Tartalom

Címlap: Vajon meddig tart a mobil szárnyalása?

Tovább szárnyal a mobil?

DR. LAJTHA GYÖRGY

lajtha.gyorgy@ln.matav.hu

Lassanként véget ér az a recesszió, amit a szellemi és anyagi tőke nélkül tőzsdére vitt cégek bukása okozott. Ennek tanulságait levonva most már igyekeznek a vállalkozások reális alapra helyezett gazdasági terveket készíteni és ezek megvalósítása érdekében új termékekkel piacra lépni. Egyértelműnek látszott, hogy a távközlés területén számítani lehet a mobil rendszerek további sikereire.

Folyamatosan jelentek meg a GSM rendszerre alapozott új szolgáltatások. Minden várakozást felülmúló sikerrel lehetett értékesíteni a képátviteli üzeneteket, az MMS-t. Fejlődött a szövegátvitel és vannak már GSM készülékek, amelyeknek klaviatúráján betűk is elhelyezkednek. A tartalmi fejlődés mellett újabb divatos készülékek jelentek meg és a gyártók versenyeznek az élénkebb színek és a vidámabb formák használatában. Az új készülékek rendszeresen fogynak a piacon és sok más műszaki cikkhez hasonlóan a felhasználók 2-3 év után szívesen lecserélik készüléküket szebbre, jobbra, nagyobb tudásura.

Ezek a tapasztalatok alátámasztották a 3G, vagy UMTS rendszerek fejlesztését. A szélessávú átvitelt lehetővé tevő új mobil megoldásokat egységesítették, szabványosították és néhány évvel ezelőtt a frekvenciasávokat elárverezték, melyen a kormányok jelentős bevételre tettek szert. Minden előfeltétel megvolt, és mégsem terjedt a várt ütemben a 3G mobil rendszer. Mintha egy láncszem hiányozna. A fejlesztők, gyártók, üzemeltetők, felhasználók láncában a fejlesztők megtették a magukét. Új elveken, csomagkapcsolt rendszerben kidolgoztak egy több 10 Mbit/sec sebességű átvitelre alkalmas távközlő rendszert. A gyártók szeretnék mielőbb gyártásba vinni, hogy bevételeiket mielőbb növelhessék. A lánc első két tagja tehát készen áll a bevezetésre, az elterjesztésre.

A felhasználók szívesen látnák az új rendszert, ha ugyanolyan költséggel vehetnék igénybe a szolgáltatást. A jelenlegi GSM és a kibővített 2,5G legtöbb reális igényüket kielégíti, ezért, bár szívesen látnák az újdonságot, de nem látják indokoltnak, hogy azért többet fizessenek. A szolgáltatók viszont túlságosan nagy összegeket fizettek ki a frekvenciahasználatért, továbbá valószínűleg újabb bázisállomásokat is kellene létesíteni a 3G bevezetése érdekében, tehát jogosnak tartják, hogy ennek egy része gyorsan megtérüljön, vagyis a felhasználók fizessenek többet. Ennél a pontnál lelassult az újdonság elterjedése.

Bár a kiút még nem látszik, de a fejlesztők tovább dolgoznak. Hallani a 4G rendszer kutatási eredményeiről, halvány elképzelések vannak már ennek szolgáltatásairól is. Ezek az eredmények tovább fékezik az üzemeltetők bevezetési készségét. Szabad-e újabb antennahálózatot építeni, ha a 4G ismét más hálózatot követel majd meg. A felhasználók bizonytalanságát sem csökkentik a 4G-ről és az Ubiquitous, mindenütt elérhető szélessávú távközlés kifejlesztéséről szóló hírek. Közben a zöldek is újabb területet éreznek a 3G megjelenésében, ahol a környezet megváltoztatása ellen küzdhetnek.

Mindezen nehézségek ellenére a fejlődés nem áll meg, újabb és újabb mobil kutatási eredményekről tudunk beszámolni. A kutatók felkészültek az IPv6 protokoll használatára mobil hálózatokon. Sokat beszélnek a mobil eszközök segítségével megvalósuló kereskedelmi tevékenységről, és érdekes újdonság a CKK eljárás. Ezen három cikkel igyekszünk képet adni a fejlesztésről. Ehhez kapcsolódnak a protokollok vizsgálatával és a számítógépfürtökkel kapcsolatos kutatások is, bár ezek az eredmények bármely hálózaton használhatók. Nem kapcsolódik szorosan ezekhez a témákhoz, de beszámolunk a kábeltévé hálózatok minőségének javításáról és a villamoshálózat távközlési hasznosításáról.

Talán egy-két hónap múlva már többet tudunk írni az újabb mobilgenerációk hazai bevezetéséről is.

Hálózati protokollok biztonsági tesztelése

LÉCZ BALÁZS*, ZÖMBIK LÁSZLÓ**

** Budapesti Műszaki és Gazdaságtudományi Egyetem, Távközlési és Médiainformatikai Tanszék, lecz@alpha.tmit.bme.hu*

*** Ericsson Magyarország, BME-TMIT, laszlo.zombik@ericsson.com*

Reviewed

Kulcsszavak: biztonság, imprementációk, forgalomelterelés, konformancia

A protokollok és implementációik viselkedését több szempontból lehet vizsgálni, ezért igen sok tesztelési módszer létezik. A legszélesebb körben kutatott és alkalmazott módszerek az implementációk konformanciáját és teljesítményét vizsgálják. Cikkünkben a protokollok megvalósításainak biztonsági vizsgálatára koncentrálunk. Ismertetünk egy új, biztonsági tesztelésre alkalmazható módszert, majd bemutatjuk alkalmazásának lehetőségeit. Végül ismertetjük az általunk megvalósított szoftverkeretrendszert és bemutatunk néhány példát annak gyakorlati alkalmazására.

1. Protokoll tesztelési módszerek

Informatikai és távközlési rendszereink mindennapos, megbízható működése egyre jobban függ a kommunikációs protokollok és implementációik stabilitásától és biztonságától. Az infokommunikációs rendszereink általános biztonságának eléréséhez a protokolloknak meg kell felelniük bizonyos szintű biztonsági elvárásoknak, melyek nagyban függenek az adott protokoll alkalmazási területétől. Ezek teljesítéséhez a protokollokat igen körültekintően kell megtervezni és megvalósítani. Mind a tervezési, mind a megvalósítási fázis ki van téve az emberi hibáknak. Az implementáció során további veszélyforrásokat hozhatnak be a felhasznált szoftvereszközök (például egy hibás függvény-könyvtár felhasználásakor a könyvtárban levő hibák öröklődhetnek). A végterméket (protokoll specifikáció és kész termék) ezért minden esetben meg kell vizsgálni.

A jelenlegi, tesztelésre alkalmas szoftver és hardver eszközök egy-egy fő területet céloznak meg az alábbiak közül: konformancia, teljesítmény és biztonság. Léteznek eszközök, melyek a protokoll formális leírását veszik alapul, míg más eszközök a megvalósítást tesztelik valós vagy emulált környezetben. A vizsgálat módszere lehet formális verifkáció, szimuláció és a megvalósítás ellenőrzése. A biztonsági vizsgálatokhoz mind a három módszert alkalmazzák. Az alábbiakban bemutatunk néhány példát ezekre.

1.1. Formális protokoll verifikáció

A formális protokoll verifikáció elsődleges célja, hogy már a tervezési fázisban visszacsatolást nyújtson. Így a protokoll implementációjának elkészítése előtt fény derülhet a problémákra. Amennyiben a verifikáció hibát mutat ki, vissza kell lépni a tervezőasztalhoz (WEP [5]). További alkalmazásként említhető a már meglévő protokollok megfelelőségének vizsgálata: formálisan ellenőrizhető, hogy egy adott protokoll megfelelő-e egy bizonyos célra (például biztosítja-e az újrajátszás vagy a lehallgatás elleni védelmet).

A protokollok teljesítményének, hibatűrésének és bizonyos biztonsági paraméterek vizsgálatára már léteznek formális módszerek. Mivel a formális protokoll verifikációs módszerek a protokollok leírását használják csak fel, az implementációkban jelentkező hibák nem detektálhatók segítségükkel. Sok esetben fordult már el ő, hogy egy protokollt a formális ellenőrzés során biztonságosnak minősítettek, azonban az implementációba került programozási hiba – ami amúgy a funkcionalitást nem befolyásolta – biztonsági szempontból végzetesnek bizonyult. Rontja a helyzetet továbbá, hogy egy formális tesztelés során biztonságosnak nyilvánított protokoll hamis biztonságérzetet kelt a végfelhasználókban.

A formális ellenőrzéshez szükséges az adott protokoll helyes és teljes formális specifikációja, melyet legtöbbször az adott vizsgáló szoftver leírónyelvén kell megfogalmazni. Ilyen leírás elkészítése sok esetben igen összetett és nagy szakértelmet igénylő feladat. Ez a folyamat is ki van téve az emberi hibáknak, így előfordulhatnak hibás pozitív és hibás negatív eredmények is.

A formális módszerek legnagyobb hátránya, hogy a vizsgálható protokollok halmazát erősen leszűkítik a verifikációs eljárások által a protokollokkal szemben támasztott előfeltételek. Ezen megszorítások sok létező és tervezett protokollt kizárnak a vizsgálható protokollok köréből. További nehézséget jelent, hogy ezek az algoritmusok nem minden esetben garantálják a véges futásidőt. A gyakorlatban alkalmazott, többnyire komplex protokollok vizsgálatához igen nagy számítási- és memóriakapacitásra van szükség.

Megemlítünk néhány, biztonsági szempontból fontosabb, formális ellenőrző szoftvert: FDR [11], Casper [9], NRL Protocol Analyzer [10].

1.2. Szimuláció

A szimulációs módszerek igen elterjedtek, távközlési protokollok teljesítmény-vizsgálatára alkalmazzák a leggyakrabban (például, hogy egy adott protokoll eléggé hatékony-e), azonban biztonsági vizsgálatok elvégzésére is haszánlhatók ezek a szimulációs eszközök.

A legismertebb hálózati protokoll-szimulációs szoftver az NS2 [3]. Ezzel többek között szolgáltatásbénító, túlterheléses támadásokat is lehet szimulálni.

1.3. Protokoll implementációk vizsgálata

Különböző módszerek és eszközök léteznek a protokollok implementációinak tesztelésére. Minden egyes módszer a tulajdonságok egy jól körülhatárolható osztályára összpontosít. A protokollok megvalósítását ellenőrző szakemberek a *konformanciát és az együttműködési képességet* vizsgáló módszereket alkalmazzák elsősorban. A hálózatüzemeltetők által leggyakrabban alkalmazott eszközök a *protokoll-analizátorok* és a *behatolás-detektáló rendszerek* (Intrusion Detection System – IDS).

A biztonsági ellenőrző szoftvereket a hálózatbiztonsági szakemberek és a rosszindulatú támadók egyaránt használják. Ide sorolhatók a különböző *biztonsági letapogatók (security scanner), forgalom-generátorok* és a *biztonsági réseket kihasználó programok (security exploit).*

Az alábbiakban néhány mondatban bemutatjuk az eddig említett módszereket, valamint alkalmazhatóságukat a protokollok biztonsági réseinek kimutatásában.

