(\omega_{RF} - \omega_{LO})t - \varphi_L\right] \quad (33)$$

ahol U és L jelöli a felső és az alsó oldalsávot. Ha a keverők, az összegző és mind az amplitúdó, mind a fázis-együttfutás tökéletes ($V_{LOi} = V_{LOq}$ és $\varphi = 0$), akkor $V_U = 0$ és $V_L = V_{LOi}$. Ezért a (felső) oldalsáv-elnyomást dB-ben a következőképpen határozhatjuk meg:

$$S = 20\log\left(\frac{V_U}{V_L}\right) \quad (34)$$

A (29)-(33) egyenletek és trigonometrikus azonosságok alkalmazásával az oldalsáv-elnyomást a következőképpen fejezhetjük ki:

$$S = 20\log\sqrt{\frac{\left[1 - m\cos(\varphi)\right]^2 + \left[m\sin(\varphi)\right]^2}{\left[1 + m\cos(\varphi)\right]^2 + \left[m\sin(\varphi)\right]^2}} \quad (35)$$

ahol

$$m = \frac{V_{LOq}}{V_{LOi}} \quad (36)$$

az amplitúdó-, φ a fázis-együttfutás hibáját jellemző tényező. Tökéletes együttfutás esetén $m = 1$ és $\varphi = 0 \pm k\pi$ ($k = 0,1...$), amely végtelenül nagy negatív vagy pozitív S értéket eredményez. A negatív (pozitív) S jelentése az, hogy a felső (alsó) oldalsáv van elnyomva.

A (35) egyenlet egy oldalsávos demodulátorok esetén is érvényes.

Köszönetnyilvánítás

A szerzők köszönetüket fejezik ki az austriamicrosystems AG vezetésének a kiváló feltételek biztosításáért. Köszönetet mondunk Dr. H. Novaknak a kézirat elolvasásáért, és Nagy Istvánnak a mérések elvégzéséért.

Irodalom

[1] J. Crols, M. Steyaert: „CMOS Wireless Transceiver Design", Kluwer Academic Publishers, 1997

[2] F. Behbahani, Y. Kishigami, J. Leete and A. A. Abidi: „CMOS Mixers and Polyphase Filters for Large Image Rejection", IEEE Journal on Solid-State Circuits, Vol. 36, No. 6, June 2001, pp. 873-887

[3] M. J. Gingell: „Single Sideband Modulation using Sequence Asymmetric Polyphase Networks", Electrical Communication, Vol. 48, No. 1-2, pp. 21-25, 1973

[4] APLAC 7.62, 2001 APLAC Solutions Corporation

Hírek

A hagyományos kereskedelemből jól ismert mintára **online bevásárlóközpontot nyitott az Axelero** Magyarország leglátogatottabb internetes portálján, az (origo)-n. Az Axelero, valamint az elektronikus kereskedelmre és aukcióra szakosodott Axio Kft. közös újdonságának működése megfelel a betonból és üvegből készült offline társaiéhoz. A bevásárlóközpont által teremtett infrastruktúra lehetővé teszi, hogy a kereskedők saját üzletet bérelhessenek, a látogatók pedig az Interneten keresztül kényelmesen vásárolhassák meg a termékeket.

A 2001-es mintegy 2 Mrd Ft-os online kiskereskedelem 2002-ben kb. 3,5 Mrd Ft-ra nőtt. Az Axelero erre a 75%-os növekedésre építve már az idei évben jelentős forgalmat remél a hazai piacon egyedülálló kínálatot nyújtó online áruházától. Ezzel a szolgáltatással az (origo) olyan független vásárlási centrumot kíván létrehozni a magyar interneten, ahol színvonalas formában koncentrálódik a legnagyobb kereslet és kínálat.

Az (origo) oldalain eddig működő Vásárteret felváltó bevásárlóközpontban bármely cég, amely teljesíti a korrekt és hatékony e-kereskedelemre vonatkozó követelményeket, létrehozhatja saját áruházát, majd egy egyszerű adminisztratív felület segítségével feltöltheti boltját áruval, és beállíthatja boltja szolgáltatásait. Az (origo) bevásárlóközpont nagy előnye, hogy az üzletek nyitása és az azokban való vásárlás egyszerű, és kedvező áron biztosítja az egyedi megjelenés lehetőségét a kereskedők számára.

MEMS elemek termikus és elektrosztatikus szimulációja a szukcesszív csomópont-redukció módszerével

POHL LÁSZLÓ

BME, Elektronikus Eszközök Tanszéke

Reviewed

Tetszőleges 3D (így pl.: mikro-elektromechanikus – MEMS) struktúrák különféle, Poisson egyenlettel leírható skalártérbeli – akár állandósult állapotbeli, akár dinamikus – viselkedésének gyors és pontos szimulációjára alkalmas a BME Elektronikus Eszközök Tanszékén kifejlesztett SUNRED (SUccessive Node REDuction) algoritmus. A cikk bemutatja az algoritmus működését, valamint alkalmazását termikus szimulációkban.

Bevezetés

Az IC-k és MEMS eszközök tervezésénél gyakran merülnek fel olyan problémák, melyeket Laplace, vagy Poisson egyenlettel adott skalárterek írnak le. A Poisson egyenlet általános alakja a következő:

$$divgrad\, S\frac{\partial^2 S}{\partial x^2}+\frac{\partial^2 S}{\partial y^2}+\frac{\partial^2 S}{\partial z^2}=Q(x,y,z)$$

Q = 0 esetben a Laplace egyenletet kapjuk. Például termikus terek esetében S a hőmérséklet, Q pedig arányos a keletkezett hővel. Elektrosztatikus tereknél S a potenciál, Q pedig arányos a töltéssűrűséggel. Nedvesség eloszlásnál S a relatív páratartalom, és Q = 0. Időtől függő esetben a diffúziós egyenletet alkalmazzuk:

$$divgrad\, S\frac{\partial^2 S}{\partial x^2}+\frac{\partial^2 S}{\partial y^2}+\frac{\partial^2 S}{\partial z^2}=\text{const}\bullet\frac{\partial S}{\partial t}$$

Sok módszer létezik e differenciálegyenleteknek megoldására [1,2]. Ezek közül a legismertebb algoritmuscsaládok: a végeselem-módszerek *(FEM – Finite Element Methods)*, a véges differencia módszerek *(FDM – Finite Difference Methods)*, és a határelemes módszerek *(BEM – Boundary Element Methods)*.

A SUNRED a véges differencia módszerrel kapott modell megoldására létrehozott új algoritmus [3,4,5], mely egyaránt alkalmas MEMS struktúrák, IC tokok, vagy nyomtatott áramköri kártyák szimulációjára.

Egyenletek

A SUNRED algoritmust végrehajtó program a következő egyenleteket oldja meg.

a) Termikus szimuláció esetében (1):

$$\mathrm{div}(\lambda\bullet\mathrm{grad}T)=\frac{\partial}{\partial x}\left(\lambda\frac{\partial T}{\partial x}\right)+\frac{\partial}{\partial y}\left(\lambda\frac{\partial T}{\partial y}\right)+\frac{\partial}{\partial z}\left(\lambda\frac{\partial T}{\partial z}\right)=-p(x,y,z)+c\frac{\partial T}{\partial t}$$

ahol λ(T) a hővezetés, T a hőmérséklet, p(x,y,z) a diszszipáció-sűrűség (hőáram), c pedig a térfogati hőkapacitás.

Állandósult (stacionárius) állapotban:

$$\mathrm{div}(\lambda\bullet\mathrm{grad}T)=\frac{\partial}{\partial x}\left(\lambda\frac{\partial T}{\partial x}\right)+\frac{\partial}{\partial y}\left(\lambda\frac{\partial T}{\partial y}\right)+\frac{\partial}{\partial z}\left(\lambda\frac{\partial T}{\partial z}\right)=-p(x,y,z)\qquad(2)$$

A λ hővezetés általában hőmérsékletfüggő, ez nemlinearitást okoz. Amennyiben a hővezetés nem függ a hőmérséklettől (a leggyakrabban használt 0-100°C tartományban általában ez a nemlinearitás elhanyagolható), akkor az egyenlet tovább egyszerűsödik:

$$divgradT=\frac{\partial^2 T}{\partial x^2}+\frac{\partial^2 T}{\partial y^2}+\frac{\partial^2 T}{\partial z^2}=-\frac{1}{\lambda}p(x,y,z)\qquad(3)$$

b) Elektrosztatikus szimuláció esetében
(csak állandósult állapotot vizsgálunk):

$$\mathrm{div}(\varepsilon\,\mathrm{grad}V)=\frac{\partial}{\partial x}\left(\varepsilon\frac{\partial V}{\partial x}\right)+\frac{\partial}{\partial y}\left(\varepsilon\frac{\partial V}{\partial y}\right)+\frac{\partial}{\partial z}\left(\varepsilon\frac{\partial V}{\partial z}\right)=-p(x,y,z)\qquad(4)$$

ahol ε a dielektromos állandó, V a potenciál, ρ pedig a töltéssűrűség.

A modell

A szukcesszív csomópont-redukciós algoritmus (SUNRED) alapja egy, a vizsgált problémát reprezentáló villamos hálózat. A nem elektromos problémákat elektromos áramköri modell írja le. A hálózatot a következőképpen kapjuk:

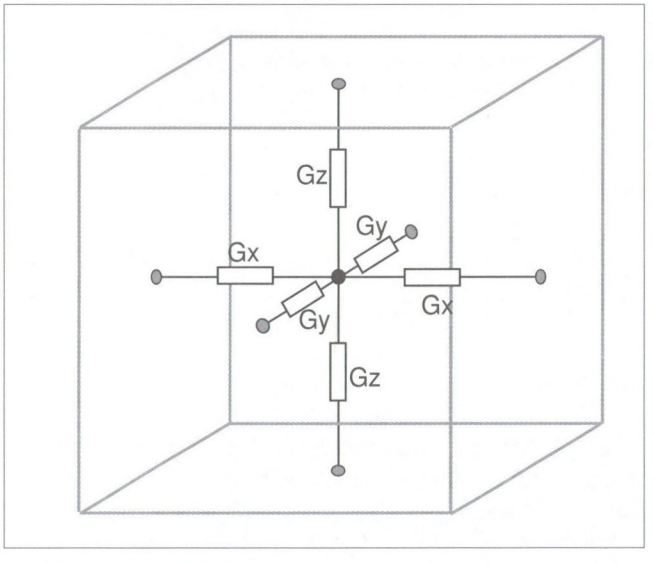
Téglatest alakú térfogatot vizsgálunk (ez nem jelent megkötést, mivel bármely részét kitölthetjük levegővel). A téglát egy 3D ráccsal n×n×m darab apró téglára osztjuk, és úgy tekintjük, hogy minden ilyen téglát adott homogén anyag tölt ki, tehát két anyag között a határvonal minden esetben az egyes kis téglákat elválasztó határvonallal esik egybe. A rács osztásközei tetszőlegesen választhatók, de az osztósíkok száma az algoritmus egyszerű és

gyors működése érdekében meghatározott: n és m kettő hatványai (a jelenlegi megvalósításban n=32...1024, m=1...16, de n×m maximum 1024).

A cellákban lévő anyagok megadása nagyon egyszerűen, m darab n×n méretű digitális (jelen esetben BMP formátumú) képpel történik. Minden használt színhez hozzárendelünk egy anyagot. Az anyagok tulajdonságait egy táblázattal adjuk meg (ezek a tulajdonságok termikus esetben a hőkapacitás, és a hővezetés, elektrosztatikus esetben a relatív dielektromos állandó, valamint mindkét esetben az esetlegesen alkalmazott kényszer típusa és értéke). Ezen a módon akár megfelelően feldolgozott valódi kép, például mikroszkóppal készült fénykép is felhasználható.

Miután a felosztást elvégeztük, minden apró téglát helyettesítünk egy hálózattal (az elosztott paraméterű rendszert koncentrált paraméterű hálózattal helyettesítjük). A hálózat elemei megfeleltethetők egy elektromos hálózat rezisztív, kapacitív, feszültség-, vagy áramgenerátor elemeinek.

A továbbiakban a modellhálózatot villamos hálózatnak tekintjük, és ezen végezzük a számításokat. Termikus esetben az elektromos vezetés megfelelője a hővezetés, a villamos kapacitásé a térfogati hőkapacitás, a feszültségforrásé egy hőmérsékletet kényszerítő elem (≈ végtelenül jó hővezetésű hűtőborda), az áramforrásé pedig egy adott teljesítményt (disszipációt) leadó hőforrás. Minden cella közepén egy, oldallapjain további hat csomópont található:



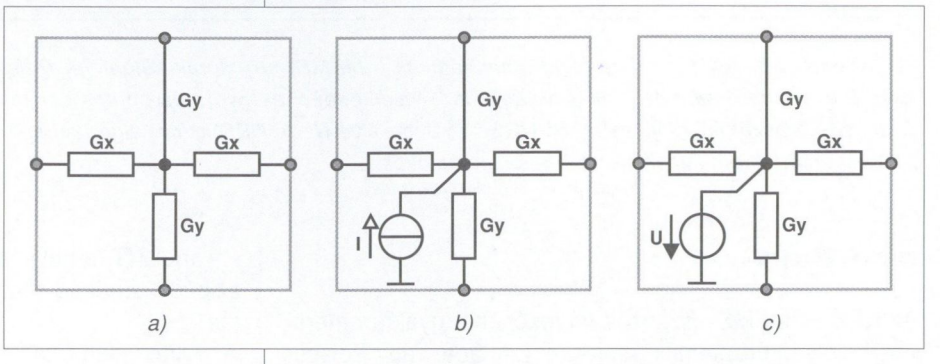
1. ábra 3D elemi cella, a problémát reprezentáló villamos hálózat építőköve

A középső csomópontra kapcsolódhat még kapacitás, feszültség-, vagy áramforrás is.. Ha ilyen elemek is csatlakoznak a cellára, akkor az új „anyagot" is jelent, vagyis az anyagot definiáló BMP képen ezekhez más szín tartozik.

A továbbiakban az egyszerűbb tárgyalásmód érdekében 2D hálózattal foglalkozunk, bemutatva azt az esetet, amikor termikus problémát oldunk meg, mégpedig stacionárius állapotban, lineáris hővezetésű anyagok esetében. Tehát a (3) egyenlet a következőképpen módosul:

$$divgradT = \frac{\partial^2 T}{\partial x^2} + \frac{\partial^2 T}{\partial y^2} = -\frac{1}{\lambda} p(x,y) \qquad (5)$$

Ebben az esetben a hálózati modell cellája a *2. ábrán* látható:



2. ábra 2D hálózat elemi cellái állandósult állapotban.
a) külső kényszer nélkül
b) áram gerjesztés
c) feszültség kényszer

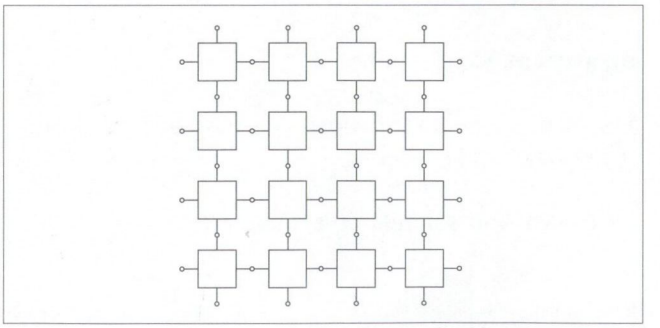
A vizsgált téglalap alakú (cellákra osztott) terület szélein meghatározott peremfeltételeket érvényesíthetünk. Ezek lehetnek:

- állandó potenciál
- nulla áram

Az elemi cellák leírhatók egy 4×4-es, valós elemű, szimmetrikus admittanciamátrixszal. Nem állandósult állapotban, tehát (1) esetben a belső csomópontra egy kapacitás is kapcsolódik, emiatt az admittanciamátrix komplex elemű lesz. A cellát egyértelműen reprezentálja az **Y** admittanciamátrix, valamint egy **J** inhomogén áramvektor. A **J** vektor a belső csomópontra kapcsolódó gerjesztés külső csomópontokra redukált alakja, tehát gerjesztés nélkül 0. A cellák teljes leírása tehát a következő: **I** = **YU**+**J**, ahol **I** a cella külső csomópontjain folyó áramvektor, **U** a külső csomópontok potenciálja.

A megoldó algoritmus

A vizsgált probléma megoldását a kapott villamos hálózati modell segítségével kapjuk, amely a következő felépítésű:

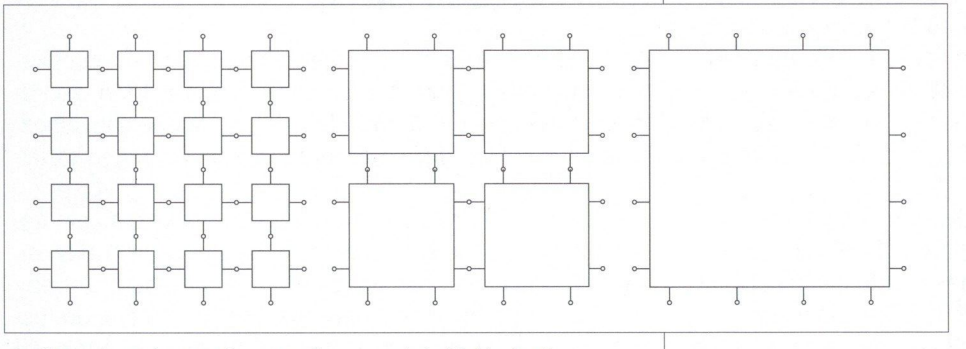


3. ábra A megoldandó villamos hálózat (részlet)

Az általunk vizsgált esetekben tipikusan 256×256 vagy 512×512 elemű rácsot használunk. Ez P = 131584, illetve P = 525312 csomópontot jelent, tehát a megoldandó lineáris egyenletrendszer együttható-mátrixa, vagyis az admittanciamátrix mérete P×P (rendre 131584×131584, illetve 525312×525312). Bár ezek a mátrixok nagyon ritkák (az elemek nagy része 0), a megoldandó feladat így is nagy problémát jelent.

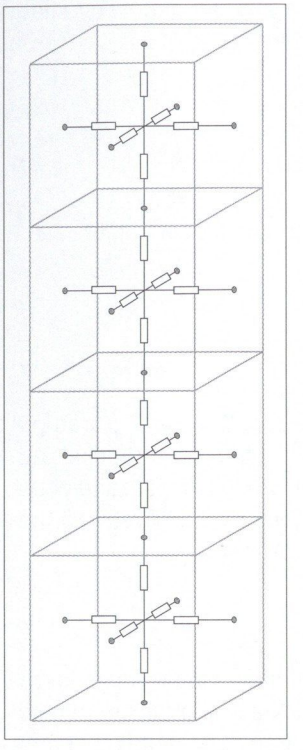
A SUNRED algoritmus (a [6]-ban leírt elképzeléshez hasonlóan) egy erre a célra kifejlesztett szukcesszív (egymásra épülő lépésekből álló) eljárást használ. (Iterációs algoritmus nem látszott alkalmasnak a leállási feltétel meghatározásának nehézsége miatt.) Az eljárás lépéseit a *4. ábrán* kísérhetjük figyelemmel. Első lépésben négy elemi (nulladrendű) cellából álló (elsőrendű) blokkokat hozunk létre. Az így kapott cellák nyolc külső, és négy belső kapoccsal rendelkeznek. Az egymáshoz csatlakozó négy belső csomópont kiejthető, az elsőrendű cella leírásában már nem jelenik meg, ezért a középső ábrán már nem is szerepel.

Az első lépéshez hasonlóan végezzük a további lépéseket egészen addig, míg a hálózatnak csak külső csomópontjai maradnak. Az ezt leíró admittanciamátrix tehát 4n×4n méretű lesz (vagyis 256×256 elemű rácsnál 1024×1024, 512×512 elemű rácsnál pedig 2048×2048 méretű). A peremfeltételek figyelembe vételével a lineáris egyenletrendszert megoldjuk, majd ennek ismeretében, fokozatos visszahelyettesítéssel megkapjuk a belső csomópontok potenciálját (ill. jelen esetben hőmérsékletét).



4. ábra A szukcesszív csomópont-redukció lépései 4x4 elemű hálózaton

A 3D esetet a SUNRED a 2D eset kiterjesztéseként kezeli, mégpedig a következőképpen: az elemi celláknak az 1. ábrán látható módon hat kapcsa van. Első lépésként vesszük az elemi cellákból álló oszlopokat *(5. ábra)*. Elvégezzük az összevonást úgy, hogy a legfelső és a legalsó csomópontra a megfelelő peremfeltételt érvényesítjük, és a belső csomópontokat kiejtjük. Ekkor egy olyan eredő admittanciamátrixot (és inhomogén áramvektort) kapunk, amelyek ugyanúgy kezelhetők, mintha 2D elemi cellákat vontunk volna össze. (Az 5. ábrán látható négy elemi cella összevonásából ugyanolyan redukált hálózat keletkezik, mint amilyet a 4. ábra harmadik képe is mutat, azzal a különbséggel, hogy itt a négy kapocs egymás alatt, és nem egymás mellett levő cellákhoz tartozik.) Tehát ezt követően az összevonás és kiértékelés 2D algoritmussal végezhető.



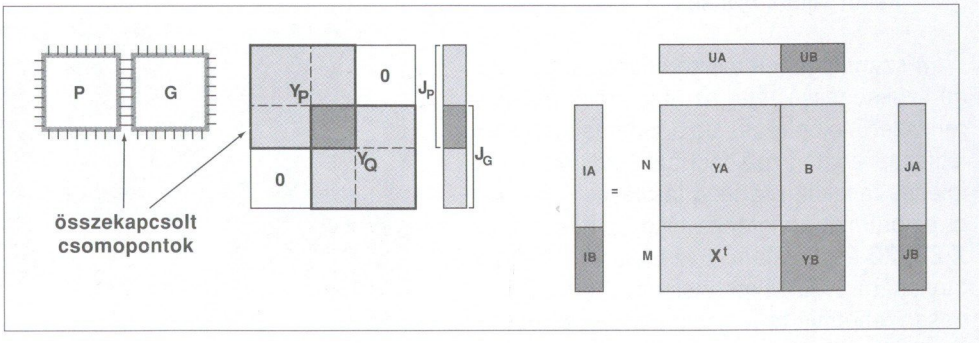
5. ábra A 3D rács egy oszlopa

Az elvi áttekintés után most nézzük a gyakorlati megvalósítást! A cellákat az **Y** admittanciamátrix, és a **J** inhomogén áramvektor írja le. A második ábrán bemutatott elemi cellákra az admittanciamátrix és az inhomogén áramvektor elemi számításokkal számolható.

Két (akár elemi, akár magasabb rendű) cella összevonása úgy történik, hogy a közös csomópontokon az **Y** mátrixok, és a **J** vektorok összeadódnak, a nem kapcsolódó csomópontok áramai, ill. az eredeti admittanciamátrixok saját admittancia értékei nem változnak, míg a két kiinduló mátrix nem kapcsolódó csomópontjai közötti kapcsolatot leíró helyekre az eredő mátrixban 0 kerül *(6/a ábra)*.

A következő lépés a belső csomópontok kiejtése. A jobb érthetőség kedvéért rendezzük át az **Y** mátrixot és a **J** vektort (6/b ábra, itt a 0-k már nincsenek külön jelölve). N külső kapocs, és M belső csomópont van. Az **YA** blokk a külső csomópontok közötti kapcsolatot írja le. Az **X** blokk (és a transzponáltja) a külső és belső kapcsok közötti kapcsolatot, **YB** pedig a belső csomópontok közötti kapcsolatot adja meg. **IA** és **IB** a csomópontokon átfolyó áramok, **UA** és **UB** a csomópontok potenciálja (illetve hőárama és hőmérséklete).

6. ábra a) Két cella összekapcsolása
b) Az átrendezett admittanciamátrix



Tehát két összekapcsolt cella lineáris mátrixegyenlete a következő:

$$\mathbf{IA} = \mathbf{YA}\cdot\mathbf{UA} + \mathbf{X}\cdot\mathbf{UB} + \mathbf{JA} \quad (6)$$

$$\mathbf{IB} = \mathbf{X}^t\cdot\mathbf{UA} + \mathbf{YB}\cdot\mathbf{UB} + \mathbf{JB} \quad (7)$$

Mivel **IB** = 0, átrendezéssel a következőt kapjuk:

$$\mathbf{Y}_{RED} = \mathbf{YA} - \mathbf{X}\cdot\mathbf{ZB}\cdot\mathbf{X}^t \quad (8)$$

$$\mathbf{J}_{RED} = \mathbf{JA} - \mathbf{X}\cdot\mathbf{ZB}\cdot\mathbf{JB} \quad (9)$$

Ahol **ZB** mátrix **YB** mátrix inverze, $\mathbf{Y}_{RED}$ és $\mathbf{J}_{RED}$ pedig a csomópontok kiejtésével kapott, úgynevezett redukált admittancia mátrix és redukált áramvektor. A visszahelyettesítés során az **UA** vektorok ismeretében a következő módon határozzuk meg az **UB** vektorokat:

$$\mathbf{UB} = -\mathbf{ZB}\cdot\mathbf{X}^t\cdot\mathbf{UA} - \mathbf{ZB}\cdot\mathbf{JB} \quad (10)$$

Mivel $(\mathbf{X}\cdot\mathbf{ZB})^t = \mathbf{ZB}\cdot\mathbf{X}^t$, ezt a mátrixot elég egyszer kiszámolni. Az **Y** mátrixok, valamint a $\mathbf{X}\cdot\mathbf{ZB}\cdot\mathbf{X}^t$ mátrix szimmetrikus, így elegendő csak a felső háromszög mátrixot eltárolni. Ugyancsak a szimmetria következtében a számítások közel fele megtakarítható.

A SUNRED algoritmus a következő lépéseket hajtja végre:

1. *Hálózat redukció.* A redukciót végző programszegmens megkapja a k-adik szintű **Y** mátrixokat, és azokat a (8) képlet alkalmazásával k+1-edik szintűekre redukálja. Fájlban tárolja a **ZB** és az **X·ZB** mátrixokat, mert ezekre szükség lesz a további lépésekben. A 3. lépés az utolsó $\mathbf{Y}_{RED}$ mátrixot is használja, ezért ez is tárolásra kerül.
2. *Áramok számítása.* A k-adik szintű áramvektorok, valamint az 1. lépésben eltárolt **X·ZB** mátrixok felhasználásával a (9) képletnek megfelelően kalkulálja, és fájlban tárolja a redukált áramvektorokat.
3. *Peremfeltételek érvényesítése.* A legmagasabb szintű admittanciamátrixot és inhomogén áramvektort felhasználva érvényesíti a hálózaton a peremfeltételeket, vagyis meghatározza a külső csomópontok potenciáljait és áramait.
4. *Visszahelyettesítés.* A belső csomópontok potenciáljait számolja ki ugyancsak szukcesszív módon, a (10) képlet felhasználásával. Az **X·ZB**, **ZB** és **J** értékeket fájlból olvassa.

A számítógépek memóriájának szűkössége szükségessé tette az algoritmus pipeline rendszerű felépítését, és a futtatás során keletkezett adatok (például az **Y** mátrixok) ideiglenes fájlokban történő tárolását. A jelenlegi algoritmus ideiglenes fájlokat használ az **X·ZB**, **ZB** és **J**, valamint az utolsó $\mathbf{Y}_{RED}$ mátrix tárolására. A RAM méretek növekedése rövidesen lehetővé teszi majd az ideiglenes fájlok mellőzését, ennek következtében a program működése is fel fog gyorsulni.

Az algoritmus lépései közül az első a legidőigényesebb, mert ebben a részben vannak Ordó($P^{3/2}$) rendű műveletek: **YB** → **ZB** mátrix invertálás, és **X·ZB**, valamint $\mathbf{X}\cdot\mathbf{ZB}\cdot\mathbf{X}^t$ mátrixszorzások (itt P az összes csomópont számát jelenti). A többi lépés ezeket az eredménymátrixokat használja, ezért ezek a műveletek legfeljebb Ordó(P) időigényűek. Amennyiben csak a gerjesztések változnak két futtatás között, a hálózatredukciót nem kell megismételni.

Az algoritmus futásának teljes időigénye:

$t = 63.5\cdot P^{3/2}\cdot t_{*+}$, ahol a t_{*+} egy szorzás, és egy összeadás végrehajtásához szükséges idő összege. (A kiinduló hálózatra felírt P×P méretű együttható-mátrixú lineáris egyenletrendszer Gauss eliminációval való megoldásához Ordó(P^3) nagyságrendű idő lenne szükséges.) Konkrét esetet vizsgálva egy 512×512 méretű rács esetén (P= 525312), egy 1,5GHz-es processzorral felszerelt PC számítógépen a futási idő mindössze 55 másodperc.

A SUNRED algoritmust használó program az állandósult állapot kiszámításán (DC analízis) felül lehetővé teszi tanziens (ugrásválasz függvény) felvételét az időtartományban (reverse-Euler integrálással), frekvenciatartományban pedig AC analízist (adott frekvencián), Bode analízist, valamint időállandó spektrum felvételét is.

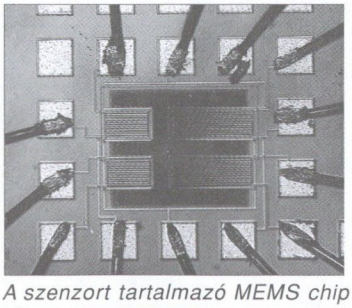
Elektrotermikus konverter termikus szimulációja

Az Elektronikus Eszközök Tanszéke nemzetközi projektegyüttműködés [9] keretében jutott hozzá a TIMA laboratóriumban tervezett MEMS elemek kísérleti példányaihoz. A kísérleti chipek egyike elektrotermikus konvertert tartalmaz.

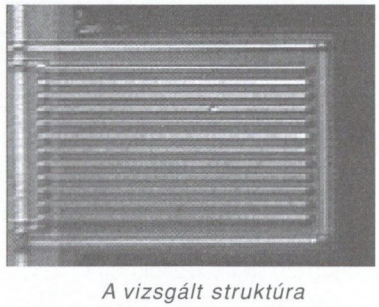
Az elektrotermikus konverter olyan eszköz, amely tetszőleges jelalakú elektromos feszültség effektív értékének mérésére alkalmas oly módon, hogy a mérendő jelet egy ellenállásra vezeti. Az ellenálláson átfolyó, a mérendő feszültséggel arányos áram (a feszültség effektív értékével arányosan) felmelegíti a MEMS struktúrát. A felmelegedés a struktúrába épített termoelemekkel mérhető.

Az elektrotermikus konverter mérését korábban elvégezték a tanszéken [7,8]. A következőkben bemutatjuk egy ilyen szenzor SUNRED szimulációját, illetve a szimulált eredmény összehasonlítását a mért görbével.

7. ábra



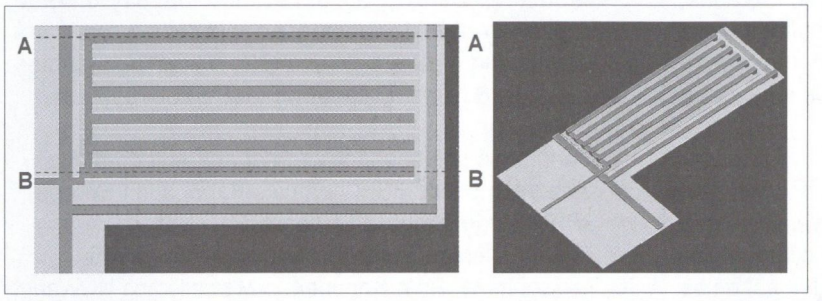
A szenzort tartalmazó MEMS chip



A vizsgált struktúra

A bemutatott mérések és szimulációk a bal alsó kantiléveren található struktúráról készültek, melynek kinagyított fényképét a jobb oldali ábra mutatja. A hőmérsékletet 12 darab sorba kapcsolt termoelem segítségével mérjük (ezek a vízszintes sávok). A kantiléver jobb oldalán látható 651 ohmos (a képen függőleges) poliszilícium ellenállással fűtjük a struktúrát (a felül és alul látható hozzávezetések alumíniumból készültek): ez a disszipátor.

A szimulációhoz használt modell képét mutatja a *8. ábra*. Mivel a struktúra szimmetrikus, a szimulációt elég a fél struktúrán elvégezni. Ez most az eszköz alsó oldala.



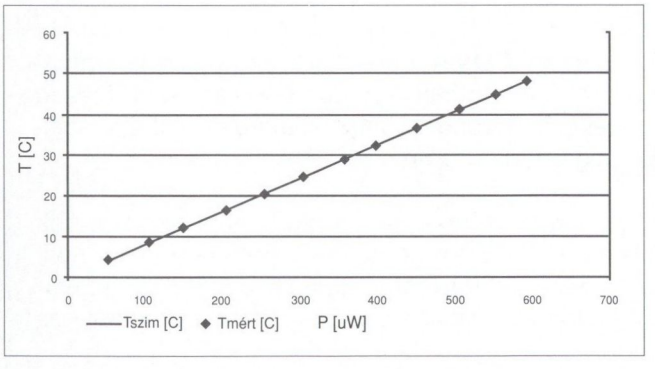
8. ábra A MEMS struktúra modellje síkban és térben

A fűtőellenállásra 50–600 μW disszipációt kapcsoltunk, és mértük a termoelemekből álló érzékelő kimeneti feszültségét. Szimuláció során ugyancsak teljesítményt kapcsoltunk a fűtőellenállásra, itt azonban közvetlenül hőmérsékletben kaptuk az eredményt. A szimulációval kapott hőmérsékletek a termoelemek végpontjai hőmérsékletkülönbségeinek átlagai.

A hőmérséklet-disszipáció görbét a *9. ábrán* láthatjuk. A mért feszültségből a hőmérsékletet egyszerűen számoltuk: egy termoelem érzékenysége 44 μV/K, és 12 termoelem kapcsolódik sorba.

Tehát: $T = U_{ki} / (528\ \mu V/K)$.

A mért és szimulált eredményeket a peremfeltételek pontosításával 400 μW disszipációnál illesztettük. A mért görbét pontokkal, a szimulált görbét folytonos vonallal jelöltük. A két görbe láthatóan jól illeszkedik. Az ábrából azt a következtetést vonhatjuk le, hogy a valódi eszköz jó linearitással, az elvárásoknak megfelelően működik.



9. ábra A MEMS struktúra hőmérsékletemelkedésének mértéke a ráadott teljesítmény függvényében

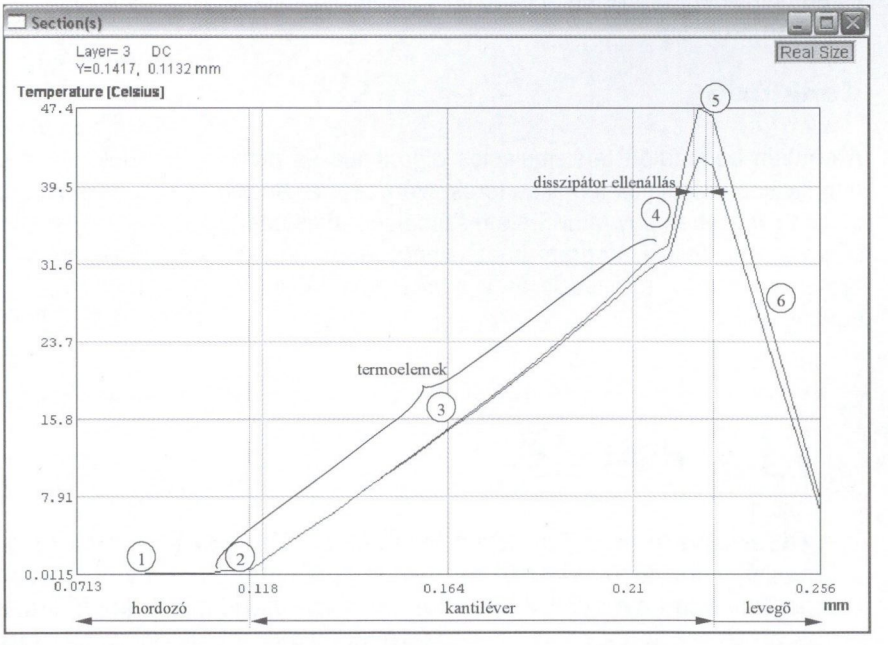
Egyszerűen nem mérhető, viszont könnyen szimulálható a hőmérséklet-eloszlás a struktúrán belül. A *10. ábra* ilyen hőmérséklet-eloszlást mutat 400 μW gerjesztés mellett.

A metszetek a következők (8. ábra):

A – vízszintes metszet a fémréteg és az alatta levő poliszilícium réteg közötti oxid rétegben (legbelső termoelem)

B – vízszintes metszet ugyancsak a fémréteg és az alatta levő poliszilícium réteg közötti oxid rétegben (külső termoelem)

A legbelső termoelem jobban felmelegszik, mint a külső, tehát az ábrán ez a felső görbe.



Amikor a 9. ábrán látható hőmérsékleteket mérjük, a termoelemek két vége közti hőmérsékletkülönbséget kapjuk. Ez a két végpont a 10. ábrán a 0,107 mm-nél (a kis plató (2) elején), illetve 0,216 mm-nél (a csúcs előtti töréspont közelében ((4) alatt) található.

A görbék magyarázata a következő:

(1) A relatíve nagyméretű Si hordozó szinte teljesen elvezeti a hőt, ezért nem számottevő a hőmérséklet-emelkedés.

(2) A kis platót már poliszilícium és fém veszi körül, amelyek ide vezetik a hőt a fűtőellenállásról, viszont az ezeket körülvevő rossz hővezető SiO_2 nem engedi teljesen lehűlni ezt a részt.

(3) A meredeken emelkedő szakasz a (levegőben lógó) kantiléveren (nyelven) található. Itt már nincs Si hordozó, ami elvezetné a hőt, így az csak a SiO_2 és a fém, valamint poliszilícium rétegben áramolhat.

(4) A töréspont, és csúcs közötti rész: itt nincs sem fémezés, sem poliszilícium, kizárólag az ezeknél sokkal rosszabb vezető oxid.

(5) A csúcsot követő viszonylag lapos rész: mivel a modell felépítéséhez viszonylag durva rácsot használtunk, a fűtőellenállást csak egyetlen pont, a csúcspont jelképezi. Az ezt követő laposabb szakasz a nyelv széléig tart. Itt is rosszul vezető oxid található. A csúcs jobb oldalán azért laposabb a görbe, mint a bal oldalán, mert itt levegővel érintkezik, amely nagyságrendekkel rosszabb vezető, mint akár a SiO_2, akár a poliszilícium, vagy a fém.

(6) Ez a meredek szakasz levegő. Azért ilyen meredek, mert 0,1 mm vastagságot állítottam be a modellben, és a jobb oldala konstans 0°C-ra kapcsolódik. A hő nagy része balra, a szilícium hordozó felé áramlik, ezért ennek a szakasznak nincs különösebb jelentősége.

A görbe talán legfontosabb tanulsága, hogy a termoelemek által észlelt hőmérséklet nem egyezik meg a fűtőellenállás hőmérsékletével, hanem attól mintegy 25-30%-kal elmarad. Ez azonban a gyakorlati felhasználás során nem jelent problémát, mindössze megfelelő kalibrációra van szükség.

Konklúzió

A cikkben bemutatott térszimulációs algoritmus és program kiválóan alkalmas termikus terek számítására. A cikk második részében egy MEMS elem szimulációjának segítségével igazoltuk a program használhatóságát. Tapasztalataink szerint a szimuláció és a mérés eredményei jól egybeesnek.

Irodalom

[1] S. Selberherr:
Analysis and simulation of semiconductor devices, p. 294, Springer-Verlag, Wien, New York, 1984

[2] G. Beer and J. O. Watson:
Introduction to finite and boundary element methods, p. 509, John Wiley & Sons, Chichester, 1992

[3] V. Székely:
SUNRED: a new thermal simulator and typical applications, 3rd THERMINIC Workshop, September 21-23, Cannes, France, pp. 84-90, 1997

[4] V. Székely and M. Rencz: Fast field solvers for thermal and electrostatic analysis, DATE Proceedings, Feb. 23-26 Paris, France, pp. 518-523, 1998

[5] V. Székely:
Algorithmic solutions for thermal and electro-static simulation of MEMS, Photonics Fabrication Europe, SPIE's International Symposium, 28 Oct – 1 Nov. 2002, Proceedings Vol. 4945

[6] T.A. Johnson, R.W. Knepper, V. Marcello and W. Wang:
Chip substrate resistance modeling technique for integrated circuit design,
IEEE Trans. on Computer-Aided Design, Vol CAD-3, No.2, pp 126-134 (1984)

[7] Unyatinszki Tamás:
Elektrotermikus MEMS elemek minősítése,
Önálló laboratórium beszámoló, BME EET, 2002

[8] Hajas István:
Elektrotermikus MEMS elemek minősítése,
Diplomaterv, BME EET, 2002

[9] PROFIT IST-1999-12529 EU Project

Hírek

A **Cisco Systems** a Partnerek Nemzetközi Találkozóján mutatta be összeépíthető kapcsolóplatformjának új generációját. Az új termékcsoport hibatűrése kiváló, használata egyszerű, ugyanakkor gigabites teljesítményt nyújt. A Cisco Stack Wise megoldásra épülő stacktechnológia. 32 gigabit/másodperces belső stack-kapcsolati rendszerével maximum kilenc switch kapcsolható össze együttes kezelésre optimalizált logikai egységgé. Előnyei a stack-hibatűrés speciális hardver- és szoftverátterhelési funkciókkal, az egységes szolgáltatás elosztott továbbítási és szolgáltatásminőségkezelési (QoS) funkciókkal, az automatizált konfiguráció az egyszerűbb használat érdekében, valamint a megfelelően nagy teljesítmény a Gigabit Ethernet kapcsolatok kezeléséhez.

Az **Ericsson** bejelentette, hogy a vállalat sikeres 2,1 GHz-es CDMA2000 hang- és adatátviteli hívásokat bonyolított le a CDMA2000 E1xEV-DV-re készen álló infrastuktúra-berendezésén. Az Ericsson létrehozta 2,1 GHz-es CDMA2000 K+F Központját is a pekingi Ericsson China vállalaton belül. Ez szállítja majd 2,1 GHz-es CDMA2000 megoldást a térség megrendelői számára.

A **Microsoft** vezérigazgatója személyesen ajánlott föl a német kormánynak engedményt termékeinek árából. Mint ismeretes, az IBM tavaly partneri megállapodást kötött a német kormánnyal a Linux nyílt forráskódú szofverjeit támogató termékeinek szállítására. A német kormány ragaszkodik ahhoz, hogy a Microsoft termékekkel bármely új, rivális termék együtt tudjon élni, mind szövetségi, mind tartományi és helyi szinten.

A Celeron 600 MHz-es processzor és hűtőbordájának vizsgálata

termovíziós kamerával és termikus tranziensmérővel

KOLLÁR ERNŐ doktorandusz
BME Elektronikus Eszközök Tanszéke
kollar@eet.bme.hu

Reviewed

Ebben a cikkben egy FC-PGA tokozású processzor termikus tranziensét vizsgáljuk termovíziós kamerával. Megvizsgáljuk, miként terjed a hő a PCB (Printed Circuit Board) hordozó felé, hogyan terjed szét a hűtőbordával felszerelt processzoron nyugvó és kényszerített légáram mellett.

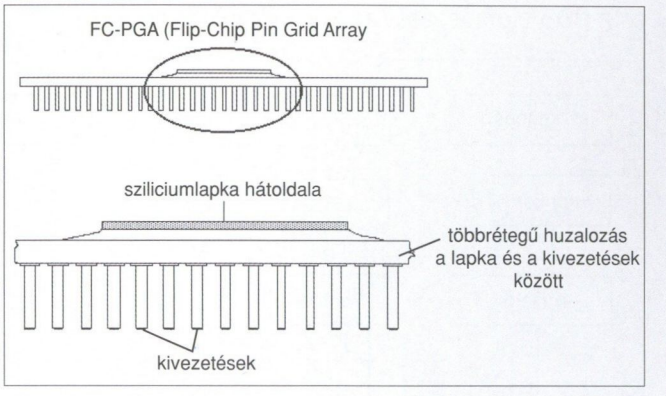
Bevezető

A processzor hőelvezetése a számítógép működése szempontjából kulcsfontosságú. Már a hordozható számítógépek is aktív (ventillátoros) processzorhűtéssel kerülnek forgalomba. A maximális aktív zóna hőmérséklet (Maximum Junction Temperature) hordozható gépeknél rendszerint 100°C fok, asztali gépeknél alacsonyabb, típustól függően általában 70°C és 90°C fok körüli. A processzor tervezésénél figyelembevett teljesítmények (TDP – Thermal Design Power) asztali gépekbe szánt élvonalat képviselő processzorok esetén 70-80W körül, a hordozható gépekbe szánt processzorok esetén pedig 25-30W körül jár *(1. táblázat)* [1][2][3][4][5].

Processzor		TDP W	Max Tcase C	Max Tjunction C
Celeron	600 MHz	19,4		90
	1.000 GHz	29		75
Pentium 4, 478-pin	1.50 GHz	59.7	73	
	2.50 GHz	75.3	76	
Pentium 4, 478, 0.13um	2.00 GHz	54.3	69	
	2.50 GHz	61.0	72	
	3.06 GHz	81.8	69	
Mobile Pentium III	450 MHz, 1.05 V	57		100
	850 MHz 1.15 V	10		100
	1.000 GHz 1.40 V	20.5		100
Mobile Pentium 4	1.2 GHz, 1.3 V	20.8		100
	1.4 GHz 1.3 V	25.8		100
	1.8 GHz 1.3 V	30		100
	2.4 GHz 1.3 V	35.0		100

1. táblázat A processzor tervezésénél figyelembevett teljesítmények és hőmérsékletek

Kísérleteinkben azt vizsgáltuk, hogy miként jut el a hő a környezet felé olyan hűtési megoldások esetén, mint a hűtőbordával ellátott processzor, hűtőborda és ventillátor, vagy a hűtőborda nélküli eset.



1. ábra Az FC-PGA tok

Ebben a cikken egy FC-PGA (Flip-Chip Pin-Grid-Array) tokozású Celeron 600 MHz-es processzor hőelvezetését vizsgáltuk. Az FC-PGA tok egyik szembetűnő sajátossága, hogy a szilíciumlapka hátoldala szabadon van, nem fedi be a tok anyaga *(1. ábra)*. Ez a tok azzal biztosít jobb hőelvezetést, mint egy teljesen zárt, hogy a hő a szilíciumlapkáról az interfész anyagon (pl.: hővezető krémen) keresztül közvetlenül a hűtőbordára jut, elkerülve a tok anyagát.

A méréseket az AGA-782 típusú termovíziós kamerával és a termikus tranziens teszterrel az Elektronikus Eszközök Tanszéke Termikus laboratóriumában végeztük.

A processzor előkészítése a méréshez

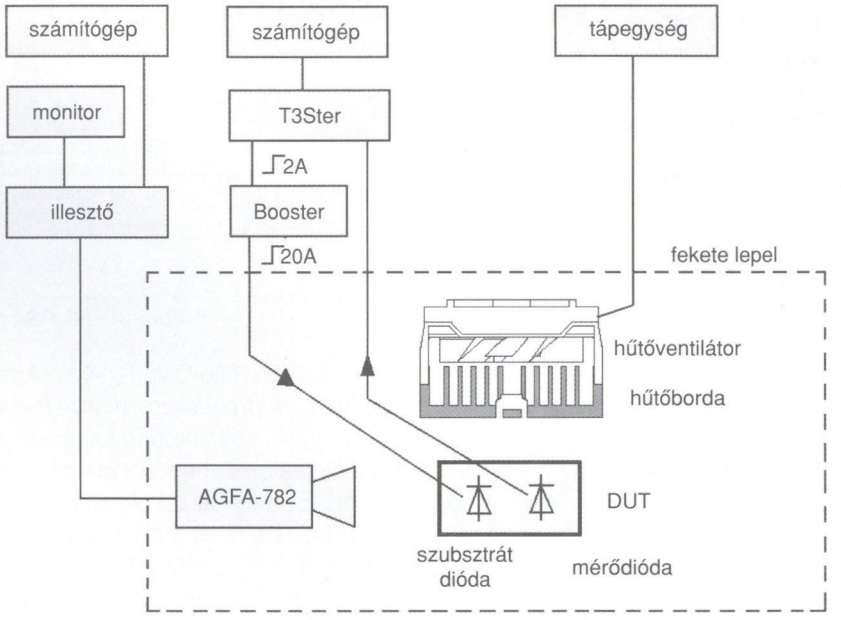
A méréshez egyfelől disszipációt kell kényszerítenünk, másfelől mérni kell a chip belső hőmérsékletét. Mindezek egy p-n átmenettel megoldhatók. Ebben a kísérletben a processzorra fordított polaritással adtuk rá tápfeszültséget, azaz a szubsztrát dióda nyitó irányban történő előfeszítésével a processzort egyetlen nagy diódaként használtuk. A diódára állandó áramot kényszerítve nyitófeszültsége az eszköz hőmérsékletének függvényében változik, így alkalmas az eszköz hőmérsékletének mérésére.

Üzemszerű működés közben ezt a módszert természetesen nem lehet alkalmazni. (Kísérleteinkben a processzor melegedését kívántuk előidézni, ami nem jelentette azt, hogy a processzort üzemszerűen kellett volna használnunk.) Kifejezetten hőmérsékletmérésre egy mérődiódát

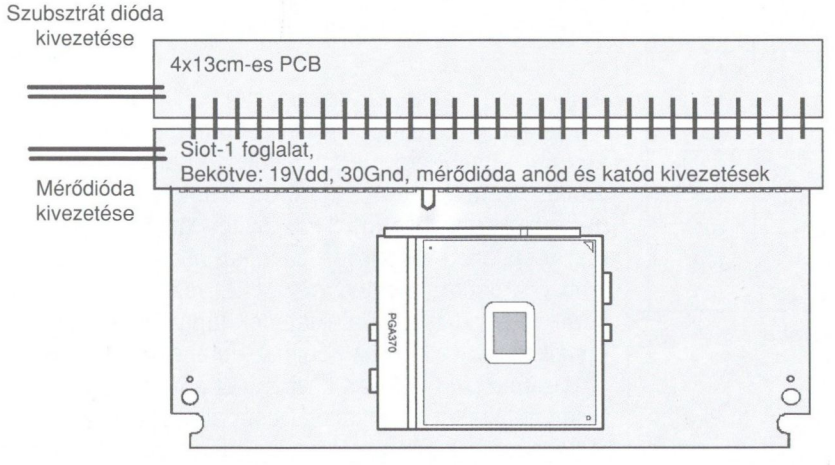
integrálnak a lapkára, ami lehetővé teszi a processzor működés közbeni hőmérséklet figyelését. Paraméterei e feladathoz igazodnak. Hőmérsékletmérésre a szubsztrátdióda helyett inkább ezt a mérődiódát használtuk.

A processzort egy Slot1–FC-PGA átalakítón keresztül egy Slot1 csatlakozóba tettünk. A Slot1 csatlakozóhoz egy kis méretű 4x13 cm-es PCB hordozó tartozott, amire kivezettük a processzor föld és táp kivezetéseit, valamint a processzorban lévő hőmérő dióda lábait. A processzor melegedését ezzel a beépített mérődiódával is nyomon követtük. Ahhoz, hogy a szubsztrát diódát 10-20 W-tal melegíteni tudjuk, megfelelő áramgenerátort kellett keresnünk, ami képes ekkora áramot átkényszeríteni. A méréshez szükséges áramforrást a Thermal Transient Tester (T3Ster) [6] egy kiegészítő egysége a T3Ster Booster [7] biztosította. A mérési elrendezést a *2/a ábra* a processzor és a PCB elrendezését az *2/b ábra* mutatja.

Pontos infra-kamerás hőmérsékletkép készítéséhez az egész áramkört matt feketére kell festeni. Ekkor az egész felület emissziós együtthatója ≈1. Amennyiben ez nem teljesül, úgy a felvétel tartalmazza az adott felületi pontra vonatkozó emisszivitást és reflexiót is. Ez azt jelenti, hogy egy homogén hőmérsékletű PCB-n más hőmérsékletűnek látszik a fehér színű foglalat, mint a zöld színű hordozó, vagy a foglalatot nyitó/záró fém kar. További hibaforrás a tárgyra vetődő külső sugárzás, mint például napfény, világítás, vagy a közelben lévő bekapcsolt fogyasztó, stb. Az említetteket kerülendő a kamera és a tárgy közötti térrészt még egy fekete lepellel is lefedtük, ezzel a szoba légmozgásából származó hatásokat is csökkentettük. A vizsgált objektum mögé fekete kartont helyeztünk.



2/a Mérési elrendezés



2/b A processzor és a PCB elrendezése

Topográfiai felvétel készítése

A tranziens kiértékelése során szükség van olyan képre is, ami segít az egyes területek azonosításában, a tárgy topográfiáját mutatja ugyanabból a szemszögből, ahonnan a termovíziós tranzienst felvettük. Ha viszont a fent vázolt előkészítés jól sikerült és a vizsgált tárgy is közel homogén hőmérsékletű, akkor a kamera legérzékenyebb állásában sem látszik szinte semmi. A kontrasztosabb felvételekért célszerű a tárgyat izzólámpával megvilágítani, ennek hatására a struktúra egyes részei felmelegednek, tehát látszanak.

Azt tapasztaltuk, hogy egy PCB topográfiai képe viszonylag gyorsan elkészíthető. Ezzel szemben a hordozóból, a hűtőbordából és ventillátorból álló struktúra képe több időt, és ügyességet igényel. Míg a ventillátor műanyag háza könnyen felmelegszik, addig az alumínium hűtőborda szinte változatlan hőmérsékletű marad. A túl erős kontraszt zavaró hatást kelthet a szemlélőben. A legjobb felvételeket a kamera felett elhelyezett lámpával értük el.

Tranziens vizsgálat egy hűtőeszköz nélküli processzoron

Egy FC-PGA tokozású processzor rendeltetésszerű használata valamilyen aktív vagy passzív hűtőeszköz nélkül valószínűtlennek tűnik.

Mégis elvégeztük ezt a kísérletet, ezzel valójában az volt a célunk, hogy a PCB hordozó felé terjedő hőt vizsgáljuk, igaz egy kicsit sarkított formában. Azzal a feltételezéssel éltünk, hogy a hő jelentős része az eszköz kivezetésein távozik el a hordozó felé. Továbbá azt vártuk, hogy a foglalat 370 darab kivezetésének négyzetes elrendezése a felvételeken látható lesz.

A kísérlet elrendezését a *3/a. ábra* mutatja. Az eszközt kímélvén mindössze 3A-rel hajtottuk meg, ami nagyjából 1,5 W-nak felelt meg. 10 perc alatt a lapka hőmérséklet emelkedése meghaladta a 26°C fokot.

A függőlegesen elhelyezett hordozót forrasz oldalról nézve azt tapasztaltuk, hogy a tranziens kezdeti szakaszában *(3/b)* valóban a kivezetések húzták ki a hőt, és a konvekció elenyésző volt. Szembe tűnő, hogy a kivezetések által közrefogott területen belüli viák (a PCB két oldalán lévő vezetékek közötti elektromos átvezetések) hőmérséklete magasabb volt, mint a közrefogott terület egyéb részei.

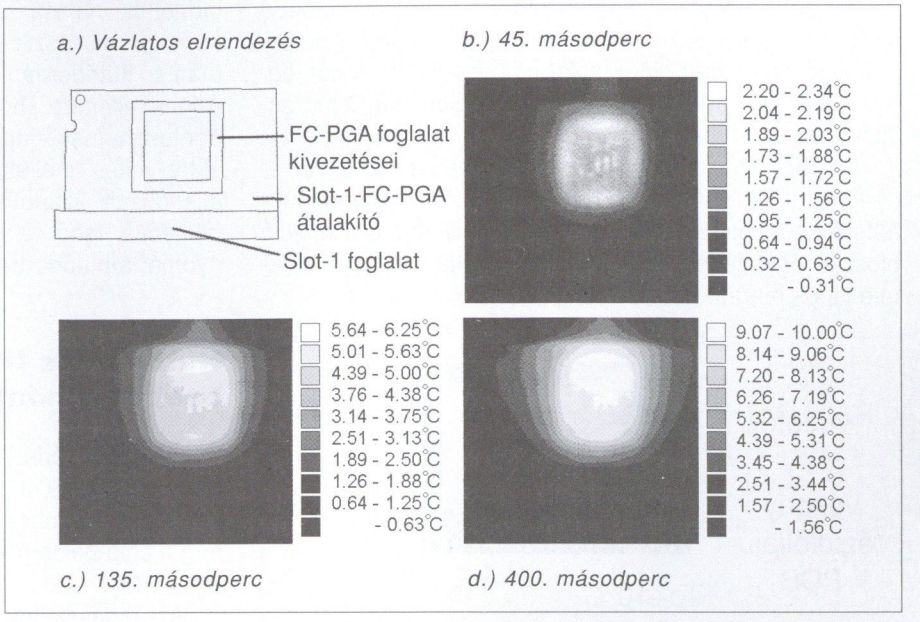
A következő szakaszban, mint azt sejteni lehetett, a közrefogott terület hőmérséklete jobban növekedett, mint a kívül eső részé *(3/c)*. A kivezetett hő még csak a processzor alatti közvetlen környezetre lokalizálódott, de már jól látható a hordozó felett kialakuló konvekciós sáv, amint az átmelegedett levegő füstszerűen felfelé száll.