Konformancia tesztelés: ezzel az eljárással a protokoll megvalósításának funkcionális helyességét vizsgáljuk. A teszt eredménye megmutatja, hogy az adott implementáció a specifikációnak megfelelően működike. A távközlési ipar által szorgalmazott trend a konformancia vizsgálat és szoftver-keretrendszerének szabványosítása felé mutat. Ennek egyik eredménye a TTCN3 [4]. A biztonsági szempontból fontos hibák egy része kimutatható ezen módszerek segítségével: a specifikáció félreértelmezéséből, programmozási hibákból adódó biztonsági rések nagy része felfedezhető ezzel az eljárással.

Együttműködési képesség vizsgálat: ezek a módszerek a különböző implementációk együttműködési képességét vizsgálják. A vizsgálat eredménye egyedül azt mutatja meg, hogy a két megvalósítás képes-e az együttműködésre. Biztonsági rések felfedezésére nem alkalmas ez a módszer.

Teljesítmény vizsgálat: a teljesítményvizsgálat során az implementáció viselkedését figyelik különböző terhelési feltételek mellett. Fő alkalmazása a különböző implementációk teljesítőképességének és hatékonyságának összehasonlítása, illetve a szűk keresztmetszetek felkutatása. Ennek ellenére egy biztonsági szempontból fontos tulajdonság vizsgálatára is használható: segítségével kimutatható, hogy a protokoll adott esetben érzékeny-e a túlterheléses (Denial of Service – DoS) támadásokra, illetve hogy az ez elleni védekezési módszer megfelelően működik-e.

Protokoll-analizátorok: céljuk, hogy valós időben megfigyeljék a hálózati forgalmat és el őre definiált szabályok szerint analizálják a csomagok tartalmát. Ezek a szabályok tartalmazhatnak protokoll adategységek értelmezésére vonatkozó információkat, így a protokollanalizátor ember által is olvasható formában képes megjeleníteni a csomagokat. A legtöbb protokoll-analizátort a hálózati vagy szoftveres hibák keresésére, illetve forgalmi statisztikák gyűjtésére fejlesztették ki. Közvetlenül nem alkalmazhatók biztonsági tulajdonságok vizsgálatára, azonban alapvető megfigyelő eszközként minden hálózattal foglalkozó szakember használja őket.

Elterjedten használt szoftverek:

`tcpdump` [8], `ethereal`.

Forgalom-elemzők (NIDS): a hálózati forgalomelemzők passzív hálózati eszközök, melyek gyanús tevékenység után kutatva folyamatosan figyelik a hálózati forgalmat. Amennyiben abnormális forgalmi szituációt vagy illetéktelen behatolást detektálnak, riasztják a hálózat üzemeltetőjét, vagy automatikus ellenlépéseket tehetnek. Ezek a rendszerek nem alkalmazhatóak közvetlenül biztonsági vizsgálatra, de az általuk felfedezett incidensek nyomán fény derülhet eddig ismeretlen biztonsági résekre is.

Példa: `snort`.

Biztonsági letapogatók (security scanners): ezek olyan aktív hálózati szoftverek, melyekkel egy adott hálózat vagy végpont sebezhetőségét lehet felmérni. Léteznek rendszer-specifikus és általános letapogatók is. Fő céljuk akár a célhálózat, akár a cél hoszt biztonsági réseinek felfedezése.

Az elterjedt szoftverek: `Nmap` [2], `Nessus` [1].

Forgalom-generátorok: olyan alapvet ő eszközök, melyekkel tetszés szerinti hálózati forgalom generálható. Intelligensebb fogralom-generátorok kiválthatnak egy vagy több kommunikációs felet vagy támadót. Önmagukban nem alkalmazhatóak biztonsági vizsgálatra, azonban a legtöbb biztonsági tesztelő szoftvernek részét képezik.

Biztonsági réseket kihasználó programok: céljuk, hogy ismert biztonsági réseket használjanak ki, általában rossz szándékkal. Elsődlegesen támadók használják őket, de a hálózatbiztonsággal foglalkozók is felhasználhatják azokat egy adott megvalósításban levő biztonsági hiányosság demonstrálására, illetve a megfelelő védekezési módszer kidolgozására. Használatuk csak az adott hiba felderítésére terjed ki.

2. A biztonsági tesztelés egy új megközelítése

Megvizsgálva az eddig kidolgozott biztonsági ellenőrző eljárásokat, arra a megállapításra jutottunk, hogy egy igen fontos terület nincs kellőképpen lefedve. A hálózati támadások egy része a beékelődésre épül, azaz a támadó kettő vagy több jóhiszemű kommunikáló fél közötti adatúton helyezkedik el. A meglévő módszerek általában nem képesek megmutatni az ilyen beékelődéses támadások hatásait, mivel az általuk alkalmazott hagyományos elrendezésben két fél kommunikál: az egyik a tesztelés alatt álló implementáció (IUT – Implementation Under Test), míg a másik maga a teszt eszköz. Ilyen elrendezés esetén a vizsgáló szoftvernek tel-

jes tudással kell rendelkeznie a protokollról, hogy a tesztelés alatt álló implementációval kommunikálhasson.

A valós életben gyakran előfordul, hogy több végpont bonyolít le forgalmat egy olyan hálózaton, mely teljesen, vagy részlegesen a támadó kezében van. Ilyen esetben a támadó megfigyelheti a felek kommunikációját, tetszőlegesen késleltetheti, eldobhatja, módosíthatja csomagjaikat, valamint generálhat tetszése szerinti csomagokat, akár más felhasználó nevében is.

A meglévő módszerekkel nem, vagy csak nehézkesen vizsgálhatók az e fajta támadások. Ezekre a szituációkra dolgoztunk ki egy általános, beékelődésre alapozott módszert. Az általunk alkalmazott vizsgáló elrendezés esetén a teszt szoftver képes végrehajtani ezeket a módosításokat, így vizsgálhatóvá válik az implementációk viselkedése beékel ődéses támadások esetén. A teszt szoftver itt az átviteli hálózat és a támadó szerepét tölti be. A módszer alkalmazásával emulálhatóak a hálózati problémák is (késleltetés, csomagvesztés, bithibák, csomagtöbbszörözés). Az elrendezés előnye, hogy a teszt szoftvernek nem szükséges implementálnia a vizsgálandó protokollt.

A következő pontban bemutatjuk az általunk megvalósított, beékelődéses elrendezésre épűlő biztonsági ellenőrzésre alkalmazható rendszert.

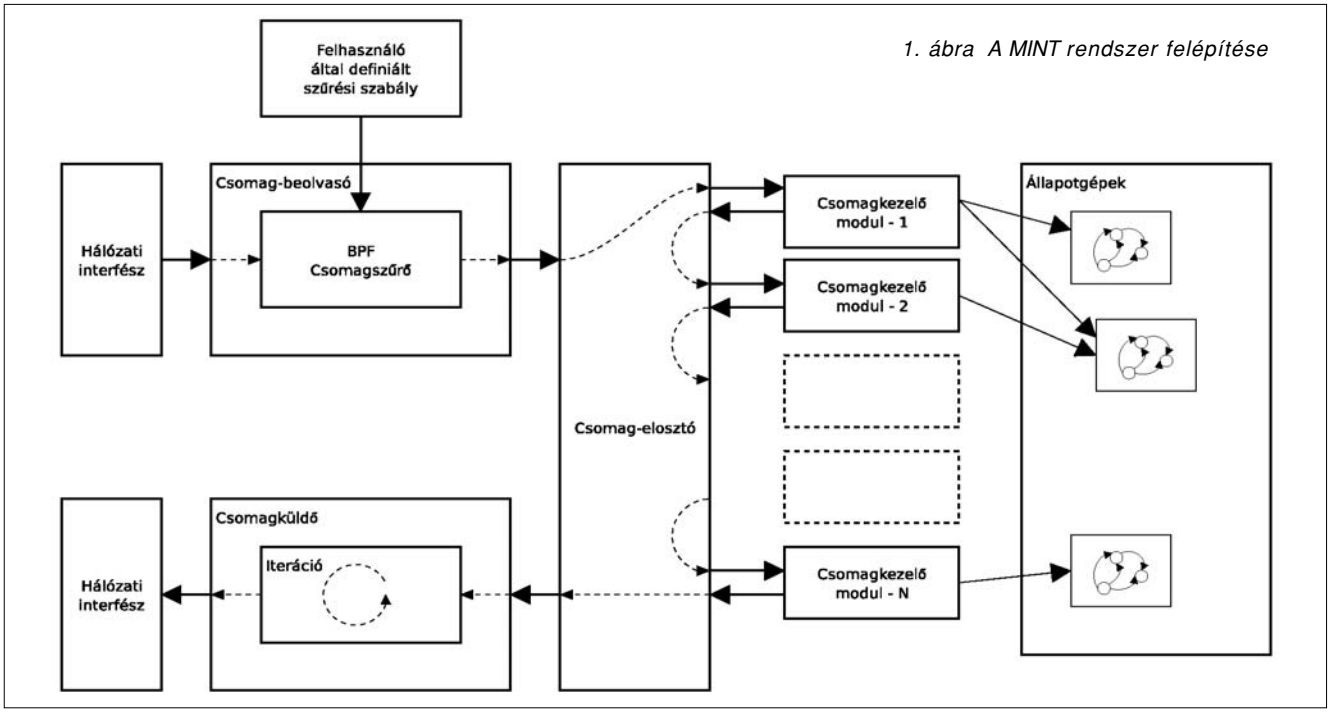
3. Megvalósítás

Fő célunk egy olyan keretrendszer megalkotása volt, mely általánosan alkalmazható hálózati protokollok implementációinak biztonsági teszteléséhez, beékelődéses elrendezésben. A tervezés során az alábbi elvárásokat fogalmaztuk meg a rendszerrel szemben:

- a hálózati csomagok kezelése adatkapcsolati szinten, ezzel a protokollfüggetlenség biztosítása;
- alapvető csomagtovábbító funkciók megvalósítása (útvonalválasztó és kapcsoló funkciók);
- a hálózati csomagok megkülönböztetése a felhasználó által megfogalmazott szabályok szerint;
- moduláris felépítés;
- általános programozási interfész (API) biztosítása és a dinamikus modulok kezelése az egyszerű bővíthetőség érdekében;
- a teszt eszköz felhasználója által betöltött modulok tetszőlegesen módosíthassák a rendszeren keresztülhaladó csomagokat;
- a felhasználó moduljai tetszőlegesen állíthassák egy csomag elküldéseinek számát (hogy emulálható legyen a csomagvesztés és csomagtöbbszörözés);
- a felhasználó küldhessen tetszőlegesen összeállított csomagokat;
- a felhasználó definiálhasson tetszőleges számú állapotgépet, melyeket a rendszer, illetve a felhasználó által generált események vezérelhetnek;
- a felhasználó rendelhessen össze eseménykezelő függvényeket az állapotgépek állapotátmeneteivel, illetve az állapotok belépési/kilépési eseményeivel.

Fejlesztési és futtatási környezetnek a C programozási nyelvet és a Linux operációs rendszert választottuk, a rendszernek a MINT nevet adtuk (MINT – Man-In-themiddle Networking Toolkit).