A tranziens ezt követő szakaszában *(3/d)* a hordozó egész területére szétterjedt a hő, és a konvekciós sáv is kiszélesedett. A közrezárt területen aszimmetria lépett fel, a felső térrész jobban melegedett. Ez a konvekcióból adódhatott. A hőmérsékleti skálák mindegyike Celsius fokban értendő és hőmérsékletemelkedést jelent.

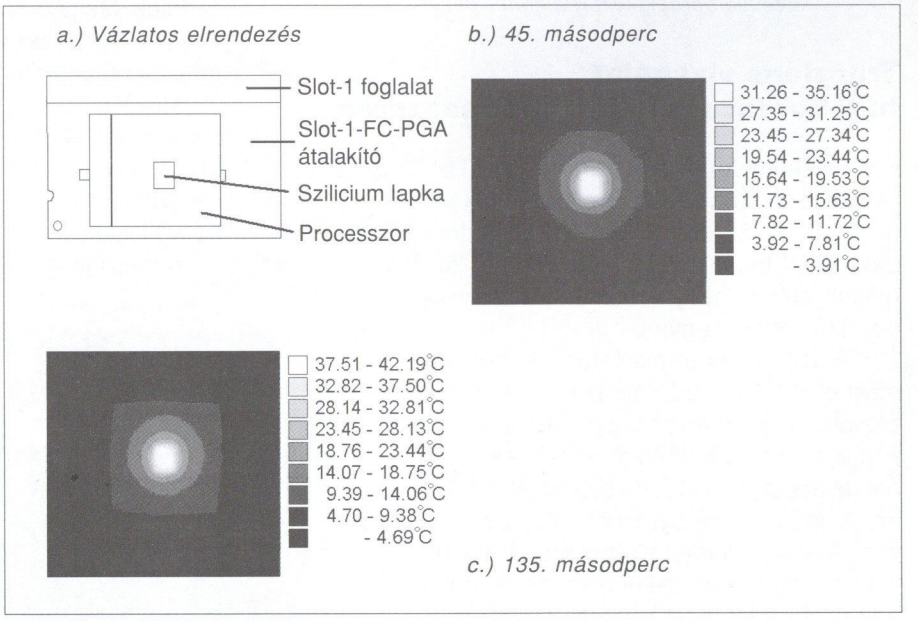
A felvételt megismételtük a processzor felől is *(4. ábra)*.

Azt tapasztaltuk, hogy a szilícium lapka téglalap körvonala a tranziens időtartama alatt mindvégig látszott, és a hőmérséklete kiugróan eltért a környezetétől. Ezzel szemben a processzor felületén szétterülő izotermikus vonalak már koncentrikus körök formájában jelentkeztek *(4/b és 4/c)*.

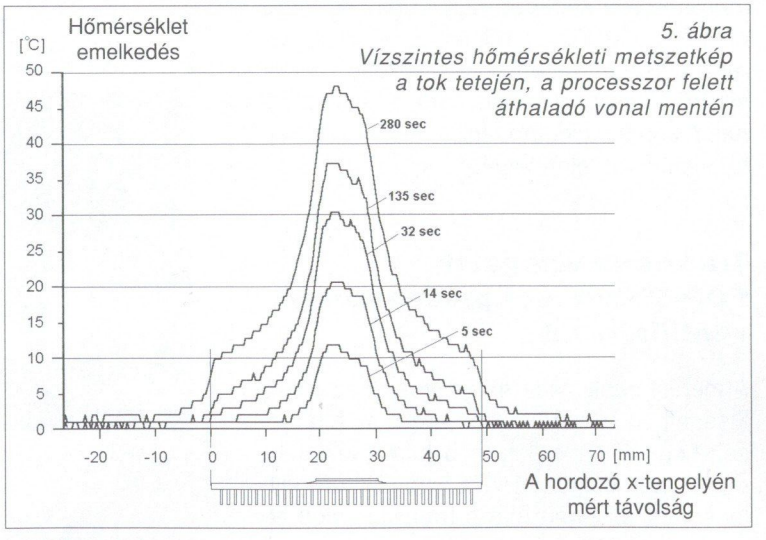
A szilícium lapka kiugró hőmérsékletét legjobban az *5. ábrán* szemlélhetjük.



3. ábra A hűtőborda nélküli processzor melegedése a forrasz oldalról nézve



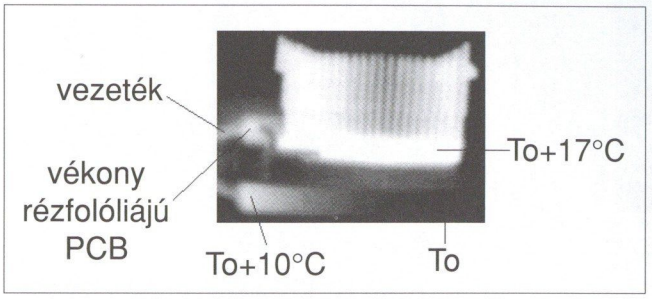
4. ábra A hűtőborda nélküli processzor melegedése a processzor oldaláról



5. ábra
Vízszintes hőmérsékleti metszetkép a tok tetején, a processzor felett áthaladó vonal mentén

Az ábra a processzor közepén vízszintesen áthaladó metszet öt különböző időpillanatát vetíti egybe. A középen lévő csúcs mutatja a lapka hőmérsékletét. A két legfelső görbéből pedig azonosíthatók a Socket370-es foglalat szélei is.

Az ábra érdekessége, hogy a lapka bal széle melegebbnek tűnik, mint a jobb oldala. Ez azért meglepő, mert feltételeztük, hogy a jó hővezetésű szilícium a disszipáció eloszlás egyenetlen voltát jól kompenzálja, és a görbék teteje lapos marad.



6. ábra Csalóka hűtőbordás kép, középső bordák között a háttér látszik

Tranziens vizsgálat hűtőbordával ellátott processzoron

Ezen kísérlet során processzort egy FOP-38-as [8] hűtővel láttuk el, de a ventillátort leszereltük róla. A processzor és a hűtőborda közé TTG-S101 ezüst tartalmú hővezetőpasztát [9] tettünk. A processzorra kb. 20 W teljesítményt adtunk ahhoz, hogy a hőmérsékletemelkedés számottevő legyen.

Eddig a tokra merőlegesen néztünk, most oldalról. A sűrű bordázatú hűtőbordák csalóka melegedési képet mutatnak. A képek szerint a hűtőborda külső része jobban melegszik, mint a belsőé *(6. ábra)*. Persze tévedés lenne azt hinni, hogy ez így is van! Amikor a kamera a hűtőborda közvetlen közelében van, akkor a szembeeső bordák között átlát. Az oldalt levő bordáknál viszont már nem a hátteret látja, hanem valamelyik borda közepét vagy végét. Az ábra még egy „hibát" is elárul, miszerint túl kis keresztmetszetű vezetéket és vékony rézfóliájú PCB hordozót használtunk a betáplálásnál. A kép bal oldalán látszik, hogy mindkettő jelentősen felmelegedett.

Tranziens vizsgálat FOP-38 hűtővel processzoron, ventillátorral

A mérési beállítások megegyeztek az előző kísérletben használtakkal, azzal az eltéréssel, hogy a kamera kisebb hőmérséklettartományban dolgozott. A hűtőventillátort névleges feszültségén már a tranziens előtt elindítottuk, hatása az első felvételen is látszik: a ventillátormotor melegszik *(7/a)*. Nem sokkal a tranziens kezdete után a hűtőbordán megjelenik a szilíciumlapka hatása. Annak ellenére, hogy takarásban van, elhelyezkedése pontosan megállapítható *(7/b)*. Az is látható, hogy az aktív hűtés mellett is melegszik a hordozó *(7/c)*. Az állandósult állapothoz közeli *7/d.* ábrán megpróbáltuk láthatóvá tenni a ventillátor által kifújt meleg levegő nyomát a hűtőborda mögött elhelyezett fekete kartonon.

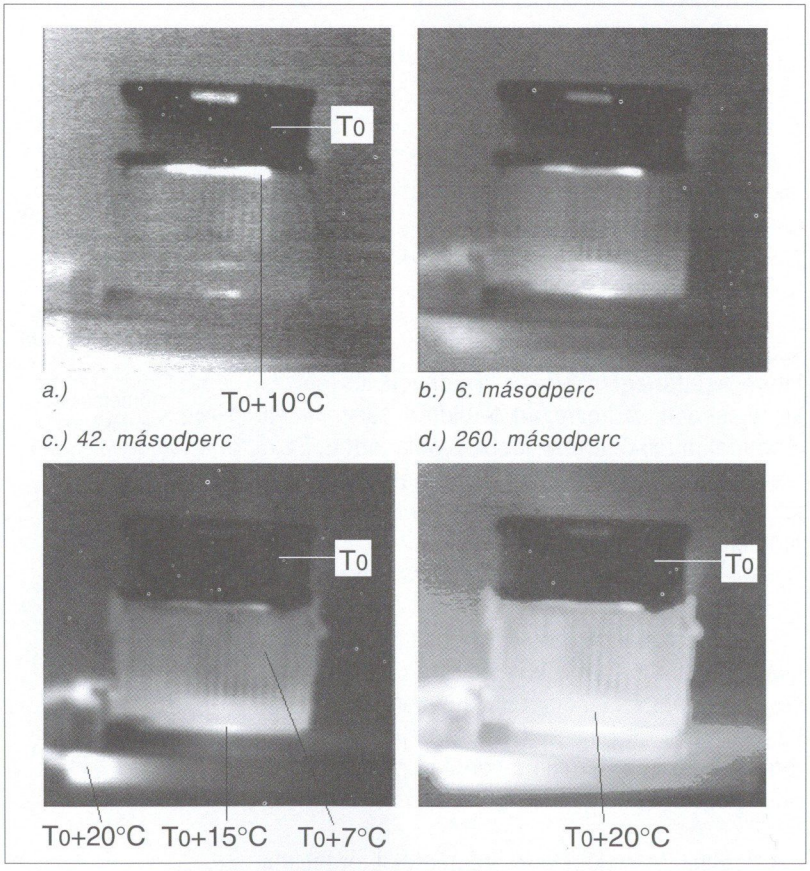
Hűtőbordás tranziensek a processzor beépített hőmérőjének szemszögéből

Következő kísérletsorozatunkban termikus tranziens mérővel vizsgáltuk a processzort. A disszipációlépcsőt továbbra is a szubsztrát dióda tápellátásával biztosítottuk, míg a chip belső hőmérsékletét a beépített hőmérődiódával mértük.

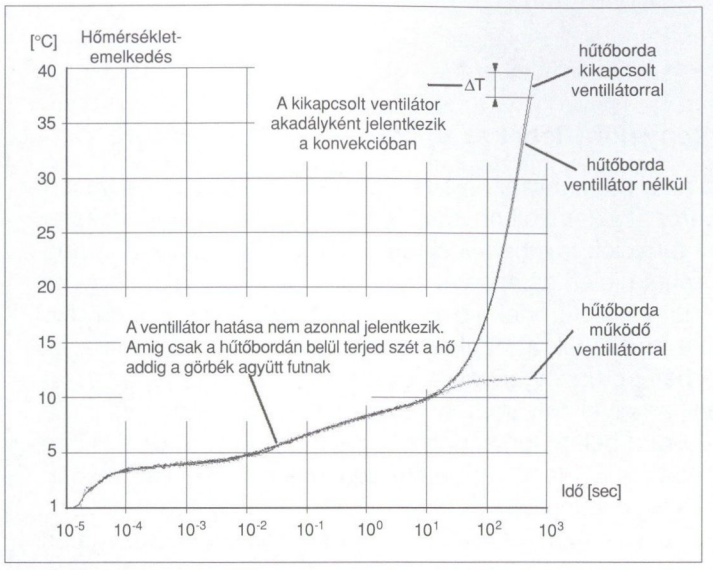
Azt tapasztaltuk, hogy az első 10 másodpercig a hővezetésnek, utána viszont már ventillátornak van döntő szerepe. Megvizsgáltuk azt az esetet is, amikor a hűtőventillátor fel van szerelve, de nem üzemel, és összehasonlítottuk a hűtőbordás tranzienssel.

Megállapítottuk, hogy a felszerelt ventillátor valamennyi akadályt jelent a konvekcióra nézve. Az elágazási ponthoz viszonyítva körülbelül 3-4%-kal volt magasabb a processzor hőmérséklete, mint ha nem lett volna akadály a konvekcióban.

A tranziensgörbék *8. ábrán* lathatók.



7. ábra Működő ventillátor mellett készített tranziens képek



8. ábra A beépített mérődiódával felvett termikus tranziensek

A fenti mérést megismételtük a névleges ventillátor feszültség 75%-án, 50%-án, 5 V-on továbbá azon a legkisebb feszültségen, ami mellett még éppen forog a ventillátor. Utóbbi 3,5 V volt. A tranziensgörbék a *9. ábrán* láthatóak.

Azt tapasztaltuk, hogy a legkisebb ventillátorfeszültség mellett is jelentős hűtőhatása van a ventillátornak az álló esethez képet. A feszültség növekedtével a hűtőhatás egy darabig erőteljesen javul, majd egy ponton túljutva egyre kisebb lesz a hűtőhatás változása. Végül szinte változatlan marad. Az első 600 másodpercben alig tapasztaltunk különbséget a 75%-os és a 100%-os névleges feszültség mellett felvett tranziensgörbéken.

Következtetések

A termovíziós felvételekből kiderült, hogy a PCB hordozón lévő viák az elektromos összekötésen túl egyúttal hőhidakként is működnek. Közvetlenül látszódott, hogy a betáplálásnál használt 35 μm rézfóliájú hordozó vékony volt a processzor áramigényéhez képest.

A processzor magja felett készített metszetképből látható, hogy jelentős hőmérséklet-különbség lépett fel a lapka szélei között, ami adódhatott a szubsztrát dióda egyenetlen hozzávezetéseiből.

A processzorba épített hőmérődióda a működés közbeni hűtőventillátor leállást a leállás után körülbelül 30-60 másodperccel később érzékeli, akárcsak azt, ha a ventillátort a processzor működése közben késve indítjuk el.

A hűtőventillátor hatása minimális feszültség mellett is jelentős. A hűtőhatást a feszültség növelésével csak egy darabig érdemes növelni, a továbbiakban nem okoz jelentős változást.

Megállapítható, hogy a processzorok a rájuk jellemző teljesítmények mellett megfelelő hűtés híján hamar elérhetik a biztonságos hőmérséklettartomány felső határát. Így különösen fontosak a megfelelő hűtésen túl az olyan védelmi megoldások is, amelyek lehetővé teszik, hogy a processzor működés közbeni hőmérséklete a kritikus hőmérséklet alatt maradjon.

Irodalom

[1] Intel ® Celeron ® Processor up to 1.10 GHz, Datasheet, January 2002, Document Number: 243658-020, 66.oldal, www.intel.com/design/celeron/datashts/243658.htm

[2] Intel ® Pentium ® 4 Processor with 512-KB L2 Cache on 0.13 Micron Process at 2 GHz–3.06 GHz, with Support for Hyper-Threading Technology 1 at 3.06 GHz Datasheet, Dec. 2002, Document Number: 298643-006, 64.oldal

[3] Intel ®Pentium ®4 Processor in the 478-Pin, Package at 1.40 GHz,1.50 GHz,1.60 GHz,1.70 GHz,1.80 GHz,1.90 GHz and 2GHz Datasheet, April, 2002, Order Number:249887-003, 79.oldal

[4] Mobile Intel® Pentium® III Processor - M Datasheet, January 2003, Order Number: 298340-006, 75.oldal, www.intel.com/design/mobile/datashts/298340.htm

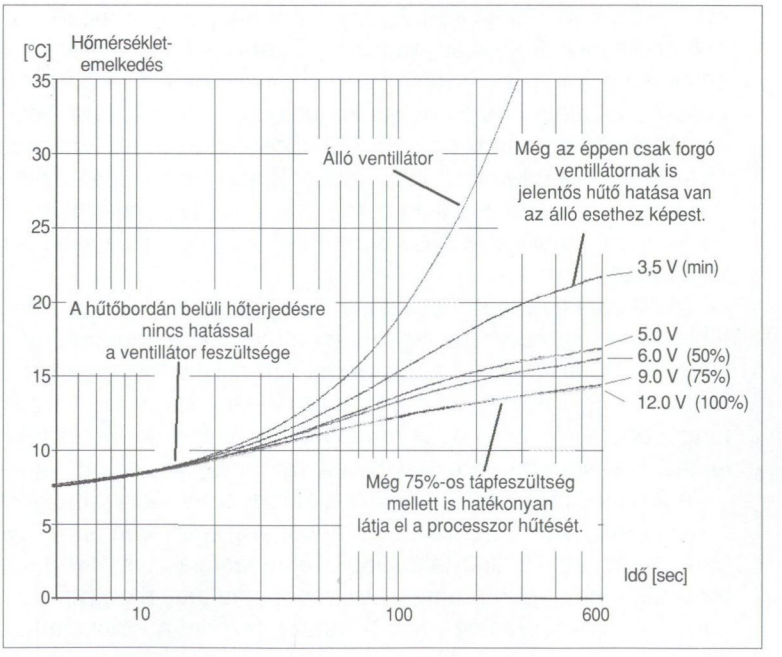
[5] Mobile Intel® Pentium® 4 Processor-M Datasheet, January 2003, Order Number: 250686-005, 89.oldal, www.intel.com/design/mobile/datashts/250686.htm

[6] T3Ster Hardware Reference Guide, Rev.1.6, 2nd Printed, July 2000, www.micred.com/t3ster.html

[7] T3Ster Booster, www.micred.com/booster.html

[8] www.globalwin.com.tw/new-product/fop38.html

[9] www.titan-cd.com/s101.htm



9. ábra
Különböző ventillátorfeszültségek mellett felvett tranziensgörbék

Hírek

Az EU-hoz csatlakozó országok számára versenyelőny lehet az új beruházások kényszere

Az Európai Unióhoz csatlakozó tíz ország számára az e-kormányzat és e-közigazgatás viszonylag egyszerű úton érhető el, mert ezeket nem terheli a nyugat-Európát jellemző bonyolult régebbi informatikai rendszerek „átkos öröksége", amely hátráltatja a fontos állami funkciók továbbfejlesztését. Nyugat Európában a meglévő architektúra áttekinthetővé tétele és modernizálása jelentős szervezeti – sőt, egyes esetekben a szabályozó környezetet érintő jogi – változtatásokat igényelhet. Ennek következtében becslések szerint minden euróból, amit technológiára költenek, 80 centet fordítanak a meglévő rendszerek karbantartására, és csak 20 cent jut az új technológia beszerzésére. A belépő országokban azonban mind a száz centet olyan innovatív technológiai megoldásokra lehetne költeni, amelyek folyamatos karbantartási költsége meglehetősen alacsony. Közelítő becslések szerint 2005-2006-ra a belépő országok közigazgatása ugyanolyan közel lesz az eEurópa célkitűzés teljesítéséhez, mint a jelenlegi EU-tagok többsége, és az e-kormányzat viszonylag könnyű kialakításának az alábbi megközelítés lehet a kulcsa:

„A számonkérhetőség és átláthatóság" elérése a Kelet-közép európai kormányzati és közigazgatási rendszerek modernizálása felé vezető első lépés. Ehhez olyan rendszerekre van szükség, amelyek kiemelten alkalmasak az EU-keretekből kapott pénzek kezelésére és felhasználásuk szigorú ellenőrzésére. A pénzügyi adminisztráció számítógépesítése mellett olyan humánerőforrás-rendszerek bevezetésével is javítani lehet a számonkérhetőséget, amelyek elősegítik a kormányzat és a közigazgatási dolgozók és biztosítják, hogy az utóbbiak átlássák és megértsék a vonatkozó előírásokat, figyelembe véve a változó jogi és szabályozói összefüggéseket.

„A költséggazdálkodás és keretellenőrzés" lehetővé teszi a belső hatékonyságot és a pénzek megfelelő, előírásos felosztását. Az EU bővítésének legutóbbi fázisában a csatlakozó országok gazdasági sikerei nagyban azon múltak, hogyan kezelték az EU pénzügyi támogatásait. Az Economist corporate Network 2002. decemberi elemzése szerint a csatlakozás lezárultával a növekedés feltétele a gazdaság stabilitása, valamint a további fejlődést szolgáló folyamatos szerkezetátalakítás. Írország például jól igazodott ehhez a felvételrendszerhez, és közel megkétszerezte az egy főre jutó GDP-t, elérve az EU átlagának 116 százalékát. Görögország viszont kezdetben nem ültette át a gyakorlatba ezeket az elveket, és most a ráfordítások gondos figyelésével és ellenőrzésével igyekszik elkerülni a korrupciót és a pazarló presztízsprojekteket.

„Lakossági és üzleti szolgáltatások." A kormányzati tevékenységeket kiszolgáló technológia megalapozása után érdemes előtérbe helyezni a külső kapcsolatok számítógépesítését megvalósító lakossági és vállalati kapcsolatokat (government-to-citizen, G2C és government-to-business, G2B). Ezt egy portálon keresztül célszerű megvalósítani, mely biztosítja az „egyablakos ügyintézéshez" szükséges közös kapcsolati pontot. Ezen az „ablakon" keresztül tarthatnak kapcsolatot a vállalkozások, a kormányzati beszállítók és az állampolgárok a helyi és központi kormányzat különböző hatóságaival. A World Markets Research Centre 196 ország 2288 kormányzati webhelyét vizsgáló elemzésében arra a következtetésre jutott, hogy „az egyablakos ügyintézés a hatóságokat és hivatalokat arra bátorítja, hogy egységesebb megközelítést alkalmazzanak a jelenlegi eltérő navigációs útvonalak és megjelenítési stílusok helyett." Ez a stratégia lehetővé teszi a csatlakozó országok számára a lakosságközpontú közigazgatás kialakítását. Itt kiemelt szerepet kap az elektronikus piactér és ehhez kapcsolódóan a közbeszerzés elektronizálása. A vállalati szférát érintő szolgáltatások (áfa, társasági adó stb.) online megvalósítását követően a kormányzat az olyan jellemzően lakosságközpontú tevékenységek felé fordulhat, mint az szja-bevallás, a lakcímnyilvántartás vagy az online munkaközvetítés.

„A telepítési modell kialakítása" a legutolsó lépés. Itt a siker központi tényezője az, hogy a szolgáltatások több csatornán keresztül legyenek elérhetőek. A hagyományos levelezés és személyes kapcsolattartás mellett ebben szerephez jut a telefonon, személyi adatkezelőkön, e-mailen és interaktív információs kioszkokon keresztüli ügyintézés. Ezáltal a kormányzat az összes állampolgár számára biztosítja a szolgáltatásokat, függetlenül attól, hogy azok rendelkeznek-e internetelérással és a szükséges technikai ismeretekkel. A csatlakozó országokban a mobil elérés válhat a legfontosabb kapcsolattartási csatornává.

A fentiek kiemelten vonatkoznak Magyarországra, ahol jelentős elmaradottság tapasztalható az elektronikus kormányzat használata és népszerűsége terén is. A Taylor Nelson Sofres (TNS) piackutató cég 2002-ben 28 ország 29 000 lakosának bevonásával készített felmérést az elektronikus kormányzati szolgáltatások elterjedtségéről (http://www.modus.hu/aktual/go.pdf), amely szerint e területen Magyarország zárja a mezőnyt 3%-os eredménnyel. A kutatás szerint a többi csatlakozó ország a rangsorban mind előkelőbb helyet foglal el.

WTLS-SSL protokoll konverzió

HORNÁK ZOLTÁN

BME Méréstechnika és Információs Rendszerek Tanszék
hornak@mit.bme.hu

Reviewed

Az Internet és a mobil eszközöket kiszolgáló WAP hálózat jól kiegészíti egymást, de a közöttük való átjárhatóság alapvető igény, melyet a WAP Gateway old meg. Azonban ha biztonságos, rejtjelezett átvitelt kívánunk megvalósítani (a tipikus mobil alkalmazások többsége – mobil bank, elektronikus vásárlás – pedig kifejezetten megköveteli a rejtjelezés alkalmazását) a protokoll-konverzió nem egyszerű megoldás, hiszen egy kódolt üzenetet kellene az egyik protokollról a másikra fordítani.
A publikáció a fenti problémára, a WTLS és SSL protokollok konverziójára mutat be megoldást. A protokoll konverzió során a rejtjel protokollok azonosítási, kézfogási (handshake) eljárását kellet olyan módon manipulálni, hogy a gateway a rejtjelezési folyamatba közbeékelődhessen, de a biztonság megőrzése miatt más (egy esetleges támadó) ezt ne tehesse meg.

1. Az alapok

A számítógépes rendszerek közötti elektronikus kapcsolat mára már szinte az Internetre és az internetes technológiákra korlátozódik. Ez alól azonban a mobil hálózatok adatátviteli megoldása, a WAP kivételt jelent. A WAP [1] lehetővé teszi, hogy a kisebb számítási kapacitású mobil telefonokról, vagy PDA-król is elérhető legyen a globális hálózat hatalmas információbázisa. Mivel a mobil hálózat nem kelhet versenyre a számítógépes hálózatok nagyobb sávszélességével, viszont biztosítja a teljes elérhetőséget, a két megoldás jól kiegészíti egymást.

A WAP hálózat és az Internet összeköttetését átjárókkal (gateway) oldották meg. Ezzel biztosítható, hogy a korlátozott képességű telefonokra már csak egy *hatékonyabb, egyszerűbb leíró nyelv,* illetve *jelentősen szűrt tartalom* jusson el. Ezen átjárók ennek megfelelően az internetes TCP/IP protokollokat és a HTML tartalmakat WAP protokollra, illetve WML tartalomra konvertálják. Ez a konverzió teszi lehetővé, hogy az egyszerű telefonokról az Internet komplex szolgáltatásai és részletdús oldalai is elérhetőek legyenek.

Ez az *átjárón alapuló megoldás* azonban azzal a hátránnyal jár, hogy a bevált, elterjedt binztonságos adatátvitelt szolgáló *rejtjelezési technikák nem alkalmazhatóak,* hiszen ilyenkor a tartalom a gateway előtt is rejtett, így a kódolt protokollok konverziója nem oldható meg.

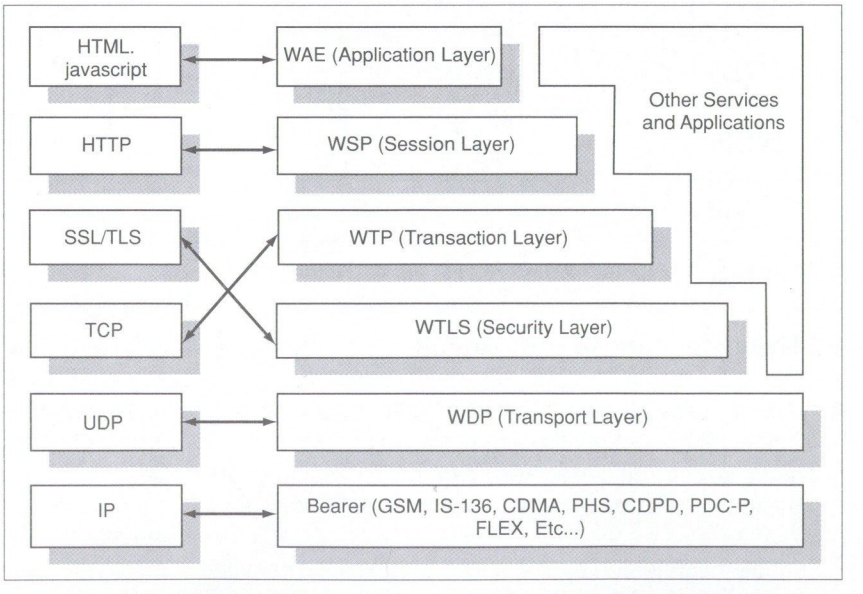
A cikk azt a szabadalmaztatott megoldást ismerteti, amely a WAP és az internetes *protokollok illetve a mobil telefonok és az internetes szerverek módosítása nélkül* oldja meg a mobil hálózatok szabványos WTLS rejtjel protokolljának [2] és az Internet de-facto szabványává vált SSL rejtjel protokolljának [3] a konverzióját.