A rendszer kerneltől független, afelett futó program. A felépítést és működést szemlélteti az *1. ábra*. A MINT csomag-olvasó modulja a hálózati interfészről olvassa be az interfészre érkező csomagokat, majd a felhasználó által definiált szűrési feltételeknek megfelelőket továbbítja a csomageloszto modulnak. A csomag-elosztó sorban meghívja a felhasználó által definiált csomagkezelő modulokat, melyek megvizsgálhatják és tetszés szerint módosíthatják a csomagot. A csomag végül a



1. ábra A MINT rendszer felépítése

csomagküldő modulhoz kerül, mely a kimeneti hálózati interfészen elküldi a csomagot.

A fejlesztést gyorsította, hogy sok funkcióra már létezik jól működő, nyílt forráskódú függvény-könyvtár. Az általunk felhasznált könyvtárak a `libpcap` (hálózati csomagok alacsony szintű olvasása) [8], a `libnet` (hálózati csomagok összeállítása és alacsony szintű elküldése) [12] és a `libconfig` (hierarchikus konfigurációs fájl feldolgozása) [13].

A `libpcap` függvénykönyvtár a kernel hálózati szolgáltatásaitól függetlenül, alacsony szinten képes a hálózaton megjelenő csomagok beolvasására. A csomagok hatékony kezelésében segít a csomagszűrési szolgáltatása. Egy magas szintű, kényelmes leírónyelven megfogalmazott szűrési feltételt (például IP cím illetve TCP port alapú szűrés) képes lefordítani a kernelben található BPF (Berkley Packet Filter) szűrő byte-kódjára. Csak az így beállított szűrési feltételeknek megfelelő csomagokat továbbítja a kernel a programnak, így nem kell a tesztelés szempontjából irreleváns csomagokat kezelni.

Az állapotgépek hatékony megvalósításához nem tal áltunk megfelelő, szabadon felhasználható függvénykönyvtárat, ezért magunk készítettünk egyet. Az állapotgép szoftvermodul a rendszertől független, saját API-val és konfigurációval rendelkezik, így akár más szoftverekben is alkalmazható.

Alapmodulok

Megvalósítottunk néhány alapvető funkciót ellátó csomagmódosító modult:

Minta-modul: egy olyan modul, amely nem tölt be valós csomagkezelési funkciót, azonban prototípusként használható újabb modulok kifejlesztésénél.

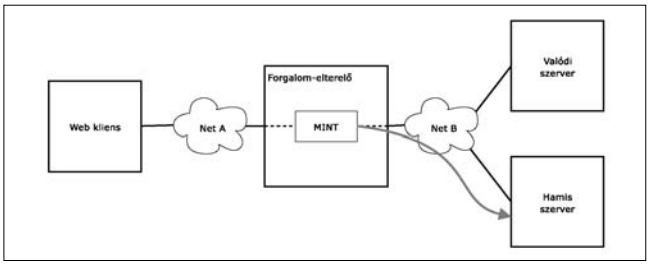
Stochasztikus hiba modul: a felhasználó által megadott hibaaránynak (BER – Bit Error Rate) megfelelően bithibákat illeszt a forgalomba. Használatával vizsgálható a protokollok hibatűrő képessége és így akár bizonyos DoS támadásokra való érzékenysége is.

Ethernet, TCP/IP fejrész-módosító modul: a kapcsoló- és forgalomirányító funkciók megvalósításához szükséges az adatkapcsolati réteg címzésének módosítása. Képes módosítani az Ethernet keretek forrás- és célcímét, az IP csomagok, valamint TCP csomagok fejrészét. Módosítás után újraszámolja a TCP ellenőrzőösszeget.

4. Alkalmazási példa – HTTPS forgalom elterelése

A MINT rendszer alkalmazására bemutatunk egy egyszerű, de tanulságos példát. Tekintsük a webszerverek és böngészők közötti biztonságos kommunikáció protokollját, mely nem más, mint a HTTP az SSL/TLS [7,6] protokoll fölött. Az SSL/TLS protokoll feladata a kommunikáló felek authentikációja és a kommunikáció titkosítása.

A HTTPS kommunikáció az SSL/TLS kézfogással (handshake) kezdődik. A kliens – esetünkben a böngésző – elküldi a ClientHello üzenetet a szervernek. A szerver válaszul ServerHello üzenet mellett elküldi a saját tanusítványát, majd a ServerHelloDone-al zárja a kommunikációt. A kliens, miután ellenőrizte a tanusítványt, előállítja a titkosításhoz szükséges adatokat, majd ennek publikus részét átküldi a szervernek a ClientKeyExchange üzenetben. Ezen kívül ChangeCipherSpec üzenettel jelzi, hogy ő már készen áll a titkosításra. A kommunikációt a kliens zárja a Finished üzenettel. A szerver miután kinyerte a közös, osztott titkot a ClientKeyExchange segítségével, Finished üzenettel válaszol. A handshake után a kliens és a szerver titkosítottan kommunikál. Ez történik például egy internetes banki belépésnél is, ahol a felhasználói név és jelszó már titkosítva kerül átvitelre.

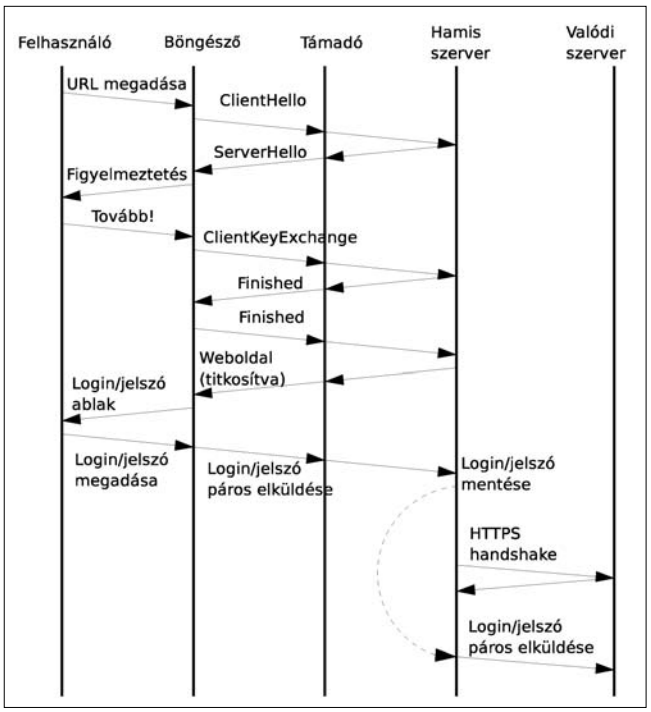


2. ábra HTTPS forgalom elterelése – Teszt topológia

Tesztünk során egy felhasználó a böngészője segítségével egy webszerverrel veszi fel a kapcsolatot. Az alkalmazott HTTPS protokoll authentikációs eljárása ellenére sikerült megtévesztenünk a felhasználót. HTTPS-en való csatlakozáskor a böngésző ellenőrzi az SSL handshake során kapott szerver-tanusítványt, hogy megbizonyosodjon a szerver valódi kiléte felől. Amennyiben az ellenőrzés sikertelen, figyelmezteti a felhasználót, majd megkérdezi, hogy ennek ellenére akarja-e folytatni a kommunikációt. A felhasználók sajnálatos módon figyelmen kívül hagyják ezeket a figyelmeztetéseket (sokszor annak elolvasása nélkül), s így hamis tanusítványokat is könnyen elfogadnak.

A tesztünk során felállítottunk egy hamis webszervert, majd a MINT szoftver segítségével eltereltük felé a HTTPS forgalmat *(2. ábra)*. Ezek alapján láthatjuk, hogy egy támadó, akinek sikerült beékelődnie a felhasználó és a szerver közé, képes a szervert megszemélyesíteni. Ehhez egyszerűen el kell terelnie a felhasználótól a valódi szerver irányába folyó forgalmat egy általa üzemeltetett hamis szerverre. Amennyiben a hamis szerveren a valódinak megfelelő vagy hasonló tartalom van, a támadó nagy valószínűséggel meg tudja téveszteni a felhasználót. Ezután a megtévesztett felhasználó jóhiszeműen megadhat bizalmas információkat, például bankkártyaszámát, jelszavait, melyekkel később a támadó visszaélhet. Egy ilyen támadás üzenetváltásait szemlélteti a *3. ábra (lásd a következő oldalon)*.

Kimutattuk tehát, hogy a TLS protokoll biztonsági szolgáltatásai ellenére a felhasználó gondatlansága miatt beékelődéses támadással célt érhetnek a támadók.



3. ábra Megszemélyesítéses támadás – Üzenetváltások

5. Összegzés

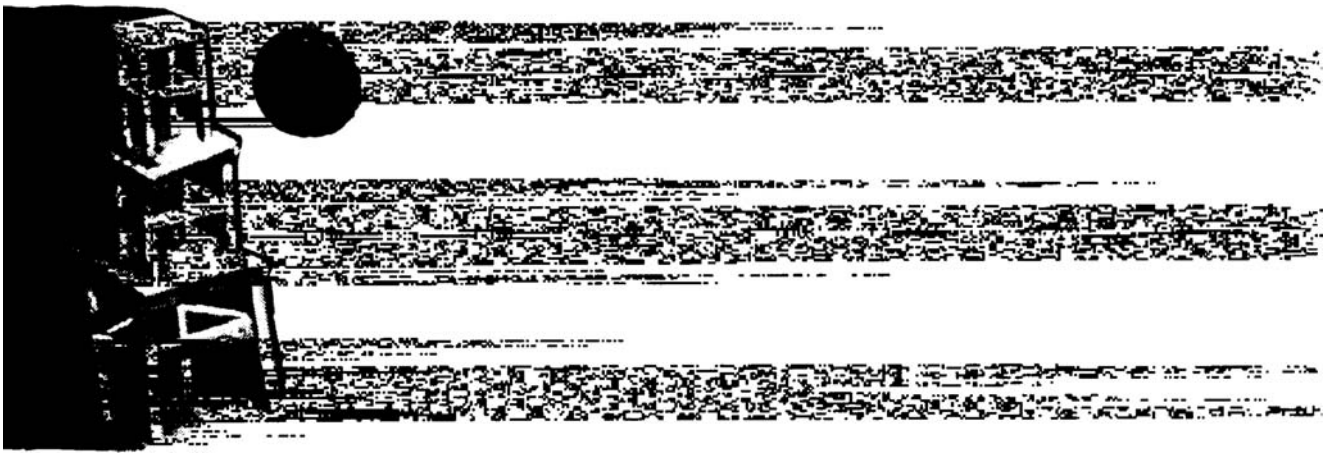
Cikkünkben bemutattunk egy olyan biztonsági vizsgálati módszert, valamint az ezen módszert alkalmazó eszközt, melynek segítségével a tesztelendő rendszerről eldönthetjük, hogy közbeékelődéses támadások esetén is megfelel-e a biztonsági elvárásoknak. Ez az eljárás ezen kívül protokollok biztonsági hibáinak felfedésére is alkalmas.

Protokollok tesztelésénél általában is nagy segítséget nyújthat az általunk megvalósított keretrendszer, mivel ezzel olyan helyzeteket tudunk teremteni, amelyek felszínre hozhatják a protokoll vagy annak megvalósításának általános hibáit. A keretrendszer használatával a fejlesztő a tesztelés szempontjából fontos részletekre koncentrálhat, anélkül, hogy az alacsony szintű csomagkezeléssel vagy állapotgép-reprezentáció megvalósításával kellene foglalkoznia.