1.1 A WAP és a TCP/IP protokollcsalád

A mobil adatátviteli rendszerek tervezésénél az Internet meglévő megoldásaiból indultak ki, azonban az internetes technológiát a korlátos sávszélesség és a kisebb feldolgozási kapacitás miatt nem lehetett közvetlenül alkalmazni. Így jött létre a WAP protokollcsalád, amely amit lehetett átvett az internetes megoldásokból, de kifejezetten a mobil környezetre adaptálva alkalmazta azokat. Ennek megfelelően a WAP hálózat rétegei funkcionalitásukat tekintve nagyjából megfeleltethetőek a TCP/IP protokollnak.

Összetartozó TCP/IP - WAP protokollok:

- **HTTP – WSP** (Wireless Session Protocol): Session kezelés
- **SSL – WTLS** (Wireless Transport Layer Security): Rejtjelezett kommunikáció
- **TCP – WTP** (Wireless Transport Protocol): Megbízható, nyugtázott adatátvitel



1. ábra TCP/IP protokollok és WAP megfelelőik

- **UDP – WDP** (Wireless Datagram Protocol): Nyugtázás nélküli, datagram üzenet
- **IP – Bearer:** Átviteli réteg. Többféle lehet: CSD, SMS, USSD, GPRS, ...

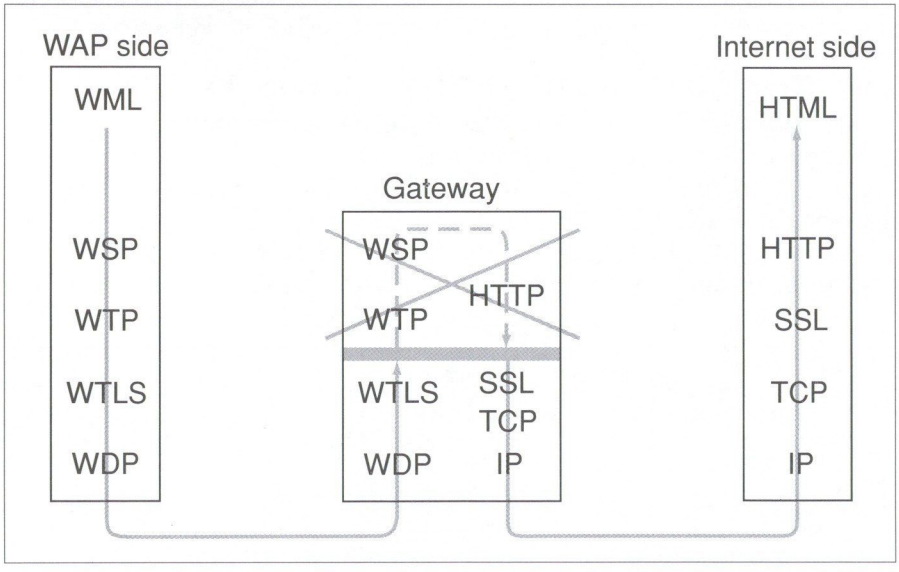
A leglényegesebb eltérés a rejtjelezést megvalósító SSL és WTLS rétegek elhelyezkedésében van. Ugyanis, amíg az SSL a TCP rétegre épül, addig a WTLS az összeköttetés-mentes, nyugtázás nélküli WDP rétegre épül, és így a megbízható átvitelt megvalósító WTP réteg alatt helyezkedik el.

1.2 Konverziós problémák

Mivel a WTLS tervezésekor is figyelembe vették a már létező megoldásokat, így a WTLS protokoll specifikációja nagy mértékben azonos az SSL szabványként elfogadott TLS (Transport Layer Security [6]) utódjával (a specifikáció szövegének nagy részét változtatás nélkül átvette a WTLS a TLS-től).

A részletes összehasonlítás azonban számos olyan lényegesnek bizonyuló eltérést mutat, amely miatt még kisebb módosítások árán sem oldható meg, hogy egy SSL rejtjel réteg egy WTLS réteggel kommunikáljon.

E felépítés következtében a gateway koncepció azért nem működik, mert a WTLS, illetve az SSL rétegek fölé nem tud menni a kommunikációs folyamat, hiszen a kódolt üzenetet a gateway sem értheti meg és így a WSP ↔ HTTP konverziót sem tudja végrehajtani *(2. ábra)*.



2. ábra Rejtjelezés miatt a gateway koncepció nem működik

1.3 Nyilvános kulcsú protokollok

A nyilvános kulcsú módszereket alkalmazó rejtjelezési protokollok felépítésükben többnyire hasonlóak: ötvözik a nyilvános kulcsú rejtjelezés kényelmi megoldásait a gyors és hatékonyan alkalmazható szimmetrikus rejtjelezési technikákkal.

Ennek megfelelően egy rejtjelező protokoll két nagy lépésre bontható. A kézfogás (handshake) eljárásra, amely során a kommunikákáló felek azonosítják egymást és nyilvános kulcsú kriptográfia segítségével egyeztetnek egy közös titkot, amelyet a későbbi szimmetrikus rejtjelezés ideiglenes kulcsaként használnak majd fel.

A továbbiakban pedig a tényleges adat-rejtjelezést az egyeztetett titkos kulcs felhasználásával általában már gyors, hatékony szimmetrikus retjelezéssel (bulk encryption) oldják meg. Ez a megoldás kiküszöböli a nyilvános és szimmetrikus rejtjelezések hiányosságait és ötvözi a módszerek előnyeit, ezért a legtöbb rejtjelezési rendszernél így járnak el.

A nyilvános kulcsú kódolást alkalmazó kézfogáshoz a kommunikáló feleknek rendelkezniük kell egy titkos-nyilvános kulcspárral. A nyilvános kulcsokat és jogos tulajdonosukat szigorúan és biztonságosan egymáshoz kell rendelni.

Ezt a célt szolgálja a nyilvános kulcsú infrastruktúra, a PKI (public key infrastructure [4]), amely tanúsítványokkal (certificate) igazolja *a személyek személyazonosságának és nyilvános kulcsuknak az összetartozását.* A tanúsítványokat a hitelesítő központok (CA - Certification Authority) állítják ki, miután meggyőződtek a tanúsított személy kilétéről.

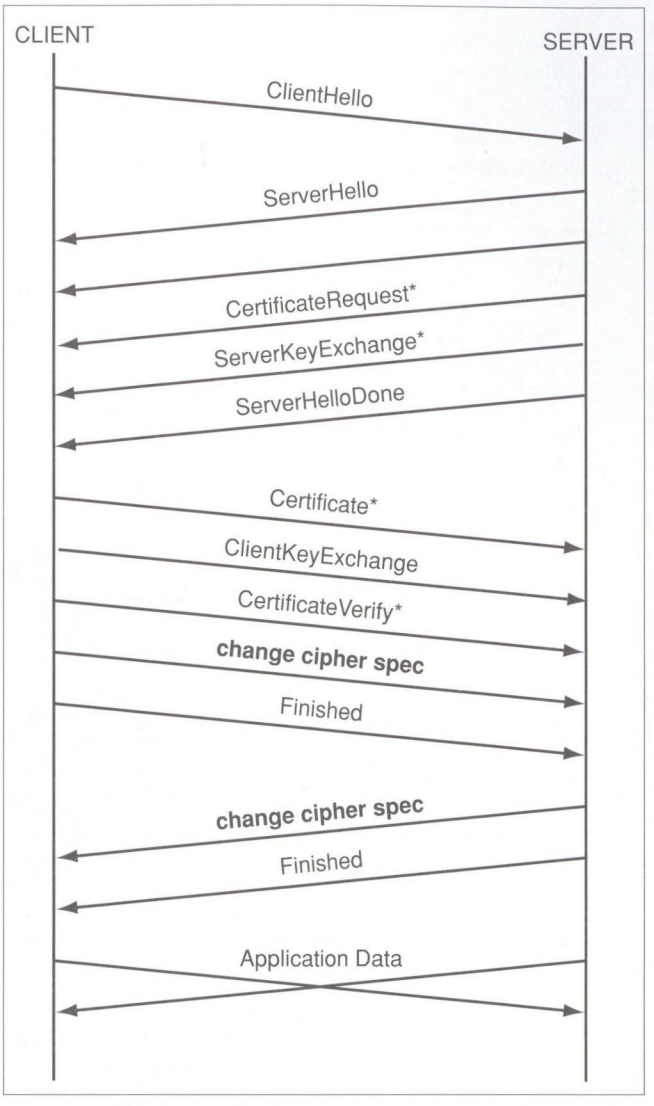
A PKI segítségével így egy személy nevét és nyilvános kulcsát tartalmazó tanúsítványának hitelességéről úgy lehet meggyőződni, hogy a CA ismert és megbízható forrásból beszerzett nyilvános kulcsával a tanúsítványon lévő digitális aláírás hitelességét ellenőrizni kell. Ezzel a módszerrel olyan megoldás készíthető, ahol az egyik félnek elegendő egy CA nyilvános kulcsát megbízhatóan, hiteles forrásból ismernie és ebből az információból kiindulva megfelelő tanúsítvánnyal rendelező felekkel biztonságos kapcsolatot tud kialakítani.

1.4 Az SSL és a WTLS működése

Az előzőekben ismertetett általános elveknek megfelelően működik az SSL és a WTLS protokoll is. A két alréteg egyike a „handshake process", a kommunikáló felek azonosítását és az ideiglenes rejtjel kulcs(ok) egyeztetését végzi, a másik a „record layer", a továbbított adatfolyamot szimmetrikus kódolással rejtjelezi [5,6,2].

Mindkét protokoll aszimmetrikus, azaz jelentősen megkülönbözteti a kapcsolatot kezdeményező kliens (client) szerepét a kiszolgáló szerver (server) működésétől. Az eltérő felépítésű üzeneteken (handshake messages) túl az azonosítás módja is eltérő a kliens és a szerver esetében.

A kézfogás során lebonyolított üzeneteket a *3. ábra* mutatja be. Az azonosítási mechanizmusok a bemutatott protokoll konverzió tekintetében fontos szerepet játszanak, ezért tekintsük át őket részletesebben.



3. ábra SSL kézfogás üzenetei (handshake messages)

Szerver azonosítása

A szervert a kliens több lépésben áttételesen azonosítja. Az első `ClientHello` kapcsolatfelvételi üzenet hatására a szerver a `ServerHello` üzenetet követően elküldi a nyilvános kulcsát és azonosítását (nevét, IP címét) tartalmazó tanúsítványát a kliensnek (`Certificate` üzenet). A CA nyilvános kulcsának ismeretében így a kliens a tanúsítvány hitelességéről az aláírás ellenőrzésével meg tud győződni.

Ezt követően a kliens generál egy véletlen számot (`pre_master_secret`), amit a szerver nyilvános kulcsával kódolva küld át a hálózaton a `ClientKeyExchange` üzenetben. Ezt az üzenetet csak az képes megfejteni aki a kódoláshoz használt nyilvános kulcshoz tartozó titkos kulcsot ismeri, azaz kizárólag a valós szerver. A szerver úgy igazolja a kliens felé, hogy az adott véletlen számot dekódolni tudta, hogy a későbbi rejtjelezési lépéseknél ebből a véletlen számból (`pre_master_secret`) képzett `master_secret`-et használja kódolási kulcsként.

Ez az azonosítási mód áttételes, hiszen egy álszerver vagy egy támadó tevékenysége csak abból derül ki, hogy a későbbi kódolt üzenetek dekódolásánál hiba keletkezik.

Kliens azonosítása

A szerver azonosításánál a nyilvános kulcsú rejtjelezés azon funkcióját használtuk ki, hogy egy nyilvános kulccsal kódolt üzenetet csak a titkos kulcs birtokosa tud visszafejteni.

Ezzel szemben a kliens azonosításakor a személyét igazolni kívánó kliens az elküldött (és kötelezően több véletlenszámot is tartalmazó, tehát mindig más) handshake üzeneteket a titkos kulcsa segítségével digitálisan aláírja és a digitális aláírást a `ClientVerify` üzenetben továbbítja a szerver felé. A szerver a kliens elektronikus igazolványát és így a benne szereplő nyilvános kulcsát a korábbi `Certificate` üzenetből kinyerve képes a digitális aláírás hitelességét ellenőrizni. A nyilvános kulcsú kriptográfia biztosítja, hogy a digitális aláírást csak a tanúsítványban található nyilvános kulcshoz tartozó titkos kulcs birtokosa, azaz kizárólag a valós kliens készíthette.

Vegyük észre, hogy a két azonosítási mód – bár a konkrét handshake üzenetekben kombinálva vannak – egymástól függetlenek. Mivel a későbbi szimmetrikus kulcsú titkosításhoz szükséges ideiglenes rejtjelkulcs egyeztetéséhez pusztán a kliens által generált `pre_master_secret` véletlen szám, illetve annak dekódolása szükséges – ami pedig csak a szerver titkos kulcsának meglétét feltételezi, a kliensét nem – a kliens azonosításának lépése elhagyható. A Interneten számos esetben élnek is ezzel a lehetőséggel, amikor csak a szerver azonosítja magát, míg a kliensnek (látogatónak) szükségtelen kilétét felfednie.

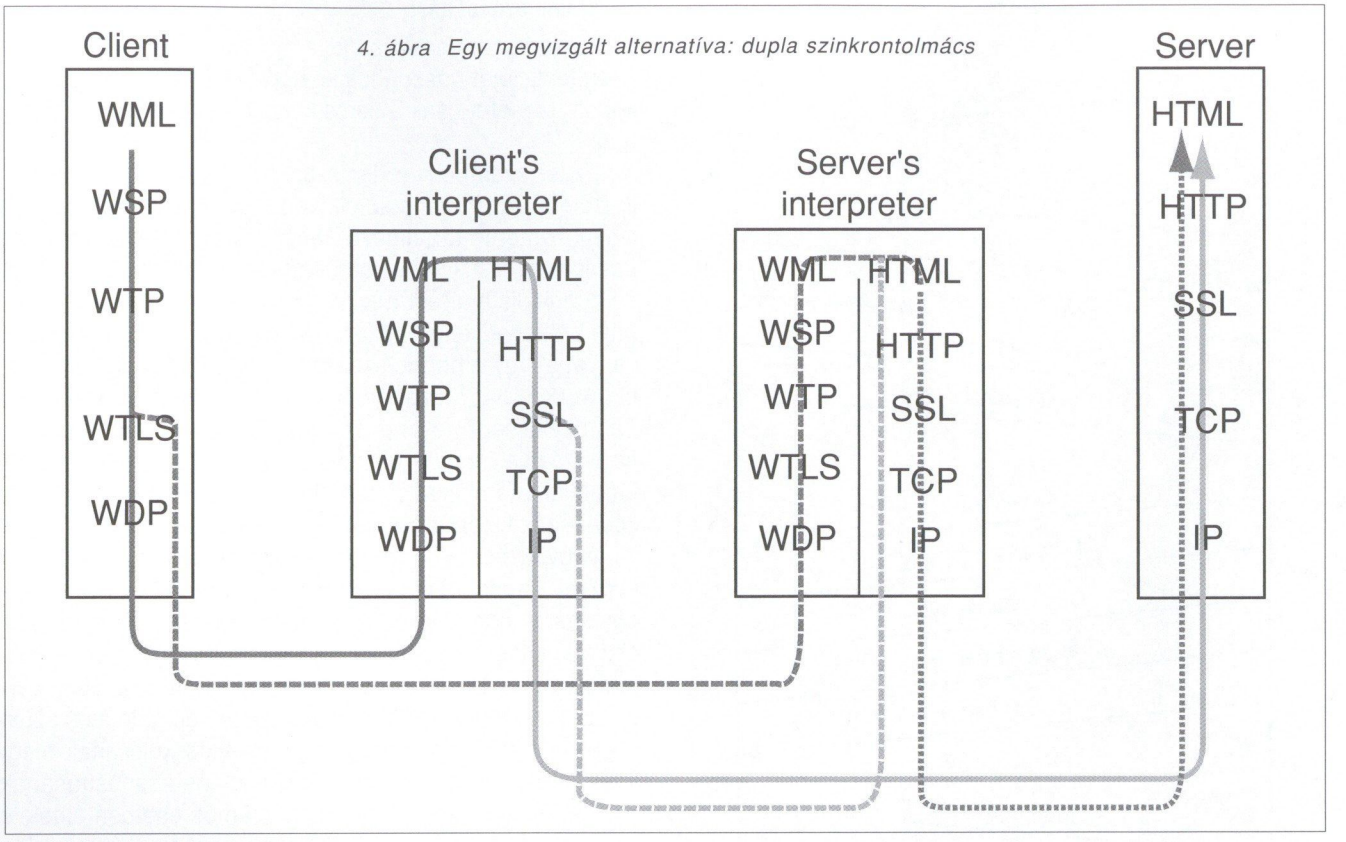
A handshake process ábráján (3. ábra) csillaggal vannak megjelölve azon opcionális üzenetek, amelyekre nincs szükség, amikor kizárólag a szerver kerül azonosítására. A kézfogási eljárás végére így a WTLS és SSL protokollok a rejtjelezett paramétereit (a rejtjel algoritmust, a MAC eljárást, a kulcshosszt és az ideiglenes kulcsot) egyeztetik és opcionálisan meggyőződnek a kommunikáló felek kilétéről.

2. A probléma megfogalmazása

A célul kitűzött protokoll konverzió során tehát olyan eljárást kellett kidolgozni, amely eredményeként a WTLS kliens meg tud győződni arról, hogy az SSL szerverrel kommunikál, míg fordítva a szerver meg tud győződni arról, hogy a klienssel kommunikál. A handshake eredményeként pedig a rejtjelezést úgy egyeztetik, hogy a kívánt üzenettartalom eljusson az egyik féltől a másikhoz, miközben egy támadó nem tud a kódolt információhoz hozzáférni és a kommunikáló feleket sem tudja megszemélyesíteni.

2.1 A WTLS és az SSL összehasonlítása

Első lépéseként annak lehetőségét vizsgáltam, hogy a WTLS és az SSL azonos rejtjelezési algoritmusban és azonos ideiglenes kulcsban egyezzenek meg, azaz a record layer-ek tudnak-e egymással kommunikálni. Tekintve, hogy a két protokoll specifikációja szövegezésük



4. ábra Egy megvizgált alternatíva: dupla szinkrontolmács

nagy részében azonos, a különbségek feltérképezése nyújtott kiinduló alapot az adott cél megvalósíthatóságának elbírálására.

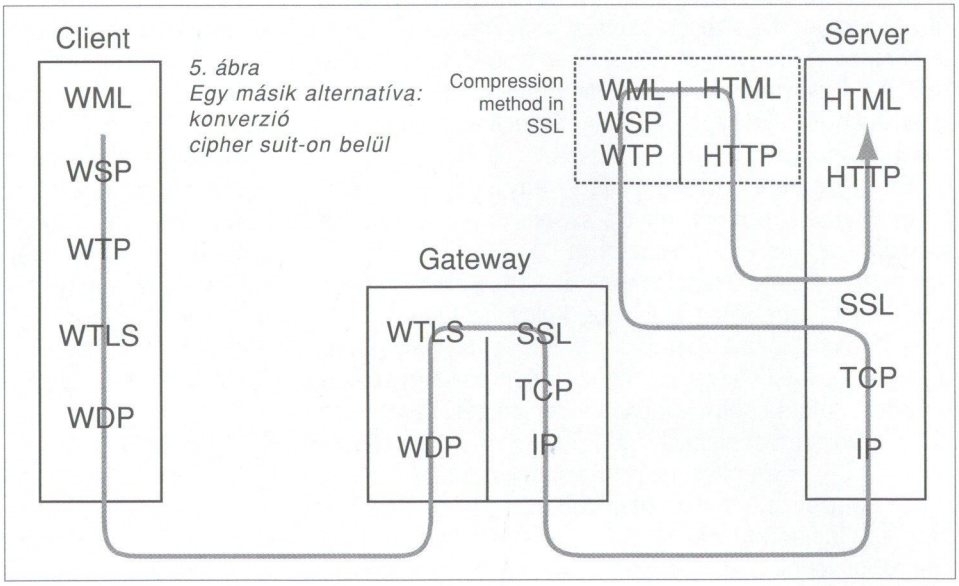
Számos olyan apró eltérés található a WTLS és az SSL között, amely esetleg „apró trükkökkel" áthidalható lehetne, de a legfontosabbanak talált különbség gyakorlatilag kizárta a két protokoll egymásba konvertálását. A handshake process során az SSL 48 byte hosszúságú `master_secret`-et (ideiglenes kulcsot), míg a WTLS csupán 20 byte hosszú ilyen közös titkot állít elő. Tekintve, hogy a `pre_master_secter` → `master_secret` számítás is jelentősen eltér a két esetben, még a hosszabb SSL `master_secret` 0-kal való feltöltése sem járhatna eséllyel.

Ezért mivel *a direkt WTLS – SSL protokoll konverzió megvalósíthatatlannak bizonyult,* egyértelművé vált, hogy a WTLS kliensnek feltétlenül WTLS szerver réteggel, míg az SSL szervernek SSL klienssel kell kommunikálnia. Még ebben az esetben is számos probléma merül fel például abból, hogy az SSL megbízható réteg fölött működik, míg a WTLS megbízhatatlan datagram réteg fölött.

A végső megoldásnál természetesen ezekre a felmerült problémákra is választ kellett találni.

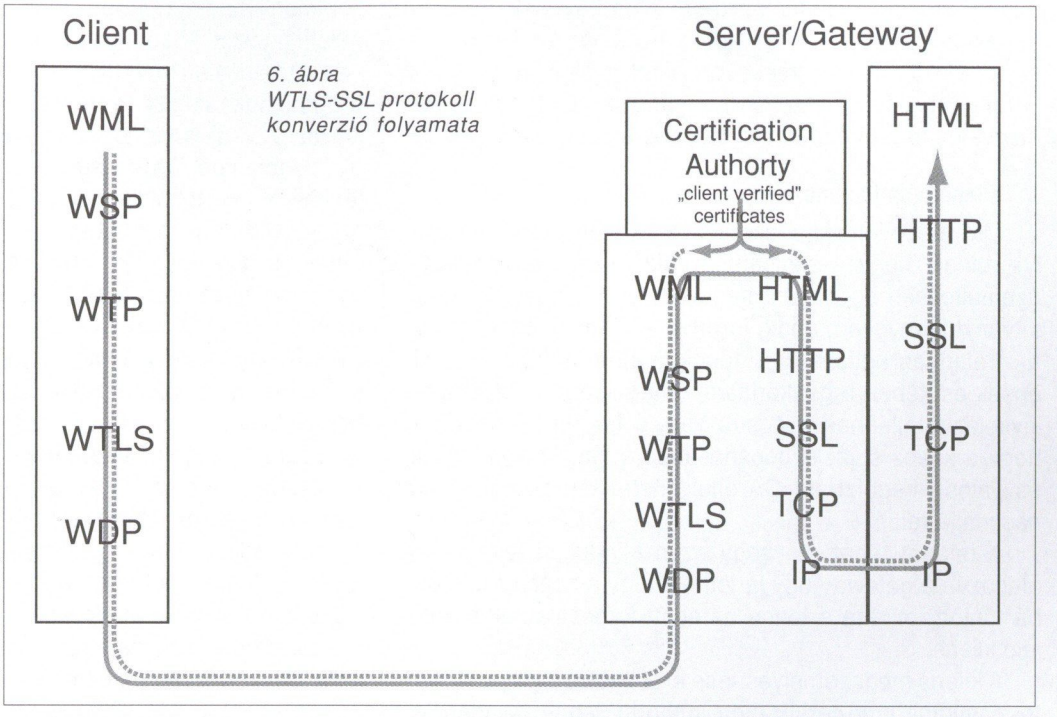
2.2 Alternatív megoldások

A korábbi gondolatmenetnek megfelelően mind a kliens WTLS réteghez, mind a szerver SSL réteghez a megoldást nyújtó rendszerben valahol meg kell lennie a WTLS szerver és SSL kliens pároknak. E rétegek elhelyezkedését tekintve számos lehetőség adódik a rejtjel protokollokba ágyazott speciális rejtjel-sűrítési algoritmusoktól a kliens vagy a szerver protokoll stackjének átírásán át az alkalmazói szinten megvalósított konverzióig. Az alternatívákat egy referencia modell segítségével alaposan végigvizsgálva (példák: *4. és 5. ábra*) adódott a javasolt megoldás, amely a többihez képest egyértelműen a legjobb megoldást nyújtotta.



5. ábra
Egy másik alternatíva: konverzió cipher suit-on belül

2.3 A javasolt megoldás



6. ábra
WTLS-SSL protokoll konverzió folyamata

A lehetőségek vizsgálata után a legjobbnak talált megoldás működési folyamata a *6. ábrán* látható.

Az ábrából az olvasható ki, hogy a működési folyamat a klaszszikus gateway koncepciót követi. Azaz a kliens a gateway-jel kommunikál, miközben azt hiszi, hogy a szerver áll a rejtjel kapcsolat túloldalán, illetve fordítva a szerver úgy érzékeli, hogy a gateway a kliens. Vagyis a gateway egy tipikus man-in-the-middle támadónak felel meg, amely támadási módot a rejtjel protokollnak nagy megbízhatósággal ki kellene zárnia. A javasolt megoldás alapötlete pontosan ez. Állítsuk be úgy a rejtjel protokollok feltételeit, manipuláljuk úgy a kulcsmenedzsment lépéseit, hogy a gateway-nek lehetővé tegyük a man-in-the-middle jellegű „támadás" kivitelezését, míg mások számára ezt a lehetőséget továbbra is zárjuk ki.

Tekintve, hogy a szerver és a kliens azonosítási módszerei és gyakorlati problémái jelentősen eltérőek, más módszer az előnyös a kliens, és más a szerver „megtévesztésére".

Szerver oldali azonosítás

Számos alternatívát végigvizsgálva az a megoldás adódik, hogy

a) vagy a gateway is rendelkezzen a szervert azonosító titkos kulccsal;

b) vagy a szerver nevére kibocsátott certificate-je (is) legyen a gateway-nek.

Az a) eset akkor járható út, ha a gateway azonos gépen fut, mint maga a WEB szerver, hiszen ilyenkor még abban az esetben is biztosítható a titkos kulcs közös használata, ha annak tárolását fizikailag védve (tipikusan valamilyen HW kripto-kártyán) tárolják.

A b) esetben az a kérdés, hogy a gateway-nek a szerver nevére kibocsátott tanúsítványa a Certification Authority szabályaival, a tanúsítvány kibocsátási politikájával mennyire ütközik. Amennyiben a gateway és a WEB szerver tulajdonosa azonos, nincs elvi akadálya annak, hogy a szerver üzemeltetője a CA-tól ilyen tanúsítványokat igényeljen.

Azonban, ha a gateway harmadik fél birtokában van, és esetleg több ügyfél számára is nyújt ilyen WAP – TCP/IP konverziós szolgáltatást, akkor ennek a megoldásnak az alkalmazása kérdéses. Ugyanis azon felül, hogy komoly bizalmi kérdéseket vet fel, hogy a szerver egy harmadik fél nevében eljárjon, a megoldás szerint pedig egy tanúsítványt más nevében bocsásson ki. Ez még az adott cég explicit kérésére is a CA-k alapszabályába ütközik. Amennyiben a szerver és a gateway azonos tulajdonban vannak, olyan tanúsítványokat használhatnak, amelyek tartalmából egy felhasználó számára világosan kiderül, hogy a kommunikációba egy gateway is beavatkozik, de a WTLS és az SSL protokollok szempontjából a megoldás transzparens marad.

Ez megoldható például úgy, hogy a gateway- és a szerver certificate-ban az azonosított fél IP címe (CN - common name mezője) azonos, míg a természetes név kifejezi, hogy a valós szervert vagy csak a gateway-t azonosítja-e a rejtjelező réteg. Példa egy összetartozó gateway és szerver tanúsítványainak „`Subject Name:`" mezőjére:

Szerver: `c=HU, o=BME, ou=SEARCH Laboratory, cn=www.search-lab.hu`

Gateway: `c=HU, o=BME, ou=SEARCH Laboratory WAP GW, cn=www.search-lab.hu`

Mivel ilyenkor a rejtjelezési réteg csak azt ellenőrzi, hogy a CN-ben megadott IP címmel kommunikálnak-e, a név többi részében esetleges változások nem befolyásolják a működését. A felhasználó számára azonban nem az IP cím, hanem a szervezet neve (OU, organizational unit) jelenik meg a képernyőn, amely egyértelműen feltüntetheti, hogy ez a tanúsítvány a gateway-nek és nem a szervernek szól. Esetünkben „SEARCH Laboratory" vagy „SEARCH Laboratory WAP GW". A manipulált tanúsítvány elfogadása vagy éppen a visszautasítása a felhasználó hatásköre.