A beékelődéses módszer és a keretrendszer gyakorlati alkalmazhatóságát szemléltette a fent bemutatott forgalomelterelési példa is.

Irodalom

[1] Nessus – a remote network security scanner, http://www.nessus.org/
[2] Nmap – Network Security Scanner, http://www.nmap.org/
[3] The Network Simulator – ns-2, http://www.isi.edu/nsnam/ns/
[4] TTCN3 – Methods for Testing and Specification (MTS) The Testing and Test Control Notation version 3, ETSI Document Nr.: ES 201 873-1.
[5] IEEE Standard 802.11, part 11., 1997. Wireless LAN Medium Access Control and Physical Layer Specification.
[6] T. Dierks and C. Allen: The TLS Protocol, 1999. FC 2246, Proposed Standard.
[7] Kocher Frier, Karlton: The SSL 3.0 Protocol, 1996. Internet Draft, Work in Progress.
[8] The Tcpdump Group: `libpcap`: Packet capture library http://www.tcpdump.org/
[9] Gevin Lowe: Casper: A compiler for the analysis of security protocols, Journal of Computer Security, 6:53–84, 1998.
[10] Catherine Meadows: The NRL Protocol Analyzer: An overview, Journal of Logic Programming, 26:113–131, 2. 1996.
[11] A. W. Roscoe: The Theory and Practice of Concurrency, Prentice Hall, 1998.
[12] Mike D. Schiffman: `libnet`: A C library for portable packet creation and injection, http://www.packetfactory.net/libnet
[13] Abraham vd Merwe: `libconfig`: A C library for parsing hierarchical configuration files, http://oasis.frogfoot.net/



Konformancia vizsgálati eszközök forgalom-analizátor vizsgálathoz

CSORBA J. MÁTÉ, PALUGYAI SÁNDOR, DR. MISKOLCZI JÁNOS
Ericsson Magyarország Konformancia Laboratórium
mate.csorba@eth.ericsson.se

Reviewed

Kulcsszavak: megbízhatóság, alkalmazási feltételek, optimalizálás

Az IP alapú hálózatok korábban elképzelhetetlen méretekben jelennek mindennapjainkban. Ezzel egyidejűleg a hang, videó és egyéb, ez idáig dedikált hálózatokat használó adatok is egyre inkább az Internet Protokollt alkalmazzák. Mindennek következtében lényeges a hálózatok minőségi paramétereinek állandó figyelemmel kísérése. Hálózati eszközök és komplex távközlési rendszerek fejlesztése közben elengedhetetlen a hálózat teljesítményének, a szolgáltatások minőségének folyamatos nyomon követése. E mellett a hálózatok üzemeltetése, karbantartása és az üzemzavarok gyors elhárítása is igényli a forgalom üzem közbeni megfigyelését. Erre a problémára kívánnak megoldást nyújtani a hálózati forgalom-analizátorok.

1. Előszó

A protokollok szabványhoz való hűségének, vagyis konformanciájának vizsgálatára alkalmazott módszerek korábban nem tették lehetővé hálózati forgalom megfigyelésére kifejlesztett, illetve még fejlesztés alatt álló eszközök vizsgálatát. A kidolgozott módszerrel, az alapvetően konformancia vizsgálatra használt TTCN *(Testing and Test Control Notation)* tesztkörnyezettel lehetővé válik a forgalom-analizátor szoftver működésének ellenőrzése.

Az általunk elkészített rutinok lehetővé teszik az analizátor automatizált és központosított tesztelését. A kész tesztkészlet a vizsgálati módszer moduláris felépítése miatt egyszerűen átalakítható és alkalmazható más forgalom-analizátor megoldások vizsgálatára is.

2. Hálózati forgalom-analizátorok

A hálózati forgalom-analizátor általánosságban a hálózati forgalmat megfigyelő olyan egység, amely egyúttal rekonstruálja és értelmezi a protokollok üzeneteit, azokat is, melyeket alacsonyabb szinten esetleg több csomagban szállíthatunk. A forgalom-analizátorok ősének a korai hálózatfelderítő-alkalmazásokat tekinthetjük, amelyek ICMP üzenetek periodikus küldésével végezték a hálózat topológiájának felderítését, majd az így kapott eredményt ábrázolták valamilyen grafikus formában. A legkorábbi megvalósítások a robusztusságukól híres VAX/VMS rendszereken jelentek meg. Napjainkban a hálózat-felügyeletben nagy szerepet kap a felhasználók aktivitásának megfigyelése, a túlterhelések és az illegális használat megakadályozása, valamint az illetéktelen behatolók felfedése *(intrusion detection)* is.

Egy hálózati menedzsment rendszer több, a vezérlést és a menedzsmentet megvalósító komponensből áll. Általában tartozik hozzá egy, a hálózat felépítését megjelenítő grafikus elem, valamint egy valós idejű megfigyelő és jelentéskészítő eszköz. A legfontosabb funkciói közé tartoznak a konfigurálás, a hibakezelés, a teljesítményt befolyásoló, valamint biztonsági beállítások. Ezen kívül általában rendelkezik valamilyen hálózattervezést segítő eszközzel is.

A forgalom megjeleníthető valós időben vagy utólag, esetleg hisztogram formájában. A hisztogramok rajzolása a leggyakrabban a TCP, UDP csatlakozási pontok (rendszer port) figyelésén alapszik, esetleg külön kitérve az ICMP üzenetek különböző típusaira. A megjelenítés kiterjedhet például adott protokollra vonatkozó meghibásodási százalékra, míg a megjelenítendő információ általában lehet bájt vagy csomag alapú. A hirdetési, valamint csoportcímű *(broadcast, multicast)* csomagok és az elveszett csomagok becsült száma is fontos paraméter. A hibás csomagok esetében elemzésre kerülhet a hiba oka, úgy mint CRC ellenőrző-kód hibák száma, csonkolt csomagok, túlméretezett csomagok, ütközések és a helyes sorrendben bekövetkező hibák száma.

A megfigyelés időtartamának megválasztása is körültekintést igényel. A túl hosszú megfigyelési időtartam képes kiátlagolni bizonyos működési rendellenességeket, így ez feltétlenül kerülendő. Általános esetben az egy órás ciklusok megfelelőek [1]. A kihasználtság és a késleltetés változása feltétlenül nyomon követendő. Hirtelen kiugró értékek általában egy kezdődő hálózati probléma jelei lehetnek, ilyen baljós jelenség lehet a csomagvesztés és a vonali hibák megnövekedése, a késleltetés hullámzása vagy a megszaporodott útválasztási forgalom.

A terhelési profil mérés a hálózat hosszú távú megfigyelését igényli. A hálózat felügyeletét végzők segítségével képet alkothatnak nemcsak az egyes végpontok a hálózatra gyakorolt hatásról, hanem arról is, hogy az egyes felhasználói programok a terhelés hány százalékát okozzák, és ez a terhelés hogyan oszlik el egy hosszabb időintervallum alatt. Hasznos lehet nyomon követni, például az Ethernet vagy más technológián alapuló hálózat kihasználtságának átlag- és csúcsértékét

is. A legtöbb esetben ezeket a paramétereket, vagy egyéb hibajelenségeket figyelő automatikus riasztások beállítása is lehetséges.

A forgalom-analizátorok döntő többsége a valós idejű adatokat az Ethernet kártya *promiscuous* üzemmódba kapcsolásával a helyi hálózatból nyeri. Ebben az üzemmódban a kártya gyakorlatilag megkerüli az Ethernet-címzést, ugyanis beolvassa az összes csomagot a hálózatról, nemcsak a közvetlenül neki címzetteket. Annak érdekében, hogy ez működhessen és megfelelő sebességet produkáljon, általában előre le kell foglalni egy bizonyos részt a memóriából a pufferelés számára.

Az Ethernet-kártya mindent beolvasó üzemmódba kapcsolása a forgalom-analizátort futtató gép működését némiképp lassíthatja, főleg abban az esetben, ha egy általános célú számítógépről van szó és nem egy céleszközről. Egy átlagos PC-s hálózati kártya a teljes mértékben leterhelt hálózatról nem képes minden csomagot beolvasni. Különösen ez a helyzet, ha a csomagok követési ideje rendkívül kicsi *(back-to-back bursts)* [2].

A feldolgozási időt természetesen nagyban befolyásolhatja a megfigyelni kívánt forgalom nagysága. Így megkülönböztetésre szorulnak a valós idejű forgalmat analizáló, illetve a késleltetett *(off-line)* feldolgozást végző eszközök. Létezik különálló, speciális kártyát használó megoldás is forgalom-analizátorra *(EtherMeter)*, bár ez napjainkban már nem túl elterjedt megoldás.

Egy protokoll analizátor segítségével a felhasználó számára lehetővé válik a hálózaton keresztül haladó csomag vizsgálata forrás- és célcím, protokoll, alkalmazás, bitminta, csomagméret s egyéb logikai változó alapján. A legtöbb esetben állítható az analizátor működéséhez szükséges néhány paraméter, például a puffertár mérete vagy a csomagok felszabdalásának lehetősége a jobb memória-kihasználás érdekében. Általában a csomagok megjelenítése során is választhatunk a logikai és a hexadecimális nézet között (például a jól ismert *EtheReal* esetében [3]). Néhány szoftver esetében a hibakeresést támogató külön modulokat is használhatunk, és a csomagok vizsgálatához szűrőket is alkalmazhatunk. Ezekkel kapcsolatban fontos, hogy azok alkalmazhatók-e a valós időben megfigyelt hálózati forgalomra, vagy csak egy előre rögzített adathalmazra.

Az analizátor szoftvereket megkülönböztethetjük abból a szempontból is, hogy a protokoll-rétegeket milyen mélységig képesek dekódolni. Esetleg mind a hét réteget vizsgálhatjuk a segítségükkel, vagy csak egy bizonyos részét. Létezik olyan megvalósítás is, melynek a képességeit a felhasználó is bővítheti a saját maga által írt protokollértelmező modulokkal (kitűnő példa erre a lengyel fejlesztésű *ANASIL* elnevezésű analizátor [4]).

A hálózati forgalom bináris tároláskor fontos a nagypontosságú időbélyegek alkalmazása a rekonstruálhatósághoz, kiváltképp fontos ez hosszú időtartamokat átölelő megfigyeléseknél, ahol a hálózat monitorozása akár több mint 24 órán keresztül is folyhat.

Hasznos lehet az összegyűjtött adathalmaz hordozhatósága, hogy a megfigyelés során összegyűjtött adatokat egy általános táblázat- és/vagy adatbázis-kezelővel, esetleg grafikonszerkesztővel is meg lehessen jeleníteni.

3. A Moniq forgalom-analizátor

3.1. Általános tulajdonságok

Vizsgálatunk tárgyát az Ericsson által fejlesztett, Moniq nevű szoftver képezte, amely egy professzionális, passzív hálózat-analizátor. A forgalmat az IP réteg szintjén vizsgálja, elsősorban a csomagkapcsolt mobil hálózatok szolgáltatásainak minőségét biztosítandó. A fejlesztésekor a mobil adathálózatok intelligens, végponttól-végpontig terjedő teljesítmény menedzselését kívánták megoldani, mivel a mobil hálózatok (GPRS, UMTS) minőségbiztosítása és felügyelete sürgető probléma.