A fenti megoldás egyszerű, olcsó lehetőséget kínál olyan ügyfelek számára, akik WAP-on keresztül is biztonságos hozzáférést kívánnak nyújtani a már meglévő

TCP/IP alapú szolgáltatásaikhoz. Ilyen ügyfelek tipikusan a bankok (home banking, mobile banking), bróker cégek, és az elektronikus kereskedelemmel foglalkozó portálok. Számukra a fenti biztonságos gateway szolgáltatásokat megvalósító terméknek van létjogosultsága, illetve piaca.

Kliens oldali azonosítás

Míg a szever oldali azonosításnál van gyakorlati esélye annak, hogy a szolgáltató saját tulajdonú gateway-t üzemeltessen és abban megbízva hozzá speciális tanúsítványt igényeljen, addig fordítva a kliensek esetében ez a – relatívan egyszerű – megoldás nem járható út. A kliensek esetében a gyakorlatban a legkisebb módosítás is kivitelezhetetlennek minősül. Vagyis fel kell tételeznünk, hogy a kliens saját azonosításához a saját titkos kulcsát és valós, megbízható CA által hitelesített tanúsítványát használja fel.

A feladat tehát az, hogy ezen kiindulási feltételekre alapozva a gateway úgy járjon el, hogy a szerver felé olybá tűnjön, mintha ő lenne az adott kapcsolatnak megfelelő kliens.

A kliens megszemélyesítése érdekében a gateway úgy tesz, mintha egy certification authority lenne. Minden klienshez készít egy saját titkos-nyilvános kulcspárost és ehhez a kulcshoz kiállít saját magának – de a kliens nevében – egy tanúsítványt. Ez a tanúsítvány hamis, érvénytelen lesz a külvilág számára, hiszen a gateway maga ezzel nem válik megbízható, elfogadott CA-vá, csupán technikai szempontból tesz úgy, mintha az lenne. Viszont a birtokában lévő titikos kulccsal és a kliens nevére kiállított tanúsítvánnyal már kezdeményezhet SSL rejtjel kapcsolatot, eljátszva a szerver felé, hogy ő maga a kliens.

A szerver oldalon az SSL rejtjel protokoll ezután technikailag tökéletesen képes végrehajtani a kézfogás eljárást, mindössze akkor ütközik hibába, amikor a kliens tanúsítványán a digitális aláírást ellenőrizni akarja, hiszen a kibocsátó – esetünkben a gateway – nyilvános kulcsa nem szerepel a megbízható CA-k listáján.

Az így jelenkező „hiba" kezelésére két lehetőség adódik:

a) Hiba lekezelése alkalmazói szinten, úgy, hogy az SSL kézfogás ne szakadjon meg.
b) Gateway felvétele a megbízható CA-k listájára.

Az a) megoldás eseti, programozói beavatkozást igényel, míg a b) eset egyszerűen járható. Amennyiben a gateway megbízható (a szerver oldali azonosításánál láttuk, hogy célszerűen a szolgáltató tulajdona a gateway is) és biztosítható, hogy csak olyan kliens nevében állítson ki magának tanúsítványt, akinek azonosságáról meggyőződött, akkor nem veszélyezteti a biztonságot. A WTLS-SSL konverziónak a kliens megszemélyesítési lépése így gyakorlatilag a szerver módosítása nélkül, mindössze a megbízható CA-k listájának egy bejegyzéssel való bővítésével megoldható.

Magában foglalt tanúsítvány (Embedded Certificate)

A fenti lépéssorozatok eredményeként a szereplők számára úgy fog tűnni, mintha minden azonosítási lépés rendben megtörténne és a kívánt féllel biztonságosan kommunikálnának. Az egyetlen eltérés a valós és a manipulált helyzet között az alkalmazott nyilvános kulcsban van. Amennyien valamilyen alkalmazói szinten működő programnak szüksége lenne a kliens valódi nyilvános kulcsára, vagy a valódi tanúsítványára, amelyet egy valódi, megbízható CA bocsátott ki, ez a követelmény is teljesíthető a protokollok módosítása nélkül.

Az X.509-es formátum [7], amelyet a certificate-ek leírására alkalmaznak, lehetővé teszi, hogy a tanúsítványokhoz tetszőleges kiterjesztéseket fűzzenek hozzá. Ezt a lehetőséget kihasználva a gateway az újonnan készített tanúsítványhoz hozzá tudja csatolni, a kliens eredeti tanúsítványát, mint kiterjesztést, amikor egy új tanúsítványt bocsát ki maga számára a kliens nevében.

Ezzel a megoldással elérhető, hogy a szerveren futó alkalmazás, amikor lekérdezi az SSL rétegtől a kliens tanúsítványát, észrevegye, hogy egy gateway által kibocsátott – nem valós – certificate-tel van dolga és a kiterjesztésből megkaphassa a kliens eredeti tanúsítványát. Ez ugyan minimális módosítást kíván a szerver oldali alkalmazói programtól, de azon kevés helyen, ahol ilyen jellegű igények felmerülnek ez elkerülhetetlen és vállalható.

Összefoglalás

Összegyűjtve, a javasolt megoldás a következő lépésekkel oldja meg a WTLS-SSL konverziót:

- A gateway-nek rendelkeznie kell egy „szerver titkos-nyilvános kulcspárral" (S_t, S_{ny}).
- A szerver CA-jától tanúsítványt kell igényelni a gateway „szerver nyilvános kulcsához" (S_{ny}) a valós szerver nevében.
- A gateway-nek rendelkeznie kell egy „CA titkos-nyilvános kulcspárral" (CA_t, CA_{ny}).
- A szerveren a gateway „CA nyilvános kulcsát" fel kell venni a megbízható CA-k listájára.
- A gatewaynek minden klienshez generálnia kell egy „kliens titkos-nyilvános kulcspárt" (K_t, K_{ny}).
- Miután a klienst tejles bizonyossággal azonosította a gateway (WTLS kézfogás lefolytatása és az adott tanúsítványok digitális aláírásainak ellenőrzése után) a „CA titkos kulcs" (CA_t) segítségével a „kliens nyilvános kulcshoz" (K_{ny}) a kliens nevében készít egy új tanúsítványt, amelyhez a kliens eredeti WTLS tanúsítványát kiterjesztésként hosszáfűzi.
- A gateway az így készült tanúsítványa és a „kliens titkos kulcs" segítségével már el tudja hitetni a szerver SSL rétegével, hogy ő a kliens.
- Amennyiben a szerveren alkalmazói szinten egy program a kliens valódi nyilvános kulcsához szeretne hozzájutni, azt ki tudja olvasni a gateway által kibocsátott tanúsítvány kiterjesztéséből.

3. Értékelés

A kidolgozott eljárás egy olyan égető problémára nyújt a gyakorlatban is kivitelezhető megoldást, amely első ránézésre megoldhatatlannak tűnt. A javasolt megoldás termékként, illetve egy termék opcionális szolgáltatása-

ként hasznosítható, amely termékre, szolgáltatásra igény jelentkezik az ügyfeleknél.

A megoldás megfelelőségét azonban további technikai szempontokból is célszerű megvizsgálni.

Biztonsági megfontolások

Felmerül a kérdés, hogy ha a rejtjel protokollok környezeti feltételeit úgy manipuláljuk, hogy a gyateway gyakorlatilag man-in-the-middle, közbeékelődő „támadást" tud végrehajtani, akkor nem nyílik-e meg ez a lehetőség más támadók felé, illetve a javasolt megoldás nem hordoz-e magában olyan lehetőségeket, amelyeket egy támadó esetlegesen ki tud használni.

A válasz egyértelműen nem. Ugyanis mind a szerver oldali azonosításánál, mind a kliens oldali azonosításnál olyan megoldásokkal tettük lehetővé a gateway számára a közbeavatkozást, amely nem nyit lehetőséget egy támadó felé:

- Egy támadó nem szerezhet a birtokában lévő titkos-nyilvános kulcspárhoz a szerver nevére szóló tanúsítványt, hiszen ennél a lépésnél egy megbízható CA garantálja a biztonságot.
- A másik esetben egy támadó nem kerülhet fel a szerver által megbízhatónak minősített CA-k listájára. Oda egyedül a gateway-t szabad felvenni, egyértelműen csak számára lehetővé téve a manipulálást.

További biztonsági probléma lehet például a gateway által az egyes kliensek számára generált titkos-nyilvános kulcspárok minősége. Amennyiben ezen kulcsok előállításához gyengébb véletlenszám-generátort alkalmaz a gateway, mint amit a kliens használt, akkor ez csökkentheti a biztonságot.

További veszély adódhat még magából a rejtjel konverzióból is, ugyanis a javasolt megoldásnál a továbbított azonos tartalmú adatcsomagokat különböző kulcsokkal kódoljuk a kliens és a gateway között, illetve a gateway és a szerver között. Bizonyos rejtjel algoritmusok esetén ugyanannak a tartalomnak az eltérő kulcsokkal való kódolása törésre adhat lehetőséget. Biztosítani kell tehát, hogy ilyen rejtjel algoritmusokat az adott megoldás mellett ne alkalmazzanak, vagy a gateway és a szerver közötti kommunikációt tegyék fizikailag védetté, nem lehallgatható belső hálózat alkalmazásával.

Teljesítmény megfontolások

A legtöbb számítási kapacitást igénylő művelet vitathatatlanul a rendkívül sok, minden kliens számára különböző titkos-nyilvános kulcspárok előállítása. A különböző nyilvános kulcsú algoritmusoknál *a kulcsgenerálás rendkívül lassú művelet.* A legelterjedtebb RSA esetében például nagy prímszámokat kell keresni, amely lépésnek az ideje nem determinisztikus, sőt még csak nem is korlátos. Méréseink során egy szerencsétlen esetben az is előfordult, hogy egy 1024 bites RSA kulcs előállításához négy percre volt szükség! Ez az idő egy kiszolgáló jellegű eszköznél fennakadásokat okozhat.

Szerencsére a kulcsgenerálás lépése időben is és térben is elhatárolódhat a gateway működésétől. Azaz a kulcsok előállítása végezhető folyamatosan a háttérben, akár speciális HW kiegészítő kártyán, sőt másik számítógépen is (jók a párhuzamosítási lehetőségek).

A dekódolás-kódolás tekintetében, mivel a műveletek elkerülhetetlenek a párhuzamosítás, vagy esetlegesen a pipeline működés jelenthet megoldást. Méréseink szerint a gateway teljesítménye mindössze fele, harmada egy rejtjelezéses WEB szervernél.

Prototípus megvalósítás

A módszer működőképességének igazolására készült tesztelés során az SSLeay (mai nevén OpenSSL) programkönyvtár segítségével SSL és TLS protokollok között hajtott végre konverziót. A sikeres futások bizonyították, hogy a kidolgozott eljárás nem csak WTLS és SSL esetén, hanem a hasonló nyilvános kulcsú azonosítási módszerekre épülő esetekben is sikerrel alkalmazható.

Referenciák

[1] „WAP Architecture Specification", WAP Forum, 30-April-1998., URL: http://www.wapforum.org/

[2] „Wireless Transport Layer Security Specification", WAP Forum, 30-April-1998. URL: http://www.wapforum.org/

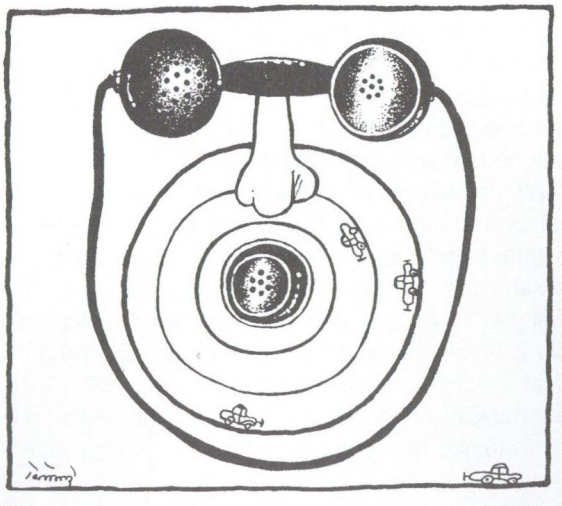
[3] „Introduction to SSL", Netscape Communication Inc. URL: http://www.netscape.com/docs/manuals/security/sslin/contents.htm

[4] „Introduction to Public-Key Cryptography", Netscape Communication Inc., URL: http://www.netscape.com/docs/manuals/security/pkin/contents.htm

[5] „The SSL Protocol Version 3", Netscape Communication Inc. URL: http://www.netscape.com/eng/ssl3/ssl-toc.html

[6] „The TLS Protocol Version 1.0", Internet Society, RFC 2246, January 1999 URL: ftp://ftp.isi.edu/in-notes/rfc2246.txt

[7] „Internet X.509 Public Key Infrastructure Certificate and CRL Profile." R. Housley, W. Ford, W. Polk, D. Solo, RFC 2459, January 1999. URL: ftp://ftp.isi.edu/in-notes/rfc2459.txt



Könyvet ajánlunk

Az európai szabványosítás áttekintése

Bár a szabványosítás története több mint 100 évre tekinthet vissza, jelentősége azonban az utóbbi időben jelentősen megnövekedett. A különböző nagy berendezések elemei csak akkor gyárthatók gazdaságosan, ha különböző összeszerelő vállalatok azonos alkatrészekből építkeznek. A kellő mennyiség a tömeggyártásban általában nagyobb, mint amennyit egy ország fel tud használni. Ezt látjuk nemcsak a távközlésben, hanem az autóiparban is, ahol bármilyen típushoz szoktunk hozzá, átülve egy másik autóba nem okoz gondot a sebességváltás, vagy az irányjelzők kezelése, mert mindez szabványok szerint készült.

A szabványosításon belül az elektrotechnikai területnek különleges jelentősége van. Itt az egységességen kívül a biztonsági feltételeket is célszerű rögzíteni. Magyarországon érdekes módon a valahai Szabványhivatal működésén belül is külön volt egy elektrotechnikai terület, amely kiemelt szerepet kapott. Az elektromos eszközök és rendszerek szabványosítása éppen az élet- és tűzvédelem miatt sok lényeges, közös jellemzőt szabványosított. Erre nem volt szükség sem a vegyiparban, sem az élelmiszeriparban.

A közös európai szabványosítás is hasonló eljárásokat követ. A CEN, az Európai Szabványosítási Testület mellett megjelent a CENELEC, amely az európai elektrotechnikai szabványokkal foglalkozik. Még további szakosodásnak lehetünk tanúi az 1980-as évek végén, amikor a CENELEC mellett a távközlési berendezések egységesítésére létrehozták az ETSI-t, az Európai Távközlési Szabványintézetet.

Ezen előzmények ismeretében érdekes és hasznos olvasmányt jelent a 2002-ben megjelent „Primer on Standards" című kiadvány, melyet a European Committee for Electrotechnical Standardization, a European Commission és az EFTA támogatásával adott ki.

A könyv hat fejezetben igyekszik mindenkihez közel hozni a szabványosítási munkát, a szabványok használatát, megvalósítva azt a célt, hogy a jövőben a szabványok ne legyenek titokzatosak.

Az első fejezet a CENELEC történetét, a tagságot és a struktúrát ismerteti. Ebben a fejezetben kapunk tájékoztatást arról, hogy mi a kapcsolat a különböző európai és világszabványosító szervezetek között. Az ETSI és a CEN már korábban említett intézmények mellett, találkozunk a három világméretű testülettel az IEC-vel (International Electrotechnical Commission), az ISO-val (International Organization for Standardization) és az ITU-val (International Telecommunication Unio), mely minden távközlési szakember számára rendszeres napi olvasmányt szolgáltat.

A második fejezet az európai szabványokról szól, melyek jele EN. Ha bárhol EN és egy szám olvasható, akkor az megadja, hogy melyik európai szabvány tartalmazza a kérdéskörre vonatkozó előírásokat. 1995-ben 2144 CENELEC szabvány volt érvényben megkötve a terület legfontosabb eszközeinek és eljárásainak jellemzőit. Ez a szám 2001-re 4004-re növekedett. Az Európa Unió tagországainak ezeket a szabványokat kell átvennie és honosítania.

A harmadik fejezet igyekszik egy sokunk előtt nem eléggé világos kérdést tisztázni. Egy időben mindenütt azt tanultuk, hogy az Európai Unióban a szabványok nem kötelezőek, csak támpontot nyújtanak a vállalatok közötti szerződések során a műszaki jellemzőket tartalmazó mellékletek kidolgozásához. Kötelezővé csak akkor válik, ha valamelyik ország minisztériuma ezt közzéteszi.

Ugyanakkor megismerhetjük a HD (harmonizált dokumentum) jellegű kiadványt is, mely különböző nemzeti szabványok összehangolását igyekszik lehetővé tenni. Időközben azonban számos egyezmény született, melyek érdekeltté teszik a résztvevőket, hogy termékeik és szolgáltatásaik megfeleljenek a szabványnak. A különböző megkötésekkel elérték, hogy ha nem is kötelező a szabvány, még szigorúbban érdemes eszerint eljárni, mert a piac csak akkor fogadja be.

A könyvben érdekes statisztikát olvashatunk arról is, hogy 2001-ben a CENELEC és az IEC előírások 66,5%-a azonos volt, 8% nem volt teljesen azonos, de tartalmilag megegyezett, vagyis indokolttá vált az európai és a világszabványok összehangolása. Sok esetben az EN és az IEC szám megegyezik, hangsúlyozva ezek tartalmi összehangolását.

A következő fejezetek bemutatják, hogy a szabványok milyen módon támasztják alá az EU törvénykezését és szabályozási eljárásait. Külön említést érdemel az európai direktívák áttekintése, melyeket az irányító hatóságok adnak ki a szabványokra támaszkodva.

Az utolsó fejezetben a CE jelölés fontosságát tárgyalja a könyv, amely jelölés garanciát jelent arra, hogy az ezzel ellátott termék megfelel az európai szabványoknak. Ha valamelyik gyártó ezzel a jellel ellátja a kibocsátott árut, akkor azt nem feltétlenül szükséges újra vizsgálni, mert aki a jelet rátette garantálja a minőséget.

A könyvvel kapcsolatos esetleges további információkat Szabó Zoltán főosztályvezetőtől (MSZT) lehet megszerezni.

Megfigyelhető black-box csatorna forrásrejtő tulajdonsága

TÓTH GERGELY, HORNÁK ZOLTÁN

Budapesti Műszaki és Gazdaságtudományi Egyetem
{tgm, hornak}@mit.bme.hu

Az anonim átviteli protokollok elemzéséhez bevezethető megfigyelhető, black-box csatorna modellje alapján a cikkben meghatározásra kerül, hogy egy passzív megfigyelő milyen bizonyossággal képes kézbesített üzeneteket küldőjükhöz visszakövetni, azaz az anonimitást kompromittálni. Ezek alapján definiálni fogjuk a forrásrejtő tulajdonságot, melyet az elérhető anonimitás objektív mértékének lehet tekinteni. Végül kimondjuk mind a protokollt megvalósító csatorna, mind pedig az üzeneteket küldő entitásokra vonatkozóan azokat a követelményeket, melyek betartása esetén a megfigyelő bizonyossága meghatározható szint alá csökkenthető, azaz garantált minőségű anonimitás biztosítható.

Bevezetés

Az anonim átviteli protokollok (mint például a MIX-net [1] vagy az Onion Routing [2] [3]) gyökeresen meg fogják változtatni az anonim üzenetküldés gyakorlatát. Céljuk, hogy az alsóbb szintű hálózati rétegtől függetlenül biztosítsák, egy kézbesített üzenetet ne lehessen a küldőjével kapcsolatba hozni. Ezen protokollok kutatása, tervezése folyamatban van, azonban elméleti elemzésük és leírásuk még nem teljes.

A következőkben ismertetett forgatókönyv alkalmazási területének egy anonim orvosi tanácsadó rendszert választottunk. A betegek kérdéseiket a megfelelő orvosnak e-mail formájában teszik fel. Az anonim átviteli protokoll feladata a kérdés eljuttatása az orvoshoz úgy, hogy kézbesítéskor ne lehessen kideríteni, ki kinek, milyen témában tette fel a kérdését. Az orvosok a kérdésekre nyilvános fórumon, például egy honlapon válaszolnak. Amennyiben az anonimitást kompromittálni lehetne, a kérdések tartalmából egy kérdező betegségeire is következtetni lehetne, amit el szeretnénk kerülni, különösen ha érzékenyebb témakörök (pl. szexualitás, kábítószer) is felmerülhetnek. Természetesen az anonim átviteli protokollok nem csak erre a példára használhatók, alkalmazhatók anonim elektronikus szavazásra, vásárlásra vagy csak egyszerű elektronikus levelezésre is. A fenti példa, ahol a kérdések és az orvosi válaszok is nyilvánossá válnak és csak a kérdezők kiléte titkos, nagyon jól reprezentálja a vizsgált anonimitási követelményeket.

Ebben a cikkben ilyen protokollok leírására bevezetésre kerül a megfigyelhető black-box csatorna modellje. A bemutatott vizsgálat tárgyát az képezi, hogy egy csupán lehallgatásra képes megfigyelő milyen következtetéseket vonhat le pusztán az események bekövetkeztének időpontjait ismerve. A modellben definiálható a forrásrejtő tulajdonság, mely az anonimitás fogalmának egy elméletileg megalapozott mértéke. Végül ismertetésre kerül az a feltételrendszer, amelynek teljesülése esetén a megfigyelő bizonyosságát a lehető legkisebbre lehet csökkenteni és így a lehető legmagasabb fokú anonimitást lehet elérni.

A megfigyelhető black-box csatorna

Vizsgálatainkhoz azért ezt a modellt választottuk, mert ebben lehet az egész átviteli rendszert egyszerűen, mégis a számunkra érdekes tulajdonságok szem előtt tartása mellett elemezni:

- A csatorna black-box, mert az egészét vizsgáljuk, a belső implementációs sajátságokat figyelmen kívül hagyjuk. A megfigyelő nem láthatja, mi történik az üzenetekkel a csatorna belsejében, hogy kerülnek ezek továbbküldésre illetve átkódolásra.
- A csatorna teljesen megfigyelhető, azaz egy lehetséges megfigyelő érzékelheti a csatornába bemenő és az azt elhagyó üzeneteket [4]. Erre azért van szükség, mert egyrészt a kriptográfiával szemben az események időzítésének fontosságára szeretnénk felhívni a figyelmet, másrészt az elvi megfontolások alapján kimondott felső korlátok a gyakorlatban előforduló részleges megfigyelhetőség mellett is érvényesek maradnak.
- Továbbá a csatornán áthaladó üzenetekről feltesszük, hogy azonos méretűek és megfelelően titkosítottak, így a megfigyelő csak az események bekövetkeztének időpontjából képes következtetéseket levonni.

A környezet leírása

Jelölje S a küldők halmazát, R a fogadókét, míg M az üzenetek halmazát. Jelölje továbbá $S(m_i)$ az m_i üzenet küldőjét, $R(m_i)$ az m_i üzenet fogadóját, $t_S(m_i)$ az m_i üzenet elküldésének, $t_R(m_i)$ pedig a fogadásának időpontját. A rendszer folytonos időben működik, ugyanazon időpillanatban nem történhet két különböző esemény. Az üzenet továbbításának idejét a küldő és a csatorna, valamint a csatorna és a fogadó között nem vesszük figyelembe.

Ezt az egyszerűsítés kedvéért vezettük be, a végkövetkeztetést érdemben nem befolyásolja. Az orvosi kérdez-felelek példánk értelmében S a betegeket jelöli, R az orvosokat, míg M a feltett kérdések halmazát.

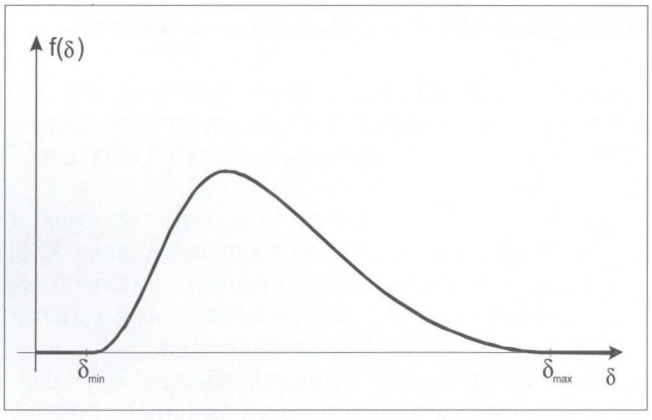
* *Köszönet illeti dr. Vajda Ferencet és dr. Selényi Endrét, akik a cikk megírásához értékes tanácsokkal és ötletekkel járultak hozzá, valamint dr. Dobrowiecki Tadeuszt, a cikk kivonatához adott ötleteiért.*
Külön köszönet Endrődi Csillának és Orvos Péternek a közös ötletelésekért.

A csatorna meghatározása

A csatorna az üzenetek továbbítására szolgál, a csatornán belül nem születik új üzenet, valamint a csatorna nem dob el beérkezett üzenetet. Egy beérkezett üzenet a következő szabályok szerinti késleletetés után kerül kézbesítésre:

- a késleltetés δ valószínűségi változó, adott $f(\delta)$ sűrűségfüggvénnyel, $\delta = t_R - t_S$, ahol δ üzenet- és időinvariáns;
- a csatorna minden üzenetet egy előre meghatározott konstans, üzenet- és időinvariáns δ_{max} (time-to-live) késleltetésen belül, de legalább egy konstans, üzenet- és időinvariáns δ_{min} (minimális késleltetés) elteltével kézbesít, azaz

$$\forall_{m_i}\left[\delta_{\min} < t_R(m_i) - t_S(m_i) < \delta_{\max}\right]$$

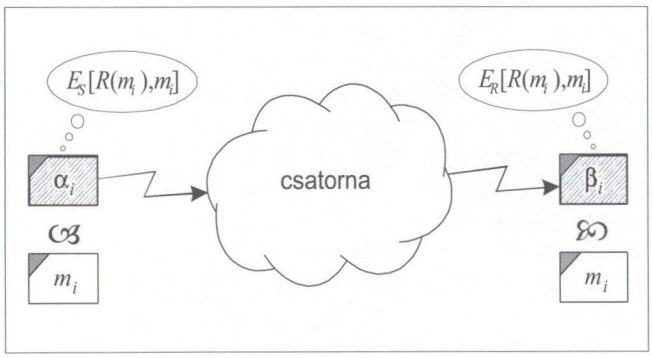


1. ábra A csatorna késleltetésének $f(\delta)$ sűrűségfüggvénye

A C csatornát így az $f(\delta)$, δ_{min}, δ_{max} paraméterekkel jellemezhetjük. A példa szerint a csatorna feladata a betegek által feltett kérdések eljuttatása az orvosokhoz úgy, hogy a kézbesítéskor már ne lehessen kideríteni, a kérdést ki tette fel, illetve hogy egy feltett kérdés melyik szakterületű orvosnak szól.

Üzenetküldés

A következőkben feltesszük, hogy $s_a \in S$, $s_a = S(m_i)$ küldő $m_i \in M$ üzenetet küld $r_b \in R$, $r_b = R(m_i)$ fogadónak. Az m_i üzenet a csatornába a titkosított $\alpha_i := E_S(r_b, m_i)$ formában $t_S(m_i) = t_S(\alpha_i)$ időpontban érkezik meg, míg a fogadóhoz egy más kulccsal titkosított $\beta_i := E_R(r_b, m_i)$ formában $t_R(m_i) = t_R(\beta_i)$ időpontban fog megérkezni.



2. ábra Üzenetküldés a csatornán keresztül

Azt is feltesszük, hogy E_S és E_R tökéletes titkosítás, így α_i-t csak a csatorna, míg β_i-t csak r_b tudja dekódolni, azaz $I[E_S(r_b, m_i), (r_b, m_i)] = 0$ és $I[E_R(r_b, m_i), (r_b, m_i)] = 0$ (ahol I a kölcsönös információtartalmat jelöli). További elemzést érdemel annak eldöntése, hogyan változnak az ebben a cikkben levont következtetések, ha az elméletileg tökéletes titkosítót egy gyakorlati értelemben vett erős titkosítóra cseréljük. Feltehetően ez nem jelent majd érdemi változást megfelelően erős gyakorlati rejtjelezés esetén; a modellben megfogalmazott ideális rejtjelezés azonban jelentősen egyszerűsíti a matematikai elemzést.