A Moniq használata nem igényel speciális hardvert, akár egy közönséges PC-re telepítve csatlakoztatható a megfigyelni kívánt hálózathoz. A szoftver architektúrája lehetővé teszi a TCP/IP struktúra elemzését statisztikus alapokon. Nagysebességű gerinchálózatok vizsgálatára is alkalmazható. Lehetőség van Gigabites sebességtartományban működő hálózatok megfigyelésére is megfelelő hardver csatlakoztatásával.

A statisztikák létrehozásakor az elsődleges szempont, hogy minél teljesebb képet lehessen kapni a végfelhasználó által érzékelt szolgáltatás-minőségről. Az analizátor számos protokoll üzeneteit képes felismerni és feldolgozni, ide értve a következőket: TCP, UDP, ICMP, DNS, RTP, HTTP, FTP, Telnet, SMTP, POP3, IMAP4, WAP, RADIUS. A statisztikák egyrészt lefedik a hálózat teljesítmény-mutatóit, másrészt a felhasználói szint is megfigyelhető és kiértékelhető. A statisztikákat készítő és analizáló képességek köre folyamatosan bővül, ahogy a fejlesztés halad.

A végponttól-végpontig kitétel ebben az esetben a mobil-terminál és a kiszolgáló közti útvonalat jelenti, vagyis a szolgáltatás-minőséget itt a felhasználó szempontjából elemzi a szoftver. Működése passzív, a méréshez külön forgalmat nem hoz létre, csupán a hálózatot használó előfizetők adatátvitelére koncentrál.

A létrehozott statisztikák finomsága változtatható, akár a csomagszintig. A kapott adatok alapján következtethetünk a forgalom összetételére, és elemezhetjük a hálózatban kialakuló tendenciákat. Felhasználói szintű problémák megoldására szűkíthető a megfigyelt tartomány. Megfigyelési pont több helyen is létesíthető, miközben a statisztikai adatbázist egy helyen tárolják, így könnyen elérhető, és a hálózat teljesítménye, valamint a tendenciák nyomon követhetők. Ezzel a módszerrel megfigyelhető például egy nagy léptékű átkonfigurálás hatása a hálózatra.

3.2. A szoftver felépítése

A szoftver igazi erőssége a hálózat teljesítménymutatóinak teljes körű felmérésében, az ok-okozati összefüggések felderítésében, a hálózat tervezés, üzemel-

tetés támogatásában rejlik. Ehhez többféle statisztikát készít, példaképpen említve néhányat: a forgalom eloszlása protokollok szerint, hálózati elakadást jelző üzenetek (pl. *ICMP unreachable)* aránya, tranzakciók száma és időbeli eloszlása, csomagok méretének eloszlása és így tovább.

Az alkalmazás moduláris jellegéből adódóan több részből épül fel. A legfontosabbnak tekinthető részek a következők voltak:

- *Moniqdump* – a forgalom rögzítéséhez;
- *Moniqparse* – a csomagok elemzéséhez;
- *ReadBin* – az eredmények ember által olvasható formába öntéséhez.

A működés első lépcsőjeként létrejön az úgynevezett forgalom *(trace)* állomány, amely tartalmazza a megfigyelés alatt a hálózaton áthaladt csomagokat. Ennek az állománynak több megjelenési formáját is alkalmazhatjuk. A legegyszerűbb, ha a Unix alapú operációs rendszerek részét képező *tcpdump* programot használva készítjük el ezt az állományt. Ennél kifinomultabb megoldást jelent a szoftver részét képező *Moniqdump* program használata, amely a forgalom állomány elkészítése közben titkosítja az előfizetői adatokat és belső IP címeket, úgy, hogy ez az adatok későbbi feldolgozását nem befolyásolja. A *Moniqdump* bemenete lehet a működő hálózat, de képes egy előre elkészített forgalom állományt is átalakítani. Annak érdekében, hogy egy hosszabb megfigyelést követően is kezelhető maradjon az állomány mérete, a csomagok fejrészét követő adattartalom tetszőleges mértékben leválasztható, azaz nem szükséges teljes csomagokat eltárolni, a későbbi kiértékelést ez nem befolyásolja. Az adattartalom leválasztásának helye azért kell, hogy változtatható legyen, mivel különböző protokollok, bizonyos esetekben további hosszú fejléceket helyezhetnek el a hálózati réteg adatait követően. (Kitűnő példa erre a WAP protokoll, mely az UDP fejléc után következő adatrészbe helyezi el fejléc-információit, időnként a többi IP protokolltól eltérően rendkívül hosszan.)

A tárolt forgalmat feldolgozható formába a *Moniqparse* program alakítja, melynek a kimenete több bináris napló állomány. Tartalmuk röviden:

- Státusz állomány;
  Valós idejű mérésnél a mérésre vonatkozó adatokat tárolja, mint például időbélyegek, aktuális időbeli felbontás.
- Rövid távú globális statisztika;
  Tartalma a halmozódó forgalmi adatok kis részletességgel és nagy időléptékben.
- Hosszú távú globális statisztika;
  Ebben az állományban nagyon részletesen, de kis időbeli felbontással tárolódnak az adatok.
- Tranzakciók naplója;
  Minden kliens-szerver közti adatátvitelt tartalmaz. Új bejegyzés akkor kerül bele, amikor egy tranzakció lezárul.
- Felhasználói kapcsolatokat tároló napló állomány;
  Bejegyzést tartalmaz minden lezárult felhasználói kapcsolatról.
- Egy perces felhasználói kapcsolat napló;
  A felhasználók által érzékelt átviteli kapacitás becslésére szolgáló statisztikákat tartalmaz.
- Tranzakció számláló napló állomány;
  Tartalma az egy időegységre eső tranzakciók száma.
- Felhasználói kapcsolatokat számláló állomány;
  Hasonlóan az előző állományhoz, az időegységre eső kapcsolatok számát naplózza.

A *Moniqparse* által előállított állományokból program modulok segítségével kinyert különböző statisztikák jeleníthetők meg egy kliens-szerver kapcsolaton keresztül. A felhasználó gépén futó grafikus felhasználói felületen (GUI) láthatók a különböző statisztikai elemzések eredményei. (A grafikus felületen keresztüli felhasználást a továbbiakban nem részletezzük, mivel annak tesztelése nem tartozott a feladataink közé.)

Az adatok kinyerésének másik módja a *ReadBin* program használata, melynek segítségével a bináris állományokból lekérdezéseket hajthatunk végre, amelyek eredményét szöveges kimenetként kapjuk. A program kimenetét parancssori kapcsolók használatával formálhatjuk. Így lehetséges szűrési feltételek beállítása, valamint azt is szabályozhatjuk, hogy az adatbázis mely mezőire vagyunk kíváncsiak.

4. A TTCN-3 nyelv

A TTCN-3 egy konformancia vizsgálatokra általánosan használt, magasszintű programozási nyelv (valójában nincs korlátozva kizárólag konformancia tesztelésre). Vizsgálható a segítségével együttműködési képesség, robosztusság, végezhető rendszer- és integrált teszt. A nyelv általában tesztelési metódusoktól és protokolloktól független tesztkészletek specifikálására hivatott. Mindezen tulajdonságok mellett alkalmas távvezérelt tesztek lebonyolítására is, amelyekben az IUT irányítása is TTCN program segítségével történik. A felhasználás más egyéb jellemző területei: a szolgáltatások tesztelése, CORBA alapú platformok, API-k tesztelése [5].

A TTCN-3 fordító protokoll független C++ forráskódot generál. Vagyis szükség van valamilyen kiegészítésre, ami megteremti a kapcsolatot a végrehajtható tesztkészlet és a tesztelendő között. Ez a tesztport, ami egy C++ nyelven írt szoftver-könyvtár. A teszt-csatoló rutin (tesztport) egy adott protokoll üzeneteinek, csomagjainak kezeléséhez szükséges, így egy adott protokoll minden verziójához külön meg kell írni. Ehhez nyújt némi segítséget, hogy a TTCN-3 fordító segítségével elő lehet állítani a tesztport alapját képező, C++ sablont, amely definiálja a szükséges függvényeket, azonban a végleges kódot a felhasználónak kell megírnia. A tesztport gyakorlatilag egy végtelen FIFO sorral modellezhető, amely egész addig tárolja a beérkező üzeneteket, míg a TTCN komponens, melyhez tartozik, ki nem olvassa azokat. Természetesen egy TTCN komponens több tesztport felett is rendelkezhet, ezt a tesztkörnyezet ki is használja [6].

A hálózatba kapcsolt tesztelést végző számítógépek futtatás alatti viselkedése tesztesetek (*Test Case*) formájában kerül kifejezésre. A nyelv hatékonyan tudja kezelni a különböző viselkedési alternatívákat, úgy, mint különböző adatok fogadása a tesztportokon keresztül, időzítő események bekövetkezése stb. A tesztesetekben kerül sor az eredményt jelentő ítéletek meghozatalára, ezek mellett a sokszor rendkívül hasznos naplóállomány készítésre is lehetőség van.

5. A Moniq vizsgálata

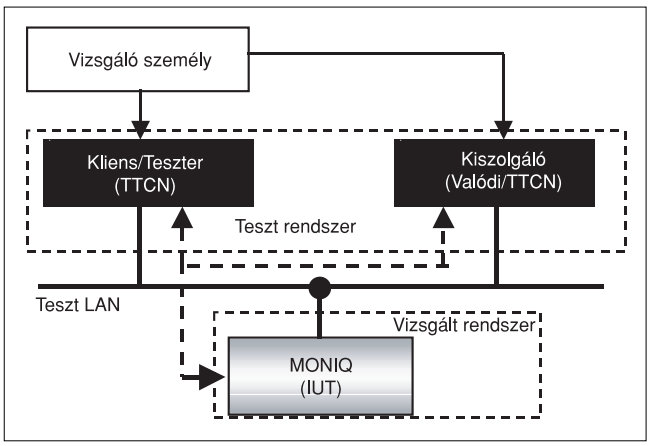
A Moniq vizsgálatához a konformancia vizsgálatok körében hagyományosnak tekinthető távoli tesztelési elrendezést alkalmaztuk, némileg módosítva azt. A teszter oldal a konformancia vizsgálati elrendezéseknek megfelelően mindig egy TTCN nyelvű program volt. Azonban a vizsgált rendszer oldalán a legtöbbször szintén egy TTCN komponens állt vagy pedig egy valódi kiszolgáló szoftver, míg az IUT a forgalom szempontjából passzív hálózati analizátor volt *(1. ábra)*.

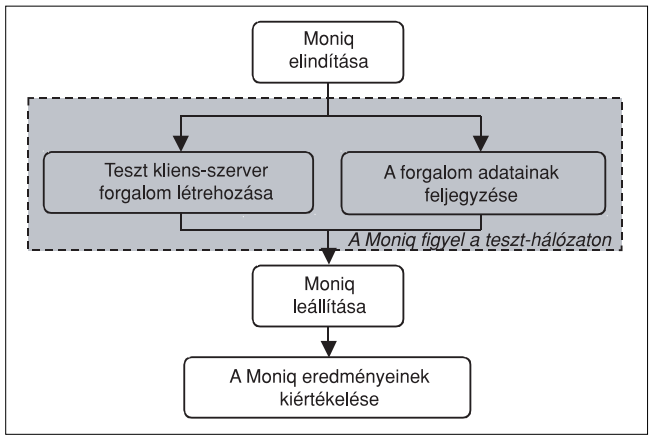
A kliens és a kiszolgáló megvalósítása nagyban hasonlít egy konformancia teszt kifejlesztéséhez, mivel a közöttük lejátszódó kommunikációt a vonatkozó ajánlások (RFC-k) alapján kell elkészíteni. Mindemellett szükség van az ajánlástól eltérő, hibás vizsgálati sorozatok előállítására is (hasonlóan a konformancia vizsgálatokhoz).