Példánkban a titkosításra azért van szükség, mert amennyiben a kérdések nyílt szövegként kerülnének továbbításra, úgy egy megfigyelő a csatorna be- és kimeneteit lehallgatva pontosan kideríthetné, ki melyik kérdést tette fel.

A megfigyelő

Vizsgáljuk meg egy passzív megfigyelő lehetőségeit ebben a modellben, aki csak lehallgatni tudja a titkosított üzeneteket, azokat nem tudja dekódolni (csak ha neki küldték), valamint azokat sem módosítani, sem elnyelni, sem visszajátszani, sem késleltetni nem áll módjában. (Vegyük észre, hogy az anonimitás megsértése érdekében a támadó a klasszikus manipuláláson túl az üzenetkésleltetés módszerével is élhet.) A megfigyelő célja, hogy a kézbesített üzeneteket (β_i-k) a küldőkhöz rendelje – vagy legalább is az összetartozást minél nagyobb valószínűséggel megtippelje – és így megmondja, ki kivel kommunikál.

Aktív támadót feltételezve, aki ha üzenetet értelmesen módosítani nem is, de üzenetet késleltetni tud, a levont következtetések sajnos nem érvényesek. Ez a lehetőség további elemzést, kutatást érdemel, de túlmutat jelen cikk tartalmán.

A megfigyelő ismeretei

A megfigyelőről feltételezzük, hogy képes a csatorna minden kimenetét megfigyelni, azaz ismeri a csatornába érkezett titkosított üzeneteket, azok küldési időpontját, a csatornát elhagyó titkosított üzeneteket, azok kézbesítési időpontját, valamint a csatorna paramétereit és környezetét. Ennek megfelelően a megfigyelő a következőket ismeri:

- a csatorna környezetét (S, R) és paramétereit ($f(\delta)$, δ_{min}, δ_{max});
- $\varepsilon_S := \{\alpha_i := E_S[S(m_i), m_i]\}$ és $\vartheta_S := \{t_S(\alpha_i)\}$ – a csatornába érkezett üzeneteket, valamint érkezésük időpontját;
- $\varepsilon_R := \{\beta_i := E_R[R(m_i), m_i]\}$ és $\vartheta_R := \{t_R(\beta_i)\}$ – a csatornát elhagyó üzeneteket, valamint kézbesítésük időpontját.

Feltehető továbbá, hogy a megfigyelő lehet az egyik küldő, vagy az egyik fogadó is. Amennyiben a megfigyelő az egyik fogadó, úgy ismeri az összes neki küldött üzenet tartalmát és tipikusan ezekről szeretné kideríteni, hogy ki küldte őket. Azonban mivel E_S tökéletes titkosító függvény

és független E_R-től, így egy ilyen fogadó-megfigyelő sem jut olyan többlet információhoz, ami a következőkben levont következtetéseket befolyásolná.

Jelölje Ψ a rendszer történetét, amit a következő paraméterek határoznak meg: C, S, R, ε_S, ε_R, ϑ_S, ϑ_R. A továbbiakban levont következtetéseknél feltételezzük, hogy a megfigyelő a rendszer teljes Ψ történetét ismeri, azaz minden lehetséges számára elérhető információt a rendszer működésének teljes időszakában képes megfigyelni. Mint látni fogjuk, még ilyen esetben is jelentősen lecsökkenthető annak esélye, hogy egy üzenet feladóját vissza lehessen követni.

Példánk szerint a megfigyelő célja annak kiderítése, melyik kérdést ki tette fel. Ehhez feltesszük, hogy legrosszabb esetben minden kommunikációs csatornát le tud hallgatni. A megfigyelő szándéka az egyszerű zsarolástól a globális adatgyűjtésig bármilyen ok lehet.

A megfigyelő bizonyossága

Legyen a rendszer egy konkrét története

$$\psi^* = (C^*, S^*, R^*, \varepsilon_S^*, \varepsilon_R^*, \vartheta_S^*, \vartheta_R^*) .$$

Annak érdekében, hogy el lehessen dönteni, melyik üzenetet ki küldte, minden β_k^* titkosított kézbesített üzenethez és minden lehetséges s_l^* küldőhöz meghatározható az a valószínűség, amely megadja, mekkora eséllyel lehetett s_l^* a β_k^* üzenet küldője. A megfigyelő ismeretei alapján így β_k^* üzenetet az s_l^* küldő ezzel a meghatározható $P_{\beta_k^*, s_l^*, \psi^*}$ valószínűséggel küldte.

Jelölje $\mu_{\beta_k^*, \psi^*}$ azon α_j^* titkosított elküldött üzenetek halmazát, melyek az $f^*(\delta)$ sűrűségfüggvény tulajdonságainak figyelembevételével egyáltalán β_k^*-ként elhagyhatták a csatornát (1). Jelölje továbbá $\eta_{\beta_k^*, s_j^*, \psi^*}$ azon $\mu_{\beta_k^*, \psi^*}$ beli α_j^*-ket, melyeket s_l^* küldött (2). Azaz:

$$\mu_{\beta_k^*, \psi^*} = \left\{ \alpha_j^* \middle| t_R(\beta_k^*) - \delta_{max}^* \right] \le t_s(\alpha_j^*) \le \left[t_R(\beta_k^*) - \delta_{max}^* \right] \right\} \quad (1)$$

$$\eta_{\beta_k^*, s_j^*, \psi^*} = \left\{ \alpha_j^* \middle| \left[\alpha_j^* \in \mu_{\beta_k^*, \psi^*} \right] \wedge \left[S(\alpha_j^*) = s_l^* \right] \right\} \quad (2)$$

Amennyiben a megfigyelő a kézbesített üzenet → küldő összerendelést minden β_k^* kézbesített üzenetre függetlenül – pusztán a csatorna késleltetési karakterisztikája alapján – végzi, úgy a következő képlet adja $P_{\beta_k^*, s_l^*, \psi^*}$-t:

$$P_{\beta_k^*, s_l^*, \psi^*} = P\left[S(\beta_k^*) = s_l^* \middle| \Psi = \Psi^* \right] = \frac{\sum f^* \left[t_R(\beta_k^*) - t_s(\alpha_j^*) \right]}{\sum f^* \left[t_R(\beta_k^*) - t_s(\alpha_j^*) \right]} \quad (3)$$

$$\forall_{\alpha_j^* \left[\alpha_i^* \in \eta_{\beta_k^*, s_l^*, \psi^*} \right]} \qquad \forall_{\alpha_j^* \left[\alpha_i^* \in \mu_{\beta_k^*, \psi^*} \right]}$$

A megfigyelő természetesen a legvalószínűbb küldőt keresi, ahol $P_{\beta_k^*, \psi^*} := \max_{s_l^*} P_{\beta_k^*, s_l^*, \psi^*}$.

Ezek alapján a megfigyelő minden kérdéshez a (3)-as képlet alapján kiszámolja annak valószínűségét, hogy egy adott kérdést egy adott beteg tett fel.

Majd ezen valószínűségek alapján megtippeli, ki lehetett a kérdést feltevő tényleges beteg.

Forrásrejtő tulajdonság

A rendszer $\Psi = (C, S, R, \varepsilon_S, \varepsilon_R, \vartheta_S, \vartheta_R)$ története forrásrejtő tulajdonságú Θ paraméterrel, amennyiben semelyik β_k titkosított kézbesített üzenethez sem tud a megfigyelő Θ-nál nagyobb valószínűséggel küldőt hozzárendelni:

$$\forall_{\beta_k \in \varepsilon_R} P_{\beta_k, \Psi} \le \Theta \quad (4)$$

A MIN/MAX-tulajdonság

Annak érdekében, hogy a forrásrejtő tulajdonságot alapvetően befolyásoló (3)-as képlet konkrét értékeit garantáltan a legrosszabb esetben is egy határ alá lehessen szorítani, az üzenetküldések között eltelt időre megkötéseket kell tenni:

- A tört számlálójában levő összegzést minél kisebb halmazon kell elvégezni. Ennek érdekében a küldők nem küldhetnek bizonyos időintervallumon belül egynél több üzenetet.
- A tört nevezőjében levő összegzést minél nagyobb halmazon kell elvégezni. Ennek érdekében a küldőknek bizonyos időintervallumon belül legalább egy üzenetet kell küldeniük. (Ha ez máshogy nem érhető el, akkor a küldőnek véletlenszerűen választott fogadóknak üres üzenetet kell küldeniük.)

A fenti megkötéseket figyelembe véve a rendszer $\Psi = (C, S, R, \varepsilon_S, \varepsilon_R, \vartheta_S, \vartheta_R)$ története MIN/MAX-tulajdonságú τ_{min}, τ_{max} paraméterekkel ($\tau_{min} \le \tau_{max}$), ha teljesül, hogy semelyik küldő sem küld τ_{min} időn belül két üzenetet (5) és minden küldő küld τ_{max} időnként (vagy azon belül) legalább egy üzenetet (6):

$$\forall_{s_l \in S} \quad \forall_{\alpha_j | S(\alpha_j) = s_l} \xi_{s_l, \alpha_j} = \varnothing \quad (5)$$

$$\forall_{s_l \in S} \quad \forall_{\alpha_j | S(\alpha_j) = s_l} \neg\left(\zeta_{s_l, \alpha_j} = \varnothing \right) \quad (6)$$

Ahol ξ_{s_l, α_j} azon elküldött titkosított üzenetek halmaza, melyeket az s_l küldő α_j elküldése után legfeljebb τ_{min} idő elteltével küldött (7), valamint ζ_{s_l, α_j} azon elküldött titkosított üzenetek halmaza, melyeket az s_l küldő α_j elküldése után legfeljebb τ_{max} idő elteltével küldött (8):

$$\xi_{s_l, \alpha_j} := \left\{ \alpha_i \middle| \left(S(\alpha_i) = s_l \right) \wedge \left(t_s(\alpha_i) > t_s(\alpha_j) \right) \wedge \left(\left[t_s(\alpha_i) - t_s(\alpha_j) \right] \le \tau_{min} \right) \right\} \quad (7)$$

$$\zeta_{s_l, \alpha_j} := \left\{ \alpha_i \middle| \left(S(\alpha_i) = s_l \right) \wedge \left(t_s(\alpha_i) > t_s(\alpha_j) \right) \wedge \left(\left[t_s(\alpha_i) - t_s(\alpha_j) \right] \le \tau_{max} \right) \right\} \quad (8)$$

Ezen feltételek teljesülése esetén a megfigyelő által tetszőleges kézbesített üzenethez és küldőhöz hozzárendelhető valószínűségre a következő üzenetinvariáns $\hat{P}_\psi$ felső becslés adható (9), amennyiben $\tau_{max} \le (\delta_{max} - \delta_{min})$:

$$P_{\beta_k, \Psi} \le \hat{P}_\psi = \frac{\sum_{i=1(i-1)\cdot\tau_{min} \le q < i\cdot\tau_{min}}^{\Delta_{min}} \max f(q)}{|S| \cdot \sum_{i=1(i-1)\cdot\tau_{max} \le q < i\cdot\tau_{max}}^{\Delta_{max}} \min f(q)} \quad (9)$$

Ahol $\Delta_{max} = \left\lceil \frac{\delta_{max} - \delta_{min}}{\tau_{max}} \right\rceil$ és $\Delta_{min} = \left\lceil \frac{\delta_{max} - \delta_{min}}{\tau_{min}} \right\rceil$.

A MIN/MAX tulajdonság lényege példánkra vetítve, hogy a betegeknek egy adott gyakorisággal kérdéseket kell feltenniük, annak érdekében, hogy egy adott szintű anonimitás általános esetben is biztosítható legyen.

Szélsőértékek

A következőkben az $f(\delta)$ sűrűségfüggvény két szélsőséges esetét vizsgáljuk.

Legrosszabb eset: determinisztikus, fix idejű késleltetés

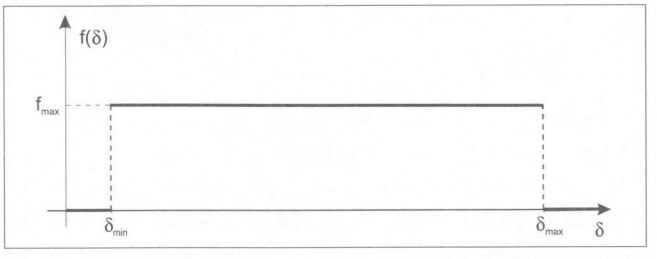
Amennyiben egy rendszer $\Psi = (C, S, R, \varepsilon_S, \varepsilon_R, \vartheta_S, \vartheta_R)$ történetének $f(\delta)$ sűrűségfüggvénye egy eltolt Dirac-delta függvény (azaz a csatorna minden üzenetet egy konstans kézbesítési idő elteltével kézbesít), úgy a megfigyelő minden kézbesített titkosított üzenethez egyértelműen hozzá tudja rendelni küldőjét.

Amennyiben az üzenetküldések rendszerességére nincsen megkötés, vagy ha egy rendszer Ψ MIN/MAX-tulajdonságú történetének τ_{min}, τ_{max} paramétereit nem az $f(\delta)$ sűrűségfüggvénynek megfelelően választották, úgy szintén előfordulhat bizonyos – nem feltétlenül az összes – β_k kézbesített üzenetekre, hogy $P_{\beta_k,\Psi} = 1$, amelyet természetesen szeretnénk elkerülni.

A legrosszabb esetben példánkban a megfigyelő minden kérdéshez hozzá tudja párosítani azt a beteget, aki ténylegesen azt fel is tette, így elérte célját.

Legjobb eset: egyenletes eloszlású késleltetés

Ez esetben a megfigyelő tetszőleges kézbesített titkosított üzenethez csak véletlenszerűen tud küldőt hozzárendelni azok közül, akik a releváns $(\delta_{min} - \delta_{max})$ időintervallumban üzenetet küldtek.



3. ábra A legjobbnak bizonyult (egyenletes eloszlású) sűrűségfüggvény

Amennyiben egy rendszer $\Psi = (C, S, R, \varepsilon_S, \varepsilon_R, \vartheta_S, \vartheta_R)$ történetének $f(\delta)$ sűrűség-függvénye egyenletes eloszlású (azaz δ_{min} és δ_{max} között konstans f_{max} értéket vesz fel), úgy minden β_k kézbesített titkosított üzenetre a következő érvényes:

$$P_{\beta_k,\Psi} = \frac{\max_{s_l} \left| \eta_{\beta_k, s_l, \Psi} \right|}{\left| \mu_{\beta_k,\Psi} \right|} \tag{10}$$

Amennyiben Ψ MIN/MAX tulajdonságú τ_{min}, τ_{max} paraméterekkel – ahol $\tau_{max} \le (\delta_{max} - \delta_{min})$ – úgy a felső becslés (9)-es képlete tovább egyszerűsödik:

$$P_{\beta_k,\Psi} \le \hat{P}_\Psi = \frac{\Delta_{\min}}{|S| \cdot \Delta_{\max}} \approx \frac{\tau_{\max}}{|S| \cdot \tau_{\min}} \tag{11}$$

Amennyiben Ψ^* még a $\tau_{min} = \tau_{max}$ feltételt is teljesíti (ahol továbbra is $\tau_{max} \le [\delta_{max} - \delta_{min}]$), azaz minden s_l küldő pontosan $\tau_{min} = \tau_{max}$ időnként pontosan egy üzenetet küld, akkor a rendszer története eléri a globális optimumot, azaz a megfigyelő tetszőleges kézbesített üzenet küldőjeként a küldők halmazának egy véletlenszerűen választott elemét kénytelen megjelölni, így:

$$P_{\beta_k,\Psi} \le \hat{P}_\Psi \approx \frac{1}{|S|} \tag{12}$$

A legjobb eseteben példánkra vonatkoztatva a megfigyelő semmit sem ért el a megfigyeléssel. Az üzenettovábbító csatorna paraméterit ismerve (azok akár nyilvánosak is lehetnek) azon betegek közül, akik a releváns időintervallumban egyáltalán kérdést tettek fel, a megfigyelő véletleszerűen kénytelen választani a tippeléshez. Amenynyiben a betegek a MIN/MAX-tulajdonságnak is megfelelnek, akkor még az anonimitás mértéke is pontosan szabályozható.

Összefoglaló

A cikkben ismertetésre került a megfigyelhető black-box csatorna modellje. Passzív megfigyelőt feltételezve megvizsgáltuk, milyen következtetéseket tud a megfigyelő az események bekövetkeztének időzítése és a csatorna tulajdonságai alapján levonni. A modellben definiáltuk a forrásrejtő tulajdonságot, mely az anonimitás fogalmának egy elméletileg megalapozott mértéke. Végül bemutattunk egy olyan módszert is, melynek alkalmazásával korlátozhatóak a megfigyelő lehetőségei, sőt a globális optimum is elérhető.

További elemzést igényel az, hogy ha a feltételezett, elméleti értelemben vett tökéletes titkosítót gyakorlati értelemben vett erős titkosítóra cseréljük. Szintén megvizsgálandó, hogyan változnak a következtetések, ha a jelenlegi black-box csatornát „felnyitjuk" és feltételezzük, hogy a megfigyelő a csatornán belülről is hozzájuthat bizonyos információkhoz. Végül azzal is számolni kell, ha az eddig passzívnak feltételezett megfigyelőt aktív támadóval helyettesítjük, aki az üzeneteket késleltetni és esetleg módosítani is tudja, hogyan módosul az anonimitás biztosítható szintje.

Irodalomjegyzék

[1] D. Chaum: „Untraceable Electronil Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, vol. 24, number 2, 1981

[2] M. Reed, P. Syverson, D. Goldschlag: „Anonymous Connections and Onion Routing", in IEEE Journal on Selected Areas in Communication Special Issue on Copyright and Privacy Protection, 1998.

[3] D. Goldschlag, M. Reed, P. Syverson: „Hiding Routing Information", in Information Hiding, R. Anderson (szerkesztő), Springer-Verlag LLNCS 1174, pp. 137–150, 1996

[4] A. Pfitzman, M. Kohntopp: „Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology", in Designing Privacy Enhancing Technologies, H. Federrath (szerkesztő), Springer-Verlag LNCS 2009, pp. 1–9, 2001

Támadási lehetőségek távközlési hálózatok ellen

DR. SÁRKÁNY TAMÁS fizikus

sarkany.tamas@mail.datanet.hu

Globalizálódó világunkban a terroristatámadások nemcsak földi célpontok ellen irányulhatnak, hanem az életünket alapvetően meghatározó távközlési eszközök rombolására is. Cikkünkben áttekintjük a távközlési műholdak és a számítógépes hálózatok ellen irányuló támadások lehetőségeit és a védekezési módszereket.

Támadások műholdak ellen

Világszerte egyre szaporodik – a már most most is több százas nagyságrendű – alacsony (2000 km alatti) röppályán keringő („LEO") műholdak alkalmazása. A műholdak feladatai távközlési, navigációs, időjárás előjelzési és biztonsági szolgáltatásokra terjednek ki. Ezek a műholdak évről évre nagyobb jelentőségűek, sok esetben biztosítanak Internet hozzáférést, távbeszélő vagy fax összeköttetéseket, és az űrkutatásban is szerepet játszanak.

A műholdak sérülékenységét a terrorista országok jól ismerik, és ezért hajlamosak lehetnek a műholdak funkcióinak megzavarására. Minthogy egyre több szervezet és vállalkozás hasznosítja a LEO műholdakat, az ellenük irányuló merényletnek súlyos kihatása lehet a gazdasági környezetre és mindennapi életünkre, továbbá nemzetbiztonsági szempontból is károkat okozhat. A terroristák támadását segíti, hogy e műholdak infrastruktúrája rendkívül törékeny. Feltételezhető, hogy terrorista államok már megfontolták ezt a lehetőséget nukleáris projektjük kialakításakor.

A nagy magasságban végrehajtott robbantás főként azért vonzó terv terrorista államok számára, mert semmilyen más fegyver, mint például konvencionális rakéták, nem okozhatnának ilyen nagy és hosszan tartó pusztítást. Ilyen robbantás csupán egyetlen viszonylag kiserejű atombombát igényel, ami a nemzetközi feketepiacon viszonylag könnyen vásárolható és a vásárlás színhelyéről kicsempészhető tetszőleges, rosszindulatú országba. Azon kívül a romboló elektron-sugárzás gyorsan szétterjed a LEO övezetben, tehát nincs szükség a műholdak célzott megtámadására. Tönkretehetik e műholdak kritikus elektronikus alkatrészeit, ezáltal üzemképtelenségüket okozva. Egyetlen 50 kilotonnás robbantás a LEO műholdak élettartamát évekről egy-két hónapra csökkentené!

Megjegyzendő, hogy a műholdakat védelemmel látják el a Van Allen öv káros sugárzásával szemben, minthogy ez a sugárzás a műholdak kritikus elektronikus áramköreit károsíthatja. A geostacionárius és fél geostacionárius pályán álló műholdak különösen ki vannak téve ennek a természetes sugárzásnak. A sugárzás elleni védelem céljából az egész műholdat árnyékolják, továbbá sugárzást tűrő elektronikai alkatrészeket alkalmaznak. A LEO pályákon keringő műholdak (2000 km alatt) aránylag védett övben haladnak, így enyhébb sugárzás-védelmet igényelnek. Ezért LEO műholdakban sokszor kereskedelmi forgalomban lévő normál elektronikai alkatrészeket alkalmaztak, minthogy ezek nagyobb választékban és jobb paraméterekkel álltak rendelkezésre, mint a sugárzást inkább tűrő alkatrészek. Ebben rejlik a LEO műholdak Achilles-sarka a nukleáris fenyegetéssel szemben: a normál körülmények között jóindulatú környezetben a romboló sugárzás szintje ezerszeresére nőhet egy nukleáris robbantás után.

Műholdak gyártásakor sokféle módszerrel lehet csökkenteni az ilyen nukleáris támadás kockázatát. Például jelentős többletköltséggel védhetik a műholdakat azáltal is, hogy járulékos fémbevonattal veszik körül a műhold érzékeny elektronikus áramköreit, de a műhold gyártási költségét kb. 20 ezer dollár/kg-mal megemeli. Másfelől a sugárzásra érzékeny elektronikai alkatrészeket a gyártás folyamán sugárzást jobban tűrő alkatrészekkel helyettesítik. E módszereket újabban egyre inkább alkalmazzák.

Támadások számítógép hálózatok ellen

A cyber támadások célja számítógépek tárolt adatainak meghamisítása, megsemmisítése vagy módosítása. Ilyen támadás információ szerzésére vagy a szóban forgó rendszer időleges üzemképtelenné tételére irányul. Fizikai támadások előtt gyakran ily módon növelik a rákövetkező támadás romboló hatását. A „hacker" és „cracker" behatolásokról már sok közlemény jelent meg, a következőkben ezért csak rövid áttekintésre szorítkozunk.

A távközlési hálózatok azért vannak kitéve terroristák fenyegetésének, mert úgyszólván minden nagyobb vállalat és kormányzati szerv tevékenysége döntően ezektől függ. Egy fizikai terrorista támadás előtt a távközlési hálózat üzemzavara, különösen az Internet hálózathoz való hozzáférés megszűnése, döntően növeli a támadás utáni zavarokat. Ez különösen érvényes katonai vagy repülőirányítási berendezésekre, kémiai üzemekre és nukleáris erőművekre. Különösen nagy a kockázat, ha egy Internet szolgáltató műholdas útvonalon közvetíti az adatokat, minthogy ez nagyobb lehetőséget ad idegen számítógépekbe való „betörésre".

A sérülékeny hálózatok elleni elektronikus támadások száma az utóbbi öt év alatt erősen megnőtt. Terroristák részére a növekvő kiterjedésű hálózatok jól kiaknázható sérülékenységet eredményeznek – lényegében egy hátsó kaput a vállalat IT-rendszerébe való behatoláshoz.

A vállatok közötti fokozott együttműködés következtében a távközlési hálózatok ellen irányuló támadások az infrastruktúra szétrombolásával egyre nagyobb károkat okoznak, és az Internet hálózat egyre szélesebb körű igénybevétele csak fokozza a terrorista behatolások kockázatát. Az Egyesült Államokban 2002-ben 110 000 cyber behatolás történt. Igen sok számítógépes támadásról érkeztek jelentések Nagy-Britanniából és Ausztráliából is. A cyber bűnözés tehát globális realitás, gyakran jelennek meg erről szóló beszámolók, de sajnálatosan kevés vállalat van ennek tudatában. Felmérések szerint európai távközlési vállalatok 95 százaléka nem tekinti a cyber terrorizmust veszélyes fenyegetésnek.

A hacker és cracker szervezetek elleni védekezéssel egy idő óta világszerte számos kormányzati szerv intenzíven foglalkozik. A védekezésre vonatkozó útmutatások azonban országos szervezetekre vonatkoznak, és egy-egy vállalat számára nem adnak elég információt a védekezéshez. A sok vállalatra azonosan érvényes irányelveket nehéz figyelembe venni, minthogy a távközlési vállalatok kereskedelmi szervezetek, amelyek érthetően vonakodnak a konkurenciával való együttműködéstől, és úgy érzi mindegyik, hogy számára nem jelent kockázatot a cyber terrorizmus. Léteznek már behatolást detektáló szoftverek is, amelyeket Amerikában már alkalmaznak néhány nagyobb távközlési hálózatban, de ezek Európában alig lelhetők fel. Az egyes hálózatok kockázati tényezői eltérőek, ezért a szükséges védelmi intézkedések is különböznek. Mértékük függ a hálózat sebezhetőségétől, a várható külső behatásoktól és a hálózat zavara esetén fellépő következményektől. Sokféle védelmi szoftver található a piacon, léteznek megoldások behatolást detektáló szoftverekre és tűzfal az adatvédelem biztosítására.

A távközlési hálózatok biztonságát csak valamennyi érdekelt fél aktív közreműködésével lehetne szavatolni. Ehhez minden kormányzatnak kezdeményeznie kellene a biztonságosabb távközlési infrastruktúra megteremtését. Először is a hálózat üzemeltetőket kellene felvilágosítani a behatolási módszerekről és azokról a következményekről, amelyek egy hacker vagy cracker támadás nyomán keletkeznek. A távközlési hálózatok és a vállalatok vezetőit világszerte rá kellene döbbenteni a fenyegető veszélyre, és cselekvésre kellene bírni, akár törvényes eszközökkel is.

Irodalom

[1] James Careless, Holding back hackers, Via Satellite, July 2000, p.50

[2] Debi Ashenden, Protect and survive, Telecommunications International, January 2003, p.29

[3] G.Kweder, R.C. Webb, Lewis Cohn, United States' Growing Dependence on Commercial Satellites, Via Satellite, July 2000, p. S6

Hírek

Vezeték nélküli LAN hálózatba kötött irodákban a kommunikáció minőségének biztosításához csillapítani kell a szekunder reflexiókat, és csökkenteni kell a rádióhullámok kijutását a külső térbe. Régebben a vezeték nélküli LAN hálózatot nem szívesen alkalmazták irodákban a nem kielégítő átviteli sebesség és a lehallgathatóság miatt.

Az újabb IEEE LAN szabványok szerint az 5,2 GHz-es frekvenciasávban 52 Mbit/s, a 2,4 GHz-es frekvenciasávban 11 Mbit/s átviteli sebesség biztosítható, és a biztonság is növelhető kódolás és rúterek alkalmazásával. E sebességek biztosításához azonban irodaépületek tervezésekor az építészeknek figyelembe kell venni a rádióhullámok reflexiójának és az irodából való kiszivárgásának szempontjait, megfelelő abszorbeáló és árnyékoló burkolatok alkalmazásával.

Japánban kifejlesztettek egy speciálisan ilyen célra szolgáló, habosított üveggyapotból gyártott abszorbeáló anyagot. A vizsgálatok szerint az ilyen anyagból gyártott burkolat alkalmazásával a LAN hálózatban elérhető adatátviteli sebesség lényegesen növelhető a kommunikáció minőségének romlása nélkül.

(New Breeze, Winter 2003, p.19.)

Az Európai Bizottság támogatja a **„Wireless Cabin"** projektet, hogy az üzleti ügyben utazók beszéd és adat kommunikációt használhassanak repülőgépen.

Az Inmarsat műholdas szolgáltatók már ma is továbbítják a földi cellás telefonok hívását a bekábelezett fedélzeti készülékekhez. A szolgáltatók ezen rendszer továbbfejlesztését javasolják egy fedélzeti bázisállomás létesítésével, amely a repülőgépen a mobil telefonokat teljesítményre állítja, kiküszöbölve a fedélzeti elektronika zavarását. Az utasok műholdas kommunikációval érik el a földi állomást a fedélzeti bázisállomáson át. Ennek funkciója hasonló, mint egy vállalaton belüli bázisállomás, amellyel különválaszthatók a vállalaton belüli hívások és a kimenő hívások (Híradástechnika, 2001/11, p.35).