A szimulációra a kiszolgáló TTCN segítségével azért volt szükség, mert helyes és helytelen vizsgálati sorozatokat egyaránt elő kellett állítani (mivel az IUT-nek mindkét esetben helyes analízissel kell szolgálnia). A fentiekből látható, hogy itt egy speciális konformancia vizsgálati módszerrel állunk szemben: a teszter úgy viselkedik, mintha a kiszolgálót vizsgálná helyes és helytelen üzenetekkel, s ez alatt a Moniq által szolgáltatott forgalmi adatokat ellenőrzi.

A cél egy olyan minősítő rendszer kialakítása volt, amely a valódi használat körülményeit szimulálva, automatizáltan teszi lehetővé a Moniq legfontosabb moduljainak (*Moniqdump, Moniqparse, ReadBin*) ellenőrzését. A vizsgálat megvalósításakor tehát alapvetően két funkciót kellett megkülönböztetnünk egymástól. Egyrészt ki kellett alakítanunk egy környezetet, melynek segítségével a Moniq automatikusan vezérelhetővé vált, mintha egy operátor ténylegesen használná [7]. Másrészt létre kellett hoznunk egy speciális forgalmat a hálózaton, amely a szabványoknak megfelelően szimulálta a vizsgált protokoll működését. Ezek után rendelkezésünkre állt egy jól definiált forgalom egy szeparált hálózaton, tehát a tesztek befejező lépése a kiértékelés kellett legyen.

1. ábra A tesztrendszer és az IUT viszonya





2. ábra A tesztprogram működése

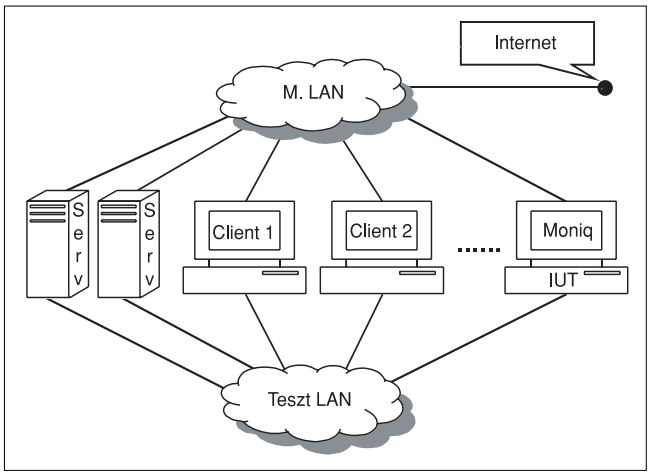
A kiértékelés során annak tudatában, hogy mi zajlott le a hálózaton, meg kellett nézni, hogy a Moniq helyesen értékelte-e a hálózaton történteket. Ezeket a lépéseket láthatjuk a *2. ábrán,* amely magába foglalja a Moniq elindítását a tesztforgalom elemzéséhez, a Moniq leállítását, a mért eredmények tárolását, illetve annak kiértékelését, valamint a mérés folyamatáról egy dátummal és a Moniq-ra vonatkozó azonosító információkkal rendelkező adatállomány előállítását.

A teszteket tesztcélok formájában dokumentáltuk, szabványos alakban megadva a teszt nevét, egy rövid leírást, utalva az adatbázis mezejére, amit vizsgálunk és egy bővebb leírást a működésről. A dokumentálást elősegítendő minden egyes teszt futása után három állományt tárol a tesztrendszer: egyrészt a TTCN program futásakor keletkező naplót (amely a mérés során bekövetkező összes eseményről tartalmaz bejegyzést), másrészt a Moniq által felvett, hálózati forgalmat tároló bináris állományt, valamint a Moniq szöveges kimenetét.

6. A rendszer vizsgálata

6.1. Vizsgálati környezet

A forgalom-analizátor vizsgálatának alapját a támogatott protokollok működésének szimulációja képezte. Mivel a vizsgált protokollok működése kliens-kiszolgáló elrendezésben folyik, ki kellett alakítani néhány kiszolgálót és a felhasználói oldalt szimuláló kliens gépeket. Az első lépés tehát a vizsgáló hálózat kiépítése, majd azt követően a megfelelő szoftverek telepítése.



3. ábra A teszthálózat

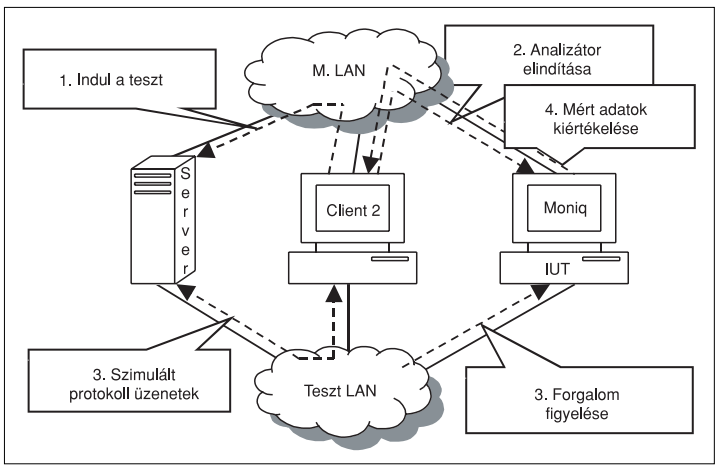
Az *3. ábrán* láthatóan két alhálózatot alakítottunk ki, melyek egymástól elkülönítve működtek. Szükség volt egy könnyen kézben tartható forgalmú ellenőrző-alhálózatra, melyen minden automatikus és/vagy felesleges kommunikációt letiltottunk, hogy kizárólag a tesztek által előállított csomagok használhassák.

A második, menedzsment hálózat *(M. LAN)* a tesztek működéséhez szükséges vezérlő üzenetek és a munkához szükséges egyéb forgalom lebonyolítására szolgált. A Moniqot vezérlése teljes egészében a hálózaton keresztül történt, vagyis tulajdonképpen a Moniq-ot kezelő felhasználó parancsait is egy TTCN programrészlet valósította meg.

6.2. A Moniq forgalom-analizátor vizsgálata

Méréseink megvalósítása a rendelkezésre álló hálózaton a *4. ábrán* látható. A példában a teszt(ek) futásának koordinálását és kiértékelését a *Client2* névvel jelzett gép végzi. A teszt indításakor jelez a kiszolgáló oldalt megvalósító *Server2* gépnek, majd elindítja a vizsgált forgalom-analizátort. Ezt követően az IUT már folyamatosan monitorozza a *Teszt LAN*-t, miközben a vizsgáló program elkezd egy adott protokollnak megfelelően kommunikálni a kiszolgálóval (például végrehajt egy FTP letöltést vagy egy levélküldést az SMTP protokollnak megfelelően). Fontos, hogy minden vezérlési információ az elkülönített menedzsment hálózaton bonyolódik, így a forgalom-analizátor ezeket a csomagokat nem érzékeli. Amikor a kívánt működés szimulációja véget ér, az IUT által mért adatok begyűjtése és kiértékelése szintén automatikusan történik, ismét az *M. LAN* igénybevételével.

4. ábra A Moniq tesztelési lépéseinek megvalósítása



6.3. Kommunikáció a csatlakozási pontokon keresztül

A TTCN-3 kódnak szüksége van egy C++ nyelven írt csatoló rutinra (port-ra), amely lehetővé teszi számára a kommunikációt a vizsgálandó objektummal. A mérési elrendezésünkben három különböző típusú csatoló rutin fordult elő.

A STORE csatoló rutin

Szükség volt először is egy speciális csatoló rutinra a mért adatok átmeneti tárolásához és kiértékeléséhez. Ez a csatoló rutin a *STORE_Port* nevet kapta. A feladatai közé tartozott a Moniq által mért adatok és a számított, tehát az elvileg helyes adatok adatbázisszerű tárolása egy-egy teszteset futása során. A csatoló rutin ezt az igen egyszerű adatbázist a memóriában tárolta, tehát az csak a teszt futása során volt hozzáférhető, ami elegendő is volt, hiszen csupán a tesztek kiértékelésénél volt rá szükség. Az adatbázis felépítése az *1. táblázatban* látható.

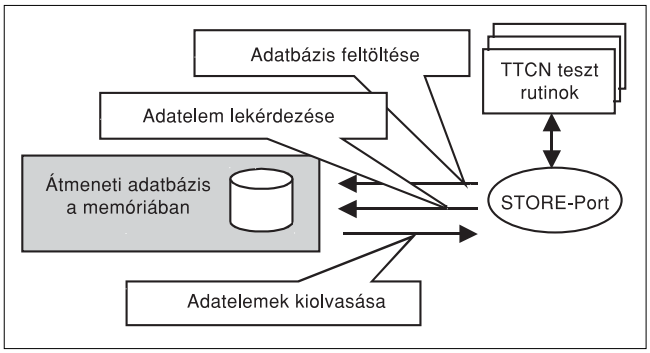
Mező neve	Tartalma
SType	Napló állomány típusa
TNO	Tranzakció sorszáma
Name	Vizsgált adatbázis mező neve
Data	A tesztelt mező várt értéke
MoniqData	A mező Moniq által mért értéke

1. táblázat A mérés kiértékeléséhez használt adatbázis rekordjainak felépítése

A csatoló rutinon keresztül ugyanúgy lehetséges volt az üzenetküldés és -fogadás, mint egy hagyományos kommunikációs ponton keresztül. Azzal a különbséggel, hogy az üzenetek nem a hálózatra kerültek ki, hanem a memóriában található adatbázissal lehetett kommunikálni a csatlakozáson keresztül. Az adatbázis elemeinek három lehetséges típusa volt:

- egész szám, különböző adatok, például csomagok számlálására;
- lebegőpontos szám, jellegzetesen idő (másodperc alapú) mérésére;
- szöveg, általában státuszinformációk tárolására.

Egy adat lekérése tehát a következő információk megadásával volt lehetséges: tranzakció sorszáma (TNO), ezzel például egy TCP kapcsolatot lehetett kiválasztani a monitor által felvett több kapcsolat közül. Egy kapcsolathoz azonban az analizátor több napló állományt is készíthe-



5. ábra A STORE-port működése

tett, tehát ki kell választani az adott kapcsolathoz tartozó, a számunkra érdekes mezőt tároló naplót (*SType*). Valamint természetesen meg kell adnunk, hogy név szerint mely mezőre vagyunk kíváncsiak (Name). A lekérdezés eredményeként a *STORE_Port* két értéket ad vissza: a tesztprogram által helyesnek ítélt *Data* mezőt és a Moniq által mért *(Moniqdata)* értéket. Ezt a két értéket ezek után könnyedén össze lehet hasonlítani.

A Telnet csatoló rutin

Ez a rutin (port) több helyen is rendkívül fontos szerepet tölt be. Az általunk írt TTCN függvény-gyűjtemény e kommunikációs port használatával csatlakozik a forgalom-analizátort futtató számítógéphez, és szabványos Telnet kapcsolaton keresztül, egy valódi felhasználót szimulálva parancsokat ad ki a gépnek, és értelmezi a válaszokat.

A másik fontos felhasználása a vizsgáló sorozatok előállításában, vagyis a protokollok működésének szimulálásában volt. Tekintve, hogy a POP3, IMAP és SMTP protokollok nem alkalmaznak külön saját csomagformátumot, hanem egy TCP kapcsolat felett, karakteres alapon működnek.

A TCP csatoló rutin

A Telnet port-nál is alkalmazott stream-csatoló *(stream socket)* egy alternatívája az úgynevezett datagram-csatoló *(datagram socket)*, amely UDP kapcsolatok létrehozására használható, vagyis nem megbízható és nem kapcsolat-orientált átvitelre.

Bizonyos teszteknél azonban nem alkalmazható sem a *stream*, sem a *datagram* csatoló *(socket)*. Ezekben az esetekben a forgalom előállításakor az alacsonyabb rétegben lévő protokollokat is befolyásolni szeretnénk. Erre például akkor lehet szükség, amikor olyan üzeneteket szeretnénk előállítani, amelyeket a rendelkezésre álló kiszolgáló szoftverből csak nehezen vagy egyáltalán nem tudunk kisajtolni.

Egy konkrét példát említve: szükség volt a tesztelés során olyan tesztesetre, mely különböző működési fázisokba juttatja az IMAP kiszolgálót, és megvizsgálja, hogy a Moniq megfelelően ismeri-e fel a kiszolgáló állapotát. Azt az állapotot azonban, amikor az IMAP kiszolgáló már nem tud több kapcsolatot fogadni, mert telített, és emiatt rögtön a TCP kapcsolat felépítése után visszautasítja a klienst, a rendelkezésre álló erőforrásokkal nehéz lett volna megvalósítani. A megoldást az jelentette, hogy a protokoll működését alacsonyabb szinten kellett modellezni.

Valamint nem lehetett használni a valódi kiszolgáló szoftvert, így a működését egy TTCN programmal kellett szimulálni. Ezen tényezők miatt szükség volt az úgynevezett *raw socket* használatára, az ezt használó port pedig a TCP port nevet kapta. A tesztek között voltak olyan alacsony szintű mérések is, mint például egy adott protokollhoz tartozó átvitt bájtok összege vagy csomagok száma, amelyekhez elkerülhetetlenül egy alacsonyabb szinten dolgozó port-ot kellett használni.

A raw-csatolót *(raw socket-et)* használó kommunikációs port esetében a teljes csomag összeállításáról nekünk kell gondoskodni, vagyis minden protokoll-rétegre a fizikai réteg felett oda kell figyelni. Tehát ezeknél a teszteknél egy csomag a következőképpen nézett ki: <Ethernet fejrész> <IP fejrész> <TCP fejrész> <TCP adatrész>. A *raw socket* használatának hátránya, hogy az így modellezett kapcsolatok esetében a szállítási protokoll működését is teljes egészében meg kell valósítani TTCN-ből, kezdve a kapcsolat-felépítéstől a bezárásáig, a TCP szabványnak megfelelően.

6.4. A Moniq tesztelését végző TTCN rutinok

A Moniq szoftver vezérlése és méréseinek kiértékelése egységesen történt. A Moniq-ot kezelő segédfüggvényeken kívül a legfőbb funkciókat a következő négy elem tartalmazta.

A moniq_start függvény

A függvény meghívása után bejelentkezik a tesztgépről az IUT-re (Moniq) és ellenőrzi, hogy fut-e a vizsgált forgalom-analizátor valamelyik részegysége. Erre azért van szükség, mivel a szoftver ellenőrzését egyszerre többen is végezhetik, ugyanezt a függvénykönyvtárat *(MoniqFunctions)* használva. Azonban a mérések tisztaságának érdekében a *moniq_start* függvény egyszerre csak egy virtuális felhasználót engedélyez az IUT-n. Abban az esetben, ha már valaki más is használja a forgalom-analizátort, a teszt futása félbeszakad.

Amint a szükséges erőforrások rendelkezésre állnak, a függvény elindítja a hálózat monitorozását végző *moniqdump* programot, de hibakereséshez segítségül tudja hívni egyúttal a Linux disztribúció részét képező *tcpdump* programot is.

A moniq_end függvény

A *moniq_end* függvény meghívására akkor kerülhet sor, ha a vizsgáló sorozatot már kiküldtük a hálózatra, vagyis a forgalom-analizátornak már nem szükséges figyelnie a hálózatot. Ekkor a függvény leállítja Telnet kapcsolaton keresztül a monitorozást, és meghívja a csomagok elemzését végző *moniqparse* programot, figyelembe véve a felhasználó által használt konfigurációs állományt.

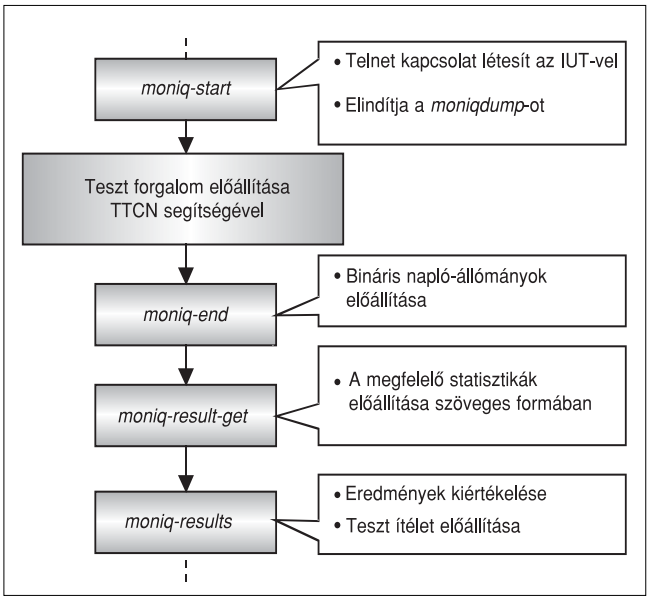
A moniq_result_get függvény

Ez a komponens a *ReadBin* program meghívásával teszi lehetővé a *moniqparse* segítségével létrehozott bináris napló állományok átalakítását. Természetesen ebben az esetben is a tesztelést végző pontosan beállíthatja a *ReadBin* program paramétereit. Az átalakítás eredményeként előálló szöveges kimenetet a függvény a *STORE_Port*-on keresztül tárolja a kiértékelés idejére, valamint szöveges állományként is menti egy megadott könyvtárba a központi kiszolgálón. Ezen kívül a hálózat monitorozása során létrejött bináris állományt is ugyanazon könyvtárba tárolja.

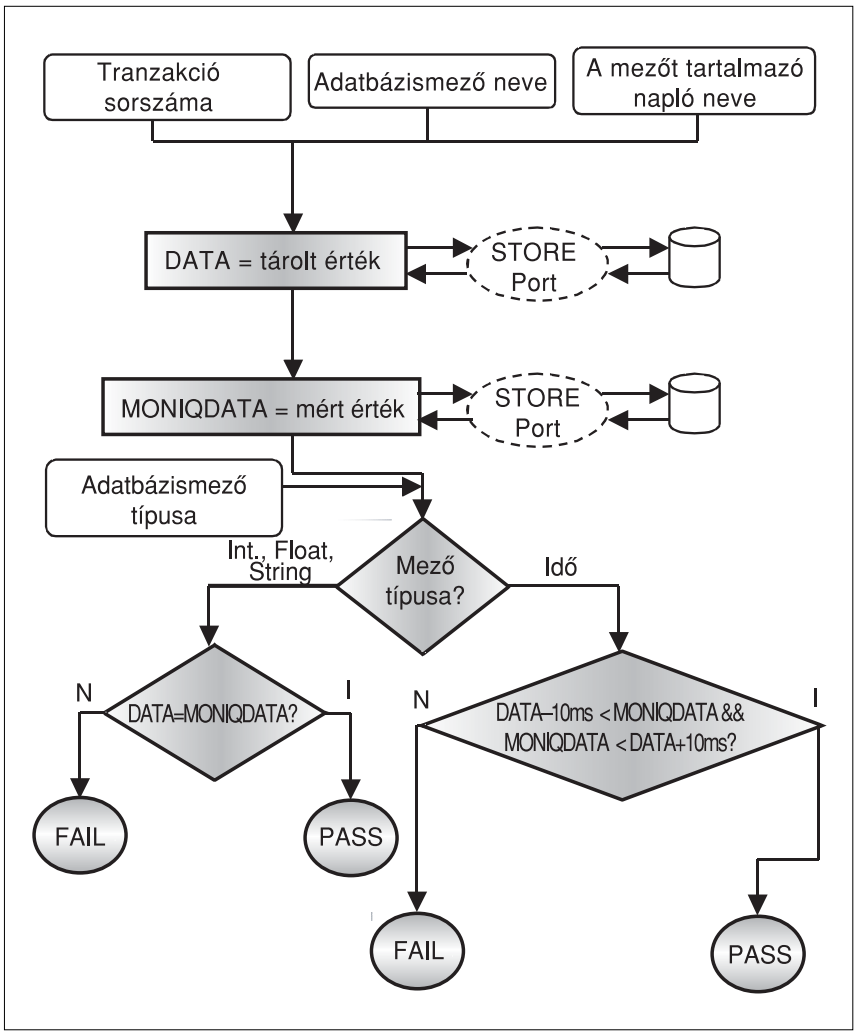
A moniq_results függvény

Amint a *moniq_result_get* függvény tárolta szöveges formában az adott teszt szempontjából érdekes napló állományt, az eredményeket a *moniq_results* segítségével értékeli.

A függvény két értéket kérdez le a *STORE_Port*-on tárolt adatbázisból. A kiolvasott két érték a tesztelő program által helyesnek ítélt és a Moniq által mért adat. A függvény bemeneti paraméterei a következők: a vizsgált adatbázismező neve, a mezőt tartalmazó statisztika neve, egy tranzakció sorszám és az adatbázismező típusa, mely négyféle lehet. A teszt ezek után átment *(pass)* ítélettel zárul, ha a kapott két érték megegyezik. Amennyiben az adat típusa egész szám, valós szám vagy szöveg, teljes egyezőséget vizsgál, ha a típusa idő, 10 ms-os pontossággal értékel ki a program.



7. ábra A Moniq-ot kezelő függvények használata



6. ábra A moniq_results függvény működése

7. A mérések értékelése

A mérési elrendezés kidolgozásánál fontos szempont, hogy a vizsgálati módszer rugalmas, könnyen átalakítható legyen. Annál is inkább, mivel a Moniq forgalom-analizátor szoftver fejlesztése a teszteléssel egyidejűleg folyt, így többször szükség volt a tesztelési eljárás kis mértékű átalakítására. Éppen ezért a forgalom-analizátor kezelését végző, tehát a Moniq-specifikus rutinokat jól elkülöníthetően kellett kialakítani.