A bázisállomás szoftverje arról is gondoskodik majd, hogy a repülőgépről kezdeményezett hívások az előfizető havi mobil számláján jelenjenek meg. Ne számítsunk azonban az új rendszer gyors bevezetésére. Várhatóan legalább 18 hónapot igényel, hogy a légügyi hatóságok globálisan jóváhagyják a fedélzeti bázisállomások rendszerét.

(Via Inmarsat, January-March 2003, p.42)

Hannoveri CeBIT: Talpra áll az ICT szektor

SIPOS LÁSZLÓ

siposlaj@axelero.hu

A Hírközlési és Informatikai Tudományos Egyesület szervezésében március közepén népes magyar küldöttség látogatott Hannoverbe. Az érdeklődő szakemberek egy egynapos „kiránduláson" igyekeztek megismerni a ma még csak csodaszámba tartozó „kütyüket", a közeljövő szolgáltatási lehetőségeit, a világ legnagyobb számítástechnika, távközlés, szoftver és szolgáltatások palettáját felvonultató szakkiállításán.

A múlt század ötvenes éveiben indított Hannover Fair nemzetközi vásárból 1986-ban kinőtt, a tavasz hírnökeként számon tartott CeBIT, melyen minden évben először láthatók, és immár kézzel is megfoghatók az újdonságok. A Mérnök Újság szerkesztőbizottságának bizalmát élvezve az idén akkreditált szakíróként jómagam is érzékelhettem, hogy a nyolcvanas évek végén indult technológiai „forradalom" még folytatódik. A csupán nyolcórás mini látogatás megtervezésekor igyekeztem előre felkészülni, hogy beszámolómmal objektív képet tudjak nyújtani az olvasóinknak.

Az idei CeBIT jellemzői

A CeBIT-re március 12 és 19. között a hatvan országból érkezett több mint hétezer kiállító termékeire, százhúsz országból közel hatszázezer látogató volt kíváncsi. A több mint két éve tartó recesszió nem volt jó előjel a kiállítók és a szervezők részére. Már az elmúlt évi CeBIT-en is csökkent a kiállítók és látogatók száma, ami idén még tovább romlott, de ennek ellenére nem kell vészharangokat kongatni.

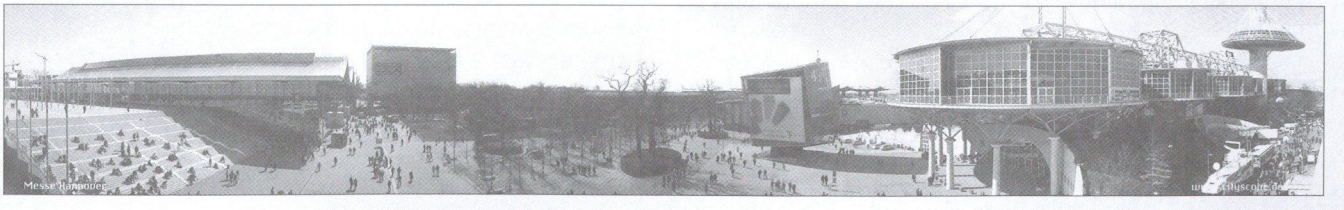
A Gartner piackutató cég szakértői szerint, a nehéz gazdasági helyzetben csökkennek a személyi számítógépekre, a mobiltelefonokra és egyéb kommunikációs eszközökre fordított kiadások, ami a piachoz kötődő kiállításokra is rányomja a bélyegét. A Deutsche Telekom a CeBIT első napjaiban jelentette be, hogy az elmúlt évben több mint húszmilliárd eurós veszteséget volt kénytelen elkönyvelni. Térségünk legnagyobb fogyasztói elektronikai cége, a Philips Electronics pedig a napokban adta hírül, hogy több mint ezerhatszáz fős leépítésre kényszerül. 2002-ben több mint kétezer informatikai cég ment csődbe Németországban, és ez hatást gyakorolt a CeBIT-re is.

Az érem másik oldalán viszont egyre fejlődő tematikus CeBIT-ek kerülnek megrendezésre például Törökországban, Kínában, és idén először az USA-ban is.

A jövőbe vetett hit alapjai

A vásár előtt a nagy hi-tech cégek vezetői, a világ rangos döntéshozói a technológiai trendekről és stratégiáról tanácskoztak, igyekezve kijelölni a válságból kivezető utat. Tanácskozásukon legjobb megoldásként a költségérzékeny vásárlóközönség ellátását jelölték meg olcsó technikai eszközökkel, szoftverekkel: *„A technológiai fejlődés mindig lökésszerűen jelentkezik: Ilyennek voltunk tanúi nyolc éve, az Internet életre hívásakor. Most is hasonló viharos fejlemény előtt állunk."* A visszaesésért jórészt maguk a cégek okolhatók, mivel olyan termékekkel és szolgáltatásokkal akarják ellátni a piacot, melyekre az még nem készült fel. Az ICT iparág másfélmilliárd dollárra tehető évi értékesítése, még ma is stagnál. A hosszú távú előjelzések ehhez képest több mint 10 százalékos növekedési ütemet jósolnak, míg a rövidtávúak csak új és korszerű eszközök elterjedése esetén vélik elkerülhetőnek a visszaesést.

Számos, az elmúlt években született találmány és fejlesztési eredmény megváltoztathatja a munkamódszereinket, szokásainkat – az eddiginél alacsonyabb költségen. Bővülhet az Internetet elérő egységek mai százmillió PC-t meghaladó köre. A változások olyan nyílt számítástechnikai szabványokat is érintenek, mint az XML, a Soap, a Java és a Linux, melyeket a platformok közötti átjárhatóság érdekében a legnagyobb cégek, például az IBM és a Microsoft is felkaroltak. Ezek a nyílt forráskódú alkalmazások a jelenlegi költség- és időráfordításnak egytizedéért is integrálhatóak és lehetővé tehetik a költségek kordában



tartását. A világgazdaság általánosan gyenge állapota, tetézve az iraki háborúval terhet rótt a fejlett technológiát termelő ágazatokra, de ezzel együtt fellendülés várható. Növekedni fog a fejlett technológiák alkalmazása, az olcsó technológiák területén, mert az IT kiadások növekedése nem várható.

Újdonságok az idei CeBIT-en

Az emberi erőforrás támogatására most először külön teret szenteltek a szervezők, az emberi erőforrással (HR – Human Resources) kapcsolatos nyilvántartási feladatoktól az elektronikus képzésen keresztül a tudásmenedzsmentig. Itt a számítógépes támogatású személyzeti munka állt a középpontban. A cégek, a vállalati tanácsadók, a szoftverkereskedők egyedi megoldásokat mutattak be a mindennapi problémák optimalizálására, valamint a gazdasági fejlesztések terén.

A jövőpark meghökkentő élményei idén sem maradtak el. Itt a technológia-átadás és innovációs piac jelenlegi „boszorkánykonyhája" mutatkozott be. Először is egy kérdés: Milyen nyelven beszélhettem Hermine-vel, a High-Tech aus Bayern standján? Bizonyára németül – vélik. De ki „ez" a Hermine? Nem más, mint a regensburgi Speech Exprets cég által felokosított Siemens high-tech mosógép, mely képes a hozzá intézett szavak megértésére, és saját maga is szavakkal válaszol. Ez lehet a háztartási eszközök jövője, és a közeljövőben több ilyen könnyen kezelhető, abszolút felhasználóbarát berendezés kerül forgalomba. A fejlesztő mérnökök úgy gondolják, hogy az egyre nagyobb tudású gépeket már-már olyannyira bonyolult kezelni, csak az emberrel szóban is kapcsolatot teremtő gépek jelenthetnek megoldást. Hermine jelenleg már több száz szót képes felismerni és kimondani, de folyamatosan fejlesztik és szókincse több ezer szóból fog majd állni. Rövidesen elérkezik az idő, amikor embertársainkkal már nem jövünk ki, így fecsegni kezdünk kedvenc háztartási gépünkkel...

A high-tech autók igazi látványosságot jelentettek. Ezek minden, manapság elérhető új technológiával fel vannak szerelve, így nagy felbontású LCD monitorok, nagy teljesítményű processzorok, DVD lejátszók és faxgépek is helyet kaptak bennük. A stuttgarti székhelyű Mercedes több olyan E és S osztályos modellt mutatott be, melyekből a cég munkatársai mozgó irodát, illetve mobil szórakoztató központot varázsoltak. Ezen autók lelke az az MFCU (Multifunction Communication Unit), vagyis multifunkciós kommunikációs egység, mely a hátsó ülések könyöklőjében kapott helyet. Segítségével lehet faxolni, szkennelni, fénymásolni, ezenkívül említésre méltó, hogy egy GSM mobiltelefon és egy nagy sávszélességű modem is részét képezi.

Természetesen itt egy PC is található, mely egy 700 MHz-es Intel Mobile Pentium III processzorra, egy 10 GB kapacitású merevlemezre, valamint 512 MB memóriára épül. Kijelzőjét alaphelyzetben nem lehet látni, viszont gombnyomásra előbújik az első ülés háttámlájából. A kínált szórakoztató elektronikai csomag két darab, az első ülések háttámlájába integrált, 6,5 colos képátlójú LCD kijelzőből, valamint hat darab DVD lemez kezelésére képes DVD-ROM meghajtóból áll. A kijelzőkön nemcsak DVD filmeket, hanem televíziós műsorokat is lehet nézni. Az autóba építhető komplett irodai rendszer ára közel húszezer, a szórakoztató elektronikai csomagé pedig több mint háromezer euró.

Telefon-csodák főként a vezeték nélküli készülékek területén voltak. Az egyik legjelentősebb, jövőbe mutató fejlesztés a vezetékes készülékeken alkalmazható képküldési szolgáltatás (Fixed Line Picture Messaging), mely lehetővé teszi, hogy MMS üzenetet is küldhessünk vezetékes telefonokra. A SVOX elnevezésű program segítségével pedig meghallgathatjuk szöveges üzeneteinket, sőt, a szoftver szükség esetén még fordítani is tud!

A wa@vebox készülék összeköttetést létesít a televízió és a PC között, és a Bluetooth-technológia segítségével lehetővé teszi, hogy az Internetről letöltött tartalmakat – filmeket, MP3 fájlokat – tévén nézzük meg, vagy meghallgassuk őket sztereó berendezésünkön.

Az új mobil-csodák között a Siemens újdonságainak egyik érdekessége, hogy a telefon két oldalán helyezkednek el a számbillentyűk. Ennek köszönhetően lehetővé vált, hogy a színes display a készülék közepére kerüljön, anélkül, hogy növelné a méretet. A központi irányítógomb segítségével a kijelzőn megjelenő képeket álló vagy fekvő formátumban is megtekinthetjük. A 160x120, vagy maximum 640x480 pixe-

les képeket összeköthetjük hangokkal és szöveggel, s így tökéletes multimédiaüzenetet hozhatunk létre. A mobilkészülékbe a fényképezőgép, videó- és audiolejátszó mellett egy FM-rádiót is beépítettek, s üzleti alkalmazásai révén a telefon egy normál PDA-nek (digitális személyi titkár) megfelelő teljesítményt nyújt, sőt számos játék is játszható vele.

A jubiláló Motorola – amely az első kereskedelmi forgalomba került mobiltelefonja huszadik évfordulóját ünnepli – a fejlett technológia elkötelezettje: újgenerációs 2,5 és 3G megoldásokkal várta az érdeklődőket. Bemutatták a világ első Java és Linux kompatibilis mobiltelefonját is, amely amellett, hogy egy PDA szolgáltatásait nyújtja, digitális kamerával, videólejátszóval, MP3 lejátszóval, kihangosítóval, fejlett üzenetkezelési funkciókkal és Internet eléréssel rendelkezik és támogatja a Bluetooth vezeték-nélküli technológiát.

A háromdimenziós monitor régóta ígért prototípusát is bemutatták az érdeklődőknek, amely ígéretes megoldásával befolyással lehet a jövő számítógépeinek világára. Az új technológia lehetővé teszi, hogy külön segédeszköz (mint pl. „3D szemüveg") nélkül nézhessünk nagyfelbontású háromdimenziós képeket. A hatás eléréséhez két LCD kijelzőt építettek egymásra, amelyeken egy speciális réteg irányítja a képpontok fényét a jobb, illetőleg bal szem irányába. Megfelelő pozícióból nézve az egyik szem csak az alsó kijelző réteg képét látja, míg a másik szem számára a felső látható. Ezek után már csak azt kell meghatározni, hogy az egyes rétegek milyen képet jelenítsenek meg, a felhasználó agya pedig a két különböző képből háromdimenziós, térhatású képet alkot. A Sharp Japánban forgalmazott SH251iS típusú telefonjában már a gyakorlatban is alkalmazza ezt a technológiát, de a nagyobb méretű kijelzők sorozatgyártása még várat magára.

Bővebb információt a Deutsche Messe AG Hannover honlapján (www.messe.de), vagy a CeBIT 2003 közvetlen címén (www.cebit.de) találhatunk. Az utóbbin virtuális formában is átélhetjük a CeBIT-et. Aktuális információkat kapunk a programokról, ízelítőt Hannover és környéke kulturális kínálatából. Számos kiállító már a vásárok előtt elhelyezi ezen a honlapon termékei leírását, cége rövid bemutatását, vagy az önálló honlapjára utaló linket.

Jövőre 2004. március 18-24. között lesz Hannoverben CeBIT, addig is ajánlom az idei választékot:

CeBIT America – június 18-20. New York City,
CeBIT Asia – szeptember 18-21. Shanghai,
CeBIT Australia – május 6-8. Sydney,
CeBIT Eurasia Bilisim – szeptember 2-7. Isztanbul,
CeBIT Home Electronics – május 14-17. Shanghai,
CeBIT Broadcast Cable & Satellite – október 17-20. Isztanbul,
CeBIT Satellite & Communications – augusztus 26-28. Long Beach, California.

Minőségi Televíziót Igénylő Nézők I. Országos Találkozója

Budapest
2003. június 25-27.

A Magyar Informatikai és Kibernetikai Egyesület Elnöksége ez évben június 25. és 27. között rendezi meg a Minőségi Televíziót Igénylő Nézők I. Országos Találkozóját.

•

A nyitó napon a Magyar Tudományos Akadémia Elnökségének tagjai és tudományos intézményeinek vezetői tartanak előadásokat. Őket követik az Országos Rádió és Televízió Testület és a közszolgálati televíziós társaságok kuratóriumainak elnökei és a kereskedelmi televíziók képviselői. Befejezésül az Országgyűlés Kulturális Bizottságának tagjaival találkozhatnak a résztvevők.

A konferencia második napján a televíziózás technikai lehetőségeibe kaphatunk betekintést, többek között az EMC, az IBM, az INTEL és a NOVELL cégek vezető szakembereinek előadásai keretében. A hazai lehetőségeket a Hírközlési Felügyelet, az Antenna Hungária és a Kábeltelevíziós Szakmai Szövetség vezetői ismertetik előadásaikban.

A harmadik napon a tudományos és művészeti egyesületek tagjai, a helyi televíziós társaságok vezetői, valamint a nézői csoportok országos képviselői mondják el véleményeiket.

•

A konferenciára az előzetes jelentkezést kérjük a szervezőkkel közölni.
Elektronikus levélcím: tvnezo@freemail.hu
Kívánságra (június 15-től)
részletes programot küldünk!

Üdvözlettel:

a MTNE Elnöksége nevében
Garádi János

A körsugárzó rövidhullámú antennák, antennarendszerek fejlődése és a hazai eredmények

DÓSA GYÖRGY
okl. villamosmérnök

A húszas évek végén, a harmincas évek elején a megindult rövidhullámú műsor és kommunikációs sugárzás a távoli célterületekkel biztosította az összeköttetést. A rövidhullámú rádiózást kedvező eredményei alapján más szolgáltatások is alkalmazni kezdték, melyek az alábbiakra terjedtek ki: tengerészeti és folyami hajózás, légiforgalom, meteorológiai szolgálat, halászat...

Azonban nem csak nagy távolságokra kellett biztosítani a megfelelő összeköttetést, hanem az adóállomások körüli közeli körgyűrűben is. Ez új antennarendszereket (sugárzókat) kívánt meg azon feltétellel, hogy a napszaknak, évszaknak megfelelő frekvencián optimális és zavarmentes összeköttetést biztosítsanak.

Az irányított rövidhullámú antennarendszerek főbb alaptípusai ezidőben már kialakultak. A körsugárzó antennák kutatása és fejlesztése is eredményes volt, így kezdték ezeket alkalmazni.

A körsugárzó antennákat, antennarendszereket az alábbiak szerint lehet csoportosítani:

I. a) Félhullámú, egészhullámú vízszintes és függőleges dipolantennák, különböző kialakításban
b) Hajlított dipol-antennák
c) Szélessávú dipol-antennák (vertikális varsa, kettős kúp, diszkon, kompenzált antennarendszerek)

II. Vízszintes dipolokból kailakított körsugárzó antennarendszerek (négyszög dipol, guadrant antennarendszerek).

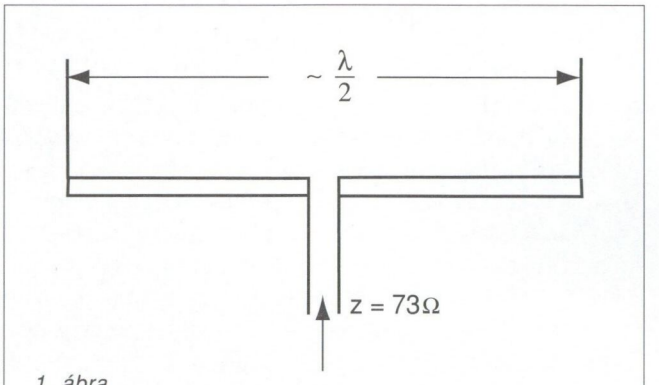
III. Körsugárzó log.per. antennarendszerek (vízszintes dipolokból kialakított log.per. körsugárzók)

Az alábbiakban időrendi sorrendben vizsgáljuk a legjelentősebb (legelterjedtebb) körsugárzó antennarendszerek sugárzási tulajdonságait és alkalmazási lehetőségeit.

A kezdeti időszak

A harmincas évek elején a legelterjedtebben használt közel korsugárzó antennarendszer a vízszintes, félhullámú, középen táplált sugárzó volt, mely meghatározott frekvencián üzemelt (rezonáns sugárzó rendszer).

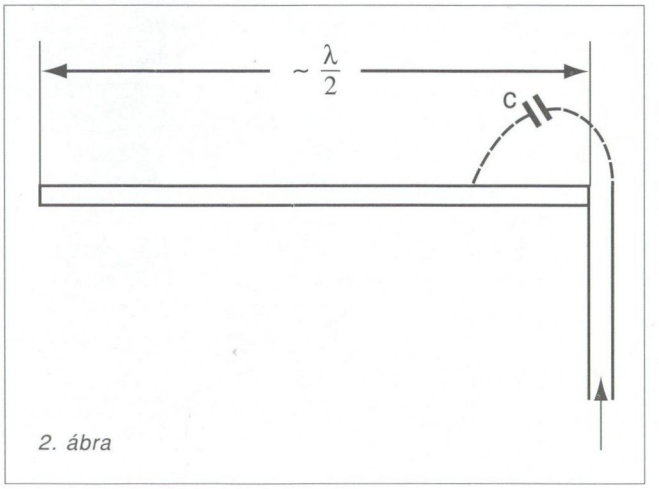
Elvi kialakítását az *1. ábra* szemlélteti. Az antennarendszer sugárzási maximum iránya a vízszintes síkban mindig 90°-ot zár be a dipol tengelyével. Amennyiben a sugárzó rendszer *H* magassága kb. λ/4, ez esetben a függőleges síkban a sugárzási főirány hajlás szöge (kilövelési szög) 30-90° között volt. Ezzel 100-900 kilométeres körterületet lehetett ellátni, figyelembe véve a napszaknak megfelelő optimális frekvenciát. Ez időben kb. 5-15 kW teljesítményt sugároztak.



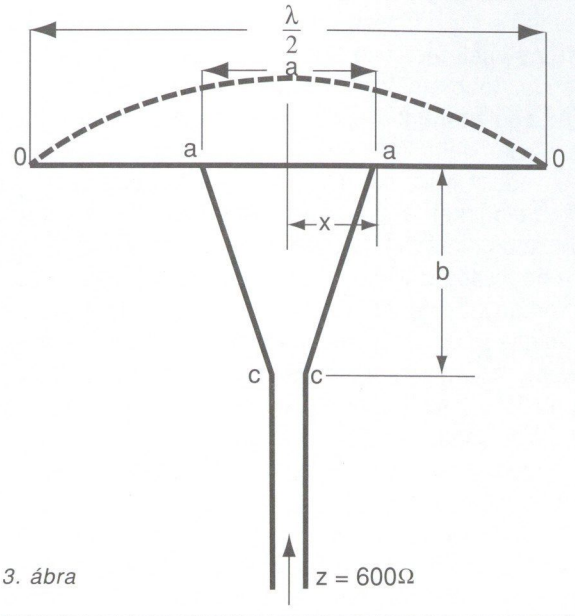
1. ábra

A félhullámú dipol bármelyik pontján táplálható. Tekintettel arra, hogy a félhullámú antenna hullámellenállása a huzal hosszától és keresztmetszetétől függően több száz ohm is lehet, a végpont ellenállása több ezer ohm értékű. Különösen nagy ellenállás érték adódik a vékony huzalból készült antennák esetében. Ezért végponton a feszültségtáplálás jöhetett szóba.

Kisebb teljesítményű rövidhullámú adóberendezéseknél, egyszerűségüknél fogva a végén táplált félhullámú dipol sugárzók kerültek alkalmazásra *(2. ábra)*. A két vezetékes tápvonal a végpontokra tolódik, egyik pontja azonban nem fémesen, hanem kapacitív úton csatlakozik az antennára.

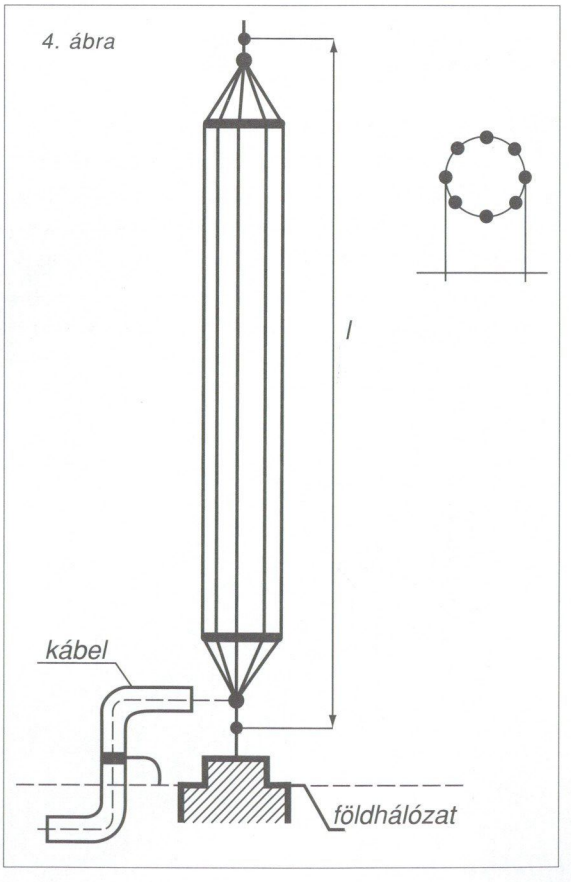


2. ábra



3. ábra

A harmincas évek második felétől alkalmazott rövidhullámú, közel körsugárzó rendszer a sönttáplálású, vagy villásdipol antennasugárzó *(3. ábra)*. A táplálási mód kedvező, mert a sugárzót nem kellett megszakítani a táppontban, a tápvezeték pedig haladóhullámú lehetett, miután az antenna *c - c* pontokban 600 ohm valós ellenállással terheli a vezetéket, és az *a - a* pontok helyes megválasztása esetén a szimmetrikus kétvezetékes tápvonal gyakorlatilag állóhullám mentes. A villaalakú vezeték közelítőleg $b = \lambda/8$ hosszúságú.



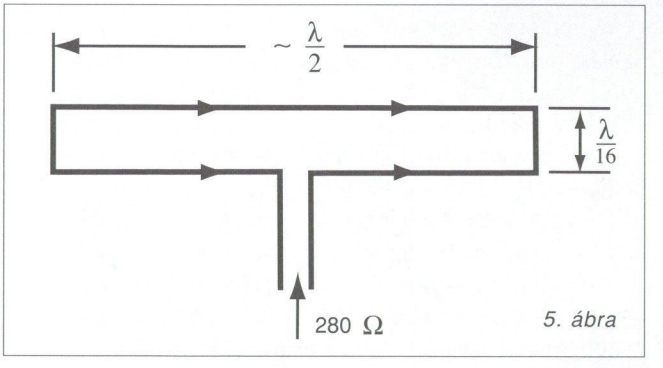
4. ábra

Ezen antennatípus aránylag könnyen és gazdaságosan volt kivitelezhető, emiatt terjedt el. A rövidhullámú adóknál szükséges, hogy egy antenna lehetőleg több frekvencián is megfelelően üzemeljen. Az ilyen szélessávú (1-2 MHz) antennák kis, kb. 100Ω hullámellenállásúak, amit az átmérő növelésével érnek el. Kezdetben a szélessávú rövidhullámú antennák egyik megoldása a horizontális dipo volt, mely varsás (Reuse) kialakításban – több vezetékből – készült. A függőleges sugárzók is ilyen kialakításban készültek, de ellensúly, vagy földrendszer kiépítése felétlen szükséges volt. *(4. ábra)*.

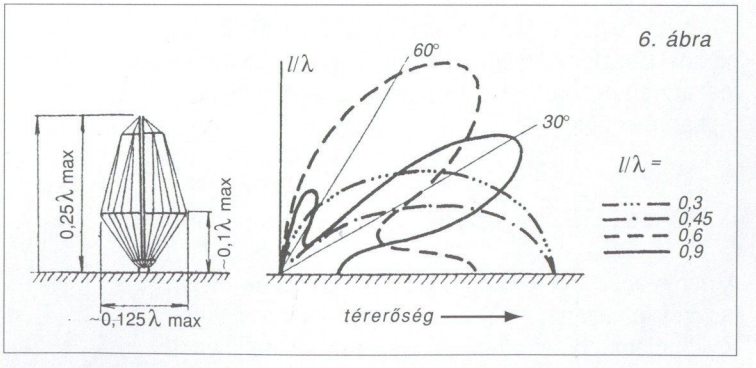
Ebben az időszakban kerültek használatba a hajlított (hurok) dipol antennák is, miután valamivel szélesebb sávot sugároztak, mint az egyszerű dipol és tápponti ellenállásuk is nagyobb volt *(5. ábra)*. Ezt 280 ohmos szimmetrikus kétvezetékes tápvonallal táplálták.

A függőleges és vízszintes dipol antennák csak egy frekvencián, vagy keskeny fekvenciasávban sugároztak. A műsorszolgáltatást a napszaknak megfelelően mindig az optimális frekvencián kellett sugározni, tehát naponta legalább két-három frekvencia használatára volt szükség. Ez tehát sok, különböző frekvenciájú antenna telepítését kívánta meg, ami gazdaságtalanná és bonyolulttá tette a szolgáltatást.

A kutatások arra irányultak, hogy olyan szélessávú körsugárzó készüljön, mely lehetőleg a rövidhullámú tartomány nagy részében, de főleg a 6-20 MHz-es tartományban illesztés nélkül üzemeltethető. A negyvenes évek végére született meg a vertikális bikónikus (exponenciális) szélessávú körsugárzó varsa sugárzó rendszer, melynél a hullámellenállás a talpponttól közel exponenciálisan növekszik. A szélessávúság érdekében az antenna talppontjánál folyamatos átmenetet kell biztosítani a konstans hullámellenállású tápvonal felé. Ezt csak konuszos végződéssel kombinlva lehetett biztosítani. Az átviteli sáv növe-



5. ábra

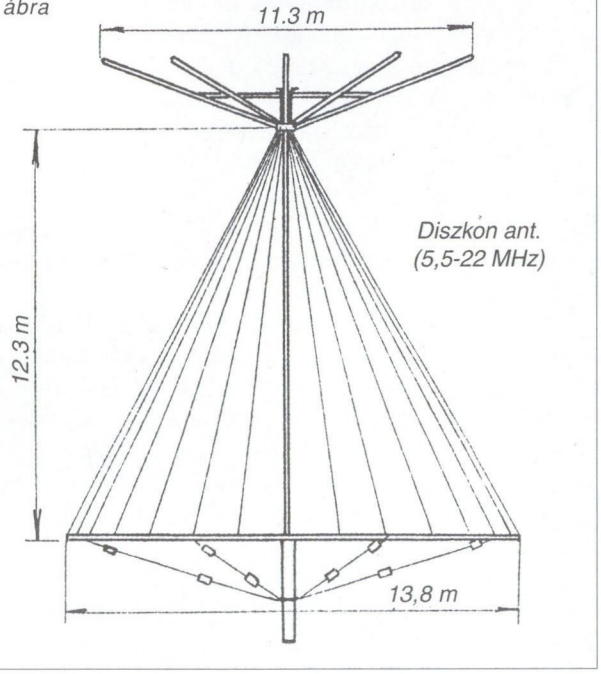


6. ábra

lése érdekében csökkenteni kellett továbbá az antenna hullámellenállását, ezért növelték az antenna ármérőjét. Ez az antenna 1:5 frekvenciatartományt hidalt át, kb. 300-2600 km-es zónában *(6. ábra)*. A megfelelő sugárzás érdekében radiális földrendszer kiépítése volt szükséges, melynek hossza az antenna magasságával azonos.

A hatvanas évek elején a Telefunken cég rövidhullámú diszkon antenna néven egy új rövidhullámú, szélessávú körsugárzó antennát fejlesztett ki *(7. ábra)*. Ez egy alul nyitott kónusz, mely tartótoronyra szerelhető, felül szigetelőkre épített több ferde fénycsőből állt. A rézszálak 30°-os (optimális) szög alatt futnak össze. Ilyen antennatípust 50 kW teljesítményre is készítettek.

7. ábra



A hetvenes évek elején kezdték használni a csillapított szélessávú körsugárzó rövidhullámú antennákat (SKD = sorosan kompenzált dipol rendszerek) függőleges és vízszintes kialakításban. Ezek a szélessávot a sugárzó rendszerbe (dipolba) meghatározott helyen és értékben kompenzáló induktívitás vagy ellenállás beépítésével biztosították. Ez növelte a sugárzási ellenállást, és el lehetett érni aránylag kis méretek mellett 1:3 frekvenciaátfogást. A csillapított antennák helyigénye kisebb, azonban az összhatásfokuk alacsonyabb, mint a csillapítatlan vertikális, bikónikus varsa sugárzó rendszereknek.

Összefolgalva tehát a szélessávú vertikális sugárzók illesztését meghatározta, hogy reflexiómentes átmenetet kellett biztosítani az antenna és a tápkábel között.

A 40-es, 50-es évek

A negyvenes évek végén, az ötvenes évek elején kezdtek alkalmazni vízszintes dipolokból kialakított rövidhullámú körsugárzó rendszereket, melynek a két legismertebb típusa a szögletantenna (quadrant antenna) és a négyszög dipol. A szögletantennák általában egyemeletes, míg a négyszög dipolokból felépített antennák több emeletes kialakításban is készülnek.

A szögletantenna két egymásra merőleges, a középfrekvencián félhullámú vízszintes dipolból áll. Középen táplált egész hullámú vízszintes dipolból úgy képezhető, hogy a dipol két fél ágát egymásra merőlegesen helyezik el. A szögletantennát a csúcspontban táplálják.

A négyszög dipol egy-egy emeletét egy négyzet oldalai mentén elhelyezett $\lambda/2$ dipolok alkotják. A négyszög dipol minden emeletét amplitudóban és fázisban azonos antenna áramokkal táplálják *(8. ábra)*. Az emeleteket egymástól $\lambda/2$ távolságban kell elhelyezni. Az alsó emelet földfeletti magassága az antenna kilövelési szögét határozza meg, tehát a terület besugárzás szempontjából fontos a tervezésnél.

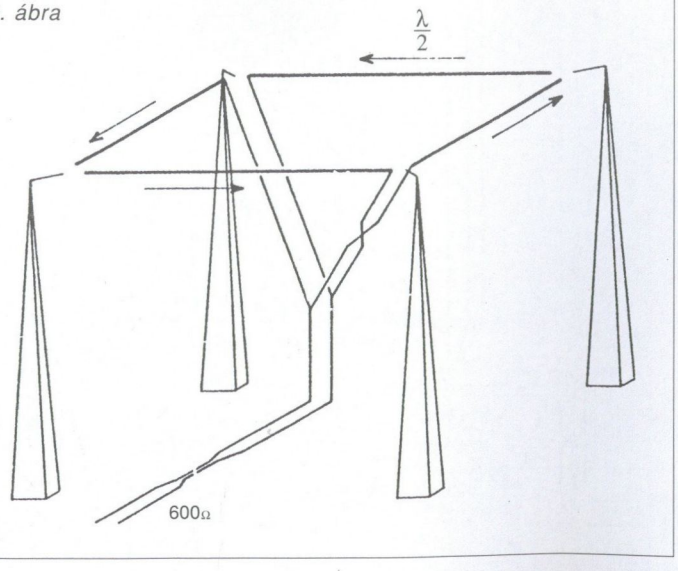
Az ötvenes évektől ezen antennák terjedtek el, mert kedvező tulajdonságuk volt, hogy az emeletek számának növelésével az irányélesség növelhető volt (nyereségnövekedés). Sugárzási karakterisztikájuk és nyereségük e típusoknál elsődlegesen az antenna elemek geometrikai elrendezésétől függ, ezért az adóállomástól kb. 400-2000 km sugarú zónában jó területi ellátást tud biztosítani. Ezen antennarendszereket 200-500 kW teljesítményre rendszeresen alkalmazták.

Feltétlen meg kell említeni, hogy egészen közeli területek, zónák ellátására (besugárzására) az ötvenes évek elején alkalmazásra kerültek a meredek sugárzók, vagy másnéven Jamaicai és Trinidad antennák, melyekkel kb. 0-500 km sugarú zónában lehetett biztosítani az ellátást.

A 60-as évek

A szélessávú körsugárzás követelményeit kielégítették tehát a kónikus és a bikónikus függőleges antennarendszerek. A kónikus antennáknál azonban több olyan probléma lépett fel, mely az alkalmazásukat korlátozta. A kónikus antennák vertikális szerkezetek (monopolok), ezért a jó

8. ábra



sugárzási hatásfok elérése érdekében ezen antennáknál meghatározott hosszúságú radiális földhálózat kiépítése volt szükséges. További hátrányt jelentett, hogy általában csak 2:1 illetve 3:1, speciális esetben 4:1 frekvencia átfogással rendelkeznek, tehát az egész rövidhullámú tartományt, a 3-30 MHz-es sávot nem tudják átfogni. Kedvezőtlen továbbá az is, hogy vertikális karakterisztikájuk is változik a frekvencia függvényében. A körsugárzó karakterisztika megfelelő előállítása hagyományos antennákkal, tehát a teljes rövidhullámú frekvencia sávban problémát jelentett.

Nagy jelentőségű volt a hatvanas évek közepén, hogy megjelentek a szélessávú körsugárzó log.per. antennák (Duhamellsbell-Carrel-Radford munkái alapján) melyek 10:1 frekvenciaátfogással rendelkeztek. További nagy előnyük ezen antennáknak, hogy az adott frekvenciatartományban a bemeneti impedancia, a nyereség, és az iránykarakterisztika a frekvenciával csak kis mértékben változik, így az egész rövidhullámú sáv átfoghatóvá vált. Ezért a rövidhullámú adóállomásokon a jóval kevesebb szélessávú körsugárzó log-per. antenna alkalmazásával jelentős terület- és költségmegtakarítás adódott.

A gyakorlatban kétféle kialakítású körsugárzó log-per. sugárzó terjedt el:

a) csúcsával lefelé, a földre merőlegesen kialakított LP síkrendszer *(9. ábra)*,
b) trapéz, esetleg háromszög fogazású, húzalstruktúrájú biplanar log-per. antennarendszer.

A biplanar log-periodikus körsugárzó huzalantenna sajátossága, hogy nincs külön tápvonalrendszere. Előnye, hogy egyszerű és tartására egy tartótorony is elegendő és külön földrendszer kiépítését nem igényli. Ezeket az antennákat ma 100-300 kW teljesítményekre alkalmazzák.

A negyvenes évek végétől Diósd és Székesfehérvár-Sóstó rádióállomásokon, főleg műsorsugárzásra a négyszög dipol kialakítású körsugárzó antennákat, több mint két évtizeden keresztül használták. A hazai fejlesztésű és gyártású (Híradótechnikai Vállalat) exponenciális (bikónikus) varsa körsugárzó antennarendszer Székesfehérvár-Sóstó rádióállomáson 20 kW-os ÉMV gyártmányú adóberendezéssel 1969 nyarán kezdett sugározni.

Ez 4-20 MHz frekvencia-tartományban 300-2600 km-es zónában tette lehetővé a vételt, így rugalmasan használhatták Európa, Észak-Afrika, Közel-Kelet területeire. Az antennarendszer meghatározott időszakban és frekvenciákon ma is résztvesz a rövidhullámú műsorsugárzásban.

A közelmúlt

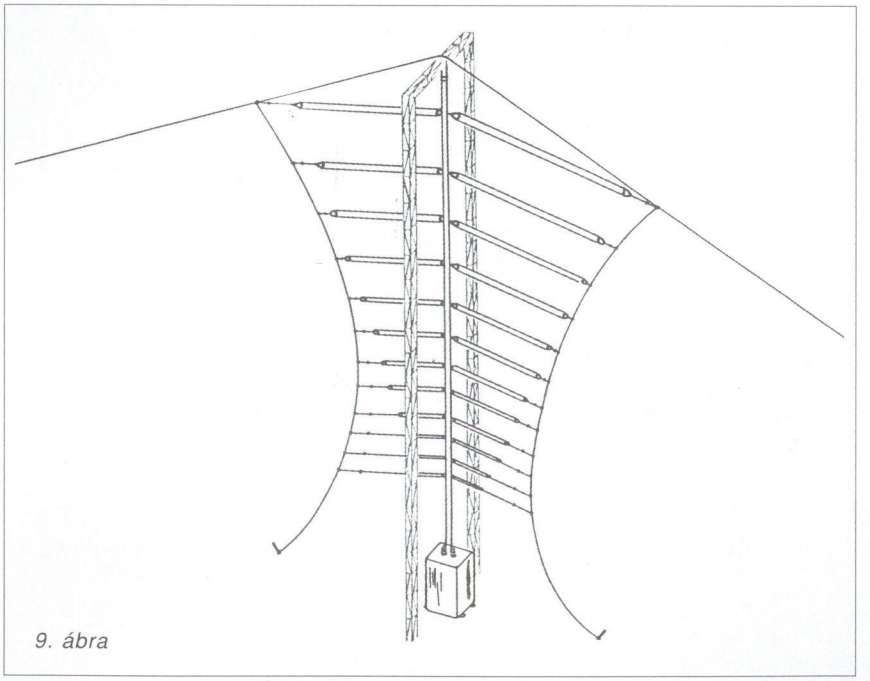
Rövidhullámú szolgáltatásunk bővítése érdekében 1983-ban és 1989-ben új, 100 kW-os BBC gyártmányú rövidhullámú adókkal kezdték meg sugárzást Diósd és Székesfehérvár-Sóstó rádióállomásokon, körsugárzó quvadrant (szöglet) antennákkal (Kossuth, Szülőföld, idegennyelvű műsorok).

Ezek jelenleg is biztosítják a Kárpát-medence és közép-európai terület besugárzását. A legkorszerűbb körsugárzó log.per. antennarendszer – teljesen hazai fejlesztéssel és hazai gyártással (Híradótechnikai Vállalat) – 1979-ben, majd 1987-ben Székesfehérvár-Sóstó rádióállomáson kezdte meg üzemét.

A körsugárzó log-per. antennarendszerek fejlesztésénél a karakterisztikák vizsgálatára 1:30, impedancia viszonyok vizsgálatára pedig 1:10 arányban kicsinyített modellantenna készült.

A modell mérések és vizsgálatok a Bugyi-Telekpusztai antennamérő telephelyen történtek. A szélessávú körsugárzó log-per. antennák egy új generáció első fejlesztett tagjai voltak és hazai, de közép-európai szinten is először kerültek alkalmazásra.

Ezek még ma is rendszeresen sugározzák a rövidhullámú idegennyelvű, illetve a Szülőföld műsorokat. Korábban az európai postai rádiótávíró forgalmazást, és a MAHART forgalmazást biztosították. A digitális adók alkalmazásakor elsősorban ezen antennarendszerek, és részben a szöglet körsugárzó antenná fogják a meghatározó szerepet betölteni.



9. ábra

Irodalom:

[1] Meinke-Gundlach: Rádiótechnika kézikönyv, Műszaki Kiadó, Budapest, 1961.
[2] E. Laport: Radio Antenna Engineering, McGraw-Hill
[3] H.Jasik: Antenna Engineering Handbook, McGraw-Hill, 1961
[4] Dósa György: Megemlékezés egy évfordulóról, HTE Hírlevél, 2000/10.

Erratum • Helyreigazítás

SZABÓ ZSOLT

A Híradástechnika 2003/3 számában megjelent „A Preisach hiszterézismodell" című cikkem számos kiadói hibával került leközlésre. A hibák főleg a matematikai összefüggések és az ábrák esetén zavarók. A cikkhez az alábbi javításokat szeretném hozzáfűzni.

48. oldal

A Preisach-háromszögön értelmezett kétváltozós eloszlást nevezzük Preisach eloszlásnak.

50. oldal

A *3. ábrán* (49. oldal) különböző mágneses térerősségek esetén a Preisach háromszögön kialakuló le- és felkapcsolt operátorokat tartalmazó tartományok, valamint a megfelelő hiszterézis görbék láthatók.

$$M = \iint_T \mu(h_1,h_2)\gamma(h_1,h_2,H)dh_1dh_2 = \iint_{T_1} \mu(h_1,h_2)dh_1dh_2 - \iint_{T_2} \mu(h_1,h_2)dh_1dh_2 = I_1 - I_2 \quad , \quad (6)$$

A Preisach eloszlás integrálját egy háromszög alakú tartományon nevezzük Everett függvénynek

$$E(x,y) = \int_x^y \int_x^{h_2} \mu(h_1,h_2)dh_1dh_2 \ . \quad (7)$$

A cikkben szereplő (7) összefüggés sajtóhiba.

A T_1 és T_2 tartományokra vett integrálok kifejezhetők az Everett függvények segítségével

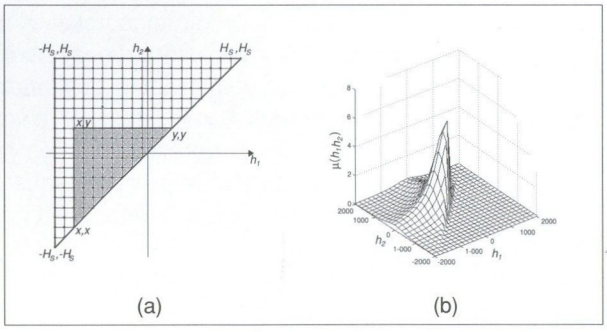
$$I_1 = E_2 - E_1 + E_4 - E_3 + E_6 - E_5 \ , \quad (8)$$

hasonlóképpen

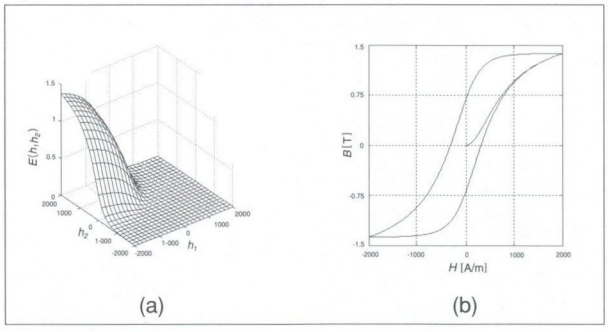
$$I_2 = -E_1 + E_3 - E_2 + E_5 - E_6 \ . \quad (9)$$

52. oldal

Kimaradt az *5. ábra* képaláírása és a *6. ábra*.



5. ábra A Preisach háromszög a rácspontokkal, amelyekben adottak az eloszlásfüggvény értékei



6. ábra Lorentz eloszlásból számolt Everett függvény és hiszterézis görbe

55. oldal

A fenti összefüggést behelyettesítve a (21) összefüggésbe a következő összefüggés adódik

56. oldal

A Preisach modell legnagyobb hiányosságának a kongruencia tulajdonságot tartják.

Ez azt jelenti, hogy az előélettől függetlenül, azonos mágneses térerősségek közötti gerjesztés esetén kapott minorhurkok egybevágók.

Könyvet ajánlunk

Ajtonyi István: Automatizálási és kommunikációs rendszerek

Ez év tavaszán jelent meg Prof. Habil Dr. Ajtonyi István szerkesztésében a könyv. Célja, hogy a villamosmérnököknek egységes képet adjon az automatizálás, távirányítás és hírközlés korszerű módszereiről. A könyv jól illeszkedik a miskolci képzéshez, ahol a hagyományoknak megfelelően gépész és kohász mérnököket nevelnek, mely szakmák jelenleg már alkalmazzák a számítástechnika és a távvezérlés eljárásait. Az automatika, a vezérlés, az irányítás és a távközlés egységes ismerete szükséges minden üzemszervezőknek, automatizálónak, gépészmérnöknek és azon technológusoknak, akik a folyamatos üzemért felelősek.

A könyv első fejezete a „folyamat közeli automatizálás", a programozható vezérlők (Programmable Logical Controllers – PLC) bemutatásával kezdődik. Ez az alapelem, amelynek ismerete elengedhetetlen bármely vezérlési, ellenőrzési folyamat tervezésénél. De ismernie kell ezek felépítését, alkalmazását azoknak is, akik egy korszerű gyárat akarnak üzemeltetni. Példával, grafikus módszerekkel alátámasztva készítik elő a szerzők ennek szakszerű használatát. A könyv első fejezete számos olyan kérdést is tárgyal, melyeket később távvezérlési, automatizálási és hírközlési fejezetek is jól használhatnak. Matematikai precizitással vezeti be a mintavételezési jeleket, ismerteti az átviteli függvényeket. Ebben a fejezetben találkozhatunk a stabilitás fogalmának meghatározásával, az átviteli függvények kezelésével, olvashatunk a Laplace transzformációról, annak alkalmazásáról, Nyquist kritériumról és részletesen megismerhetjük a Bode-diagrammokat is. Ez utóbbi olyan alaposságú, amely az eredeti Bode könyv óta kevés helyen jelent meg. Továbbmenve a Hurwitz polinomok, pólus és zérus helyeivel bővíti az alapismereteket. A könyvben megjelennek a neurális szabályozók is, és a hallgatók megismerkedhetnek a korszerű Fuzzy logika szerepével. Ez az első 170 oldalas fejezet a korszerű egyetemi oktatás alapját képezheti.

A következő fejezet címe: Ipari kommunikációs rendszerek. Ez a cím meglehetősen szerény a tartalomhoz képest, mert a fejezet széles körben és igen alaposan bemutatja a távközlés összes alapfogalmát is. Felsorolásszerűen a következő címek jellemzik ezt a fejezetet: Fourier sor és integrál, mintavételezés, kvantálás, analóg és digitális modulációs rendszerek, hang és képkódolás Ez a rész egyértelműen minden távközlési oktatásnak alapját képezi és felkészíti az egyetemi hallgatókat arra, hogy később ezen a területen is biztonsággal dolgozhassanak. A különböző hálózati struktúrák, átviteli közegek után áttekinti a speciálisan irányítástechnikai hálózatokat. Ezen ismeretek birtokában a gyakorlati üzemi, automatizálási hálózatok már biztos alapokra építhetők. A fejezet további része valós ipari, energiaellátó hálózatok kialakításával foglalkozik.

A negyedik fejezet már speciális, irányítási és informatikai rendszerek bemutatását tűzi ki célul. Az olvasó megismerkedhet a különböző LabVIEW mérésnek, adatgyűjtési eljárásokkal, találkozhat adatbázis kezelő és folyamatirányítási rendszerekkel. Gyakorlati példákkal és a szolgálat minőségének meghatározásával is foglalkozik. Ez a rész a mérnökképzésnek olyan speciális területét mutatja be, melynek segítségével az olvasók, vagy egyetemi hallgatók a gyakorlatban legtöbbször használt eszközöket ismerik meg.

A következő rész feltételezi, hogy a folyamatok szabályozása, ellenőrzése, vezérlése távol helyezkedik el a gyakorlati üzemeltetési helytől. Ilyenkor az automatizálási feladatot megoldó mérnököknek magánhálózatot, vagy virtuális magánhálózatot, vagy közforgalmi hálózatot kell igénybe venniük. Ezen döntésük meghozatalához ismerniük kell a különböző átviteltechnikai, kapcsolástechnikai módszereket, a fix és a mobil hálózatok főbb jellemzőit és ezeket kell a saját feladatukhoz, átviteli követelményeikhez illeszteni. Az ehhez szükséges ismereteket a korszerű eszközök figyelembe vételével szintén elsajátíthatják ebből a könyvből. Megfelelő előrelátással a jelenleg még fejlesztés alatt álló mobil és csomagkapcsolt rendszerekről is képet kapunk. A fejezet különös jelentőségű abból a szempontból, hogy az automatizálási és távközlési szakemberek együttműködéséhez megadja a közös nyelvet.

A hatodik fejezet az információvédelem, a kriptográfiai módszerek alapjainak bemutatása után bemutatja a digitális aláírás, a személyi kártyák, a személyazonosítás korszerű eszközeit. Ezzel a könyv lehetővé teszi, hogy az automatizálási szakemberek saját ismereteik alapján dönthessenek a rendszer biztonságához szükséges eljárásokról is.

A szerkesztő és a könyv nagy részét író Ajtonyi professzor jeles munkát végzett mind az anyag összeállításában, mind a nyolc különböző érdeklődésű szerző eltérő szemléletmódjának összehangolásában. A könyvet Csopaki Gyula lektorálta.

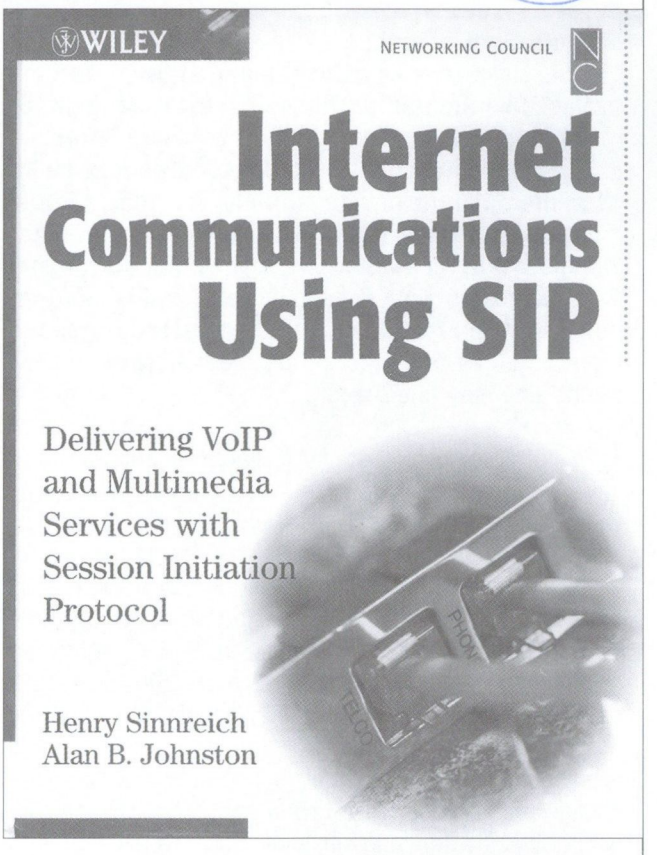
A könyv szerzői nagyrészt a Miskolci Műszaki Egyetemen dolgoznak. Korábbi előadásaik anyagát és több év tapasztalatát tartalmazza a könyv. Biztosak vagyunk abban, hogy ez a felsőoktatásban jól használható lesz és elősegíti, hogy a szakemberek kiválóan ismerjék a szakma alapjait és gyakorlatát.

(L. Gy.)

Könyvet ajánlunk

Henry Sinnreich, Alan B. Johnston: Internet Communications Using SIP

A könyv a John Wiley and Sons kiadásában jelent meg a „Networking Council Books" sorozatban, 2001-ben. A könyv két izgalmas, mai témát kapcsol össze, az Internet kommunikációt és napjaink egyik, talán legtöbbet emlegetett protokollját, a SIP-et (Session Initialization Protocol).



Multimédiás alkalmazások az Interneten – ez a célkitűzés indította el a SIP fejlesztését, de a SIP elterjedése forradalmi változásokat hozhat a távközlésben is, mert a hangátvitelt beilleszti az Internet szolgáltatások közé, és így nincs szükség külön beszédátviteli hálózatra.

A könyv szerzői, Henry Sinnreich, aki korábban a Bukaresti Postai és Távközlési Intézet kutatója volt és Alan B. Johnston az Internetes társadalom megbecsült szakemberei, mindketten az Internet szabványok aktív kidolgozói, az IETF (Internet Engineering Task Force) szakértői. Fő szakmai területük az IP alapú telefónia, munkahelyük a WordCom.

A könyv terjedelme 298 oldal, 18 fejezetből áll. Az első négy fejezet áttekintést ad az Internetről a szolgáltatások szempontjából. Röviden bemutatja, hogyan használhatják az intelligens hálózati szolgáltatások a SIP-et, hogyan tud a SIP együttműködni ITU-T protokollokkal és hogyan valósítja meg az eredetileg kitűzött célt, az Internet multimédiás szolgáltatásait.

A következő fejezetek bemutatják a SIP szolgáltatások értékes tulajdonságait megkísérelve a hagyományos és Internetes távközlés fogalomvilágát érthetővé tenni mindkét terület szakértői számára. Ezek a fejezetek bemutatják a SIP hálózatot és szolgáltatásait, elsősorban a felhasználó szempontjából.

A következő öt fejezet az alábbi izgalmas témákkal foglalkozik:

- A PSTN és az Internet telefonos szolgáltatásainak vegyes használata
- Hálózati címzések (DNS és ENUM)
- A SIP és a mobil hálózatok
- Szolgáltatások minősége
- Komponens szerver architekturák

Befejezésül a könyv felvillantja a SIP jövőjét, a várható új alkalmazásokat. A nyilvánvaló 3G alkalmazásokon kívül jelentős fejlesztések várhatók sürgősségi szolgáltatások, helymeghatározás és tűzfallal kapcsolatos biztonsági intézkedések területén.

Minden fejezet végén irodalomjegyzék van, amelyekben az Internet szabványok, az RFC-k részletesen szerepelnek. A könyv végén levő rövidítésjegyzék is megkönnyíti a megértést. A könyv illusztrációs anyaga és összehasonlító táblázatai kitűnőek.

Hogyan értékelhetjük a könyvet, mi az erőssége és melyek a vitatható pontjai?

A könyv világosan elmagyarázza, hogyan egyesíti a SIP a telefonálás előnyeit az internetével. A feltételezett olvasókört azok alkotják, akik mindkét terület iránt érdeklődnek. A könyv erőssége az Internet technológia és a hagyományos távközlés határterületének jól érthető bemutatása.

Kevés vitatható pontot sorolhatunk fel, egyet mégis megemlítenék, amely kétségtelenül a recenziót író személyes elfogultságát is tükrözi és ez a téma a SIP konformancia tesztelése, ami teljesen elkerülte a szerzők figyelmét, bár a felsorolt fejezeteknél korábban találkozhattunk a SIP jövőbe mutató lehetőségeivel. Ennek során tárgyalja a virtuális jelenlétet, az adat biztonságot, és a multimédia alkalmazásokat.

Mindez azt bizonyítja, hogy a szerzők egyértelműen meg vannak győződve, hogy a SIP-nek átütő sikeres lesz. Persze ehhez olyan precizitás ajánlások kellenek, mint amilyeneket az ITU dolgozott ki a H 323 alapú együttműködés zavarmentessége érdekében.

(T.K.)

Contents

Cover: Let us not wait sleepily for the future, but let us shape it actively

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

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

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

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

2003-as előfizetési díjak
Hazai közületi előfizetők részére:
1 évre bruttó 30.000 Ft
Hazai egyéni előfizetők részére:
1 évre bruttó 6.000 Ft

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

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

HU ISSN 0018-2028

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