Ennek a moduláris felépítésnek köszönhetően egy másik forgalom-analizátor megvalósítás tesztelése sem igényelne óriási beavatkozást a tesztrendszerbe, mivel csak a Moniq specifikus részek cseréjére lenne szükség. A teszteléshez használt protokollok körét a modularitásból adódóan úgyszintén könnyedén lehet bővíteni.

A kidolgozott módszer működéséből látható, hogy a felhasznált konformancia vizsgálati eszközök rugalmasságuknak köszönhetően más, a konformancia vizsgálatoktól eltérő feladatok megoldására is alkalmazhatók. A TTCN-3 nyelv használatával olyan vizsgálatok is elvégezhetőek,

melyek más módszerrel nem lehetségesek, például logikailag hibás vizsgálati sorozatok előállítása vagy adott értékű válaszidők szimulálása.

A teljes tesztkészlet futtatására a vizsgált szoftver minden újabb verziójának *(build)* létrejöttekor lehetőség van. Ekkor az összes teszteset emberi beavatkozás nélküli futtatása után a tesztek által készített naplóállományokból kiválaszthatók a hibás *(fail)* ítélettel zárult tesztek. Ezután az ilyen naplók részletes elemzésével megtudható, hogy a kiértékelés során melyik adatbázis mező tartalmazott hibás értéket, illetve következtethetünk a hiba okára is.

Amint a vizsgálat során egy hibára fény derül, az azonnal hibajelentésként *(Trouble Report)* továbbítható a fejlesztőkhöz, és a hiba akár már a következő fejlesztői változatban kiküszöbölhető.

Irodalom

[1] Stine, R.: FYI on a Network Management Tool Catalog: Tools for Monitoring and Debugging TCP/IP Internets and Interconnected Devices [RFC1147]
[2] Bradner, S., McQuiad, J.: Benchmarking Methodology for Network Interconnect Devices [RFC 2544]
[3] A GNU/GPL értelmében ingyen hozzáférhető Ethereal programcsomag weboldala: http://www.ethereal.com/
[4] A lengyel A plus C Ltd. által fejlesztett Anasil programcsomag weboldala: http://www.anasil.net/
[5] HTE Online könyv: Távközlő hálózatok és informatikai szolgáltatások
[6] Szabó, J.Z. (Ericsson Mo. Konformancia Laboratórium): User Documentation for the TTCN-3 Test Executor
[7] Agilent Technologies: Test Automation for Network Routing Devices [Technical Report ; http://www.agilent.com]

Hírek

Az **Oracle a kaliforniai San Diegoban zajló Apps World konferenciáján** több újdonságot jelentett be termékeiről, az alkalmazásfejlesztés legújabb irányairól és várható fejleményeiről.
Az Oracle betekintést nyújtott új üzleti alkalmazásegyüttesének, az Oracle® E-Business Suite 11i.10 jellemzőibe. A nemsokára megjelenő új változatban komoly továbbfejlesztéseket hajtottak verge az integrációs rétegben, és jelentősen bővült az ágazatspecifikus üzleti folyamatokat támogató funkciók köre. Az Oracle alkalmazásait használó szervezetek több mint 85 százaléka jelenleg az Oracle E-Business Suite 11i verziót használja, így az ügyfelek többségének nem okoz majd gondot az áttérés a 11i.10-re. Az új verzió az Open Applications Group (OAG) által definiált nyílt szabványú interfészeket is támogatja, amelyek egységes szabványokat biztosítanak az üzleti alkalmazások integrálásához. A 11i.10 változat több, mint 150 szabványos OAG üzleti objektumot támogat, amelyek például rögzítik, hogyan kell definiálni egy beszerzési megrendelést.
Egy másik újdonsága az integrációs interfészek katalógusa, amely az Oracle E-Business Suite közzétett API-jait írja le. Emellett az Oracle Application Server 10g képességeit is kihasználja az integrációhoz más fejlesztők alkalmazásaival és az üzleti partnerekkel.
Továbbfejlesztett automatizálási és felügyeleti szolgáltatások az E-Business Suite Outsourcing-ban. A továbbfejlesztések megkönnyítik a rendszeradminisztrációt, automatizálják a szoftverfelügyelet egyes fontos folyamatait, proaktív rendszermonitoringot biztosítanak, és csökkentik a karbantartási költségeket.
Az ügyfél változó üzleti követelményeinek rugalmas kiszolgálásához az Oracle egy- vagy többéves szerződéseket kínál 30 napos felmondással; az ügyfél megválaszthatja, hol üzemeljen a hardver, és a kihelyezéses szolgáltatásokat az Oracle kínálatában szereplő bármely termékhez igénybe veheti.

A **Linux World Konferencián bejelentett újdonságok** három fő csoportba sorolhatók.
Az első az új generációs asztali technológiák, amelynek keretében megjelenik a Sun Java Desktop System új verzója Linuxon. Ebben bővülnek a szoftver felügyeleti funkciói, valamint megjelenik egy új háromdimenziós, Java alapú PC desktopfelület.
A második csoportba a vállalati szoftverek és hardverek sorolhatók: a Java Enterprise System, integrált infrastruktúraszoftver-megoldás, és támogatni fogja a Linux operációs rendszert Intel Xeon rendszereken és az AMD Opteron processzor alapú x86 szervereken is.
A harmadik csoportot a Linuxos fejlesztőeszközök képezik: a Sun bemutatott egy asztali megoldást, amely a Sun új Java Studio Creatorát, egy egyszerűen használható Java-alkalmazáskészítőt. A Sun a tervek szerint 2004 végéig fejlesztőeszközeinek teljes sorát megjelenteti Linuxra is.

Folyamatok hibatoleráns futtatása számítógépfürtön

KATONA ZOLTÁN

Budapesti Műszaki és Gazdaságtudományi Egyetem, Szélessávú Hírközlés és Villamosságtan Tanszék
kz340@hszk.bme.hu

Kulcsszavak: nagy kapacitást igénylő programok, MPI, együttműködési hibák

A cikkben két hibatűrő rendszert mutatok be, melyet az egy-két processzoros személyi számítógépekből álló számítógépfürtökre dolgoztak ki. Jelen esetben hiba alatt az olyan véletlenül bekövetkező eseményeket értjük, melyek miatt egy, vagy több számítógép többé nem része a számítógépfürtnek. A kiváltó ok lehet többek között a merevlemez, memória, alaplap, vagy a processzor meghibásodása, áramszünet, de akár az operációs rendszer, vagy bármelyik létfontosságú szoftver lefagyása is. A hibatűrő rendszerek legfontosabb feladata, hogy a több hétig, hónapig futó nagy számításigényű alkalmazást ne kelljen újraindítani egy ilyen nem várt esemény miatt. Biztosítaniuk kell az alkalmazás zavartalan futását, amelyet a hibák detektálásával, illetve ezek kiküszöbölésével érhetnek el.

Bevezetés

A kutatás és a tudományok területén egyre nagyobb szükség van olyan számítógépes háttérre, amely támogatja a nagy számításigényű, nagy pontosságú alkalmazások *(HPC – High Performance Computing)* futtatását. Ezekhez a feltételekhez a legalkalmasabb környezetet az igen drága, azonban gyors és megbízható, több processzoros, nagy memóriával és háttértárral rendelkező szuperszámítógépek nyújtják. Többnyire az egyetemek, kutatóközpontok nem engedhetik meg maguknak, hogy saját célra ilyen eszközt vásároljanak, ezért sorba kell állniuk, hogy használhassák a világ valamelyik szuperszámítógép-központjánál rendelkezésre álló kapacitást. A helyzet azonban enyhült azóta, hogy Magyarországon a Nemzeti Információs Infrastruktúra Fejlesztési Iroda Szuperszámítógép Központjában [1] 2001-ben üzembehelyeztek egy mára, 196 processzorosra bővült Sun szuperszámítógépet.

Sajnos ennek ellenére is fennállnak a fent említett nehézségek, amelyeknek a kiküszöbölésére kidolgoztak egy megoldást, melyben olcsó, egy-két processzoros, kis számítási kapacitással rendelkező személyi számítógépeket kötnek össze egy hálózattal *(Workstation Cluster)*, hogy az együttes számítási teljesítményük elég nagy legyen ahhoz, hogy megközelítsék a szuperszámítógépekét. Ez a megoldás két problémát vet fel:

- Hogyan lehet elérni a számítógépek és a rajtuk futó folyamatok (processzek) összehangolt működését?
- A személyi számítógépek olcsóságukból eredően megbízhatatlanok lehetnek, vagyis a meghibásodásig tartó idő várhatóértéke sokkal kisebb, mint a szuperszámítógépeké *(MTBF – Mean Time Between Failures)*.

Az 1990-es évek elején az első problémakör megoldására hozta létre az MPI Forum több mint 40 szervezet részvételével az MPI szabványt [2, 3]. Az üzenettovábbító illesztő felület *(MPI – Message Passing Interface)* célja az, hogy a gyakorlatban is alkalmazható, hordozható, hatékony és rugalmas felületet biztosítson üzenettovábbítás céljából. Ennek az interfésznek a segítségével lehet megoldani több számítógépen futó folyamatoknak a hatékony kommunikációját. A szabvány által definiált MPI a viszonyréteget és a megjelenítési réteget foglalja el az ISO OSI hétrétegű modelljében [4, 5]. Olyan értéknövelt szolgáltatásokat nyújt, mint a folyamatok szinkronizálása, a feladat szétosztás, másrészt foglalkozik a továbbítandó információk szintaktikájával és szemantikájával, amivel az adatábrázolás különbözőségeiből eredő problémákat kiküszöböli a heterogén rendszerekben (SGI IRIX, DEC Alpha stb.).

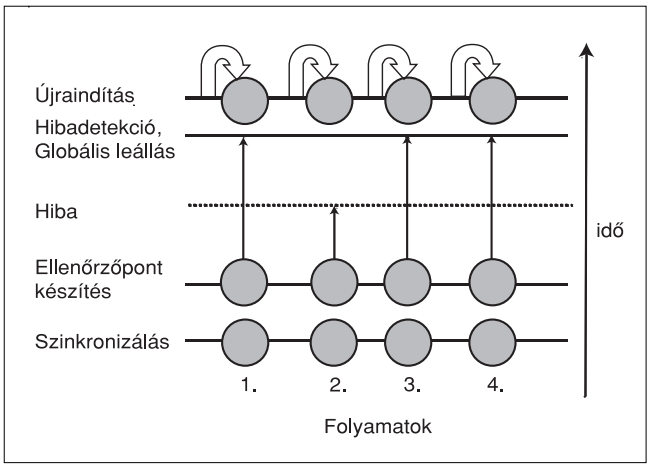
A második probléma megszüntetésére különböző hibadetektáló és elhárító technikák jelentek meg az évek során, melyeknek az előbb ismertetett MPI szabványon alapuló két eltérő gyakorlati megvalósítását szeretném bemutatni.

A hibadetektáló és elhárító technikák

A következő pontban leírt hibatűrő rendszerek működésének megértéséhez néhány alapfogalmat tisztázni kell. A cikkben MPI alkalmazásnak nevezzük a számítógépfürtön futó, nagy számítási kapacitást igénylő programot. Az MPI alkalmazás több folyamatból áll, melyek mindegyike ideális esetben egy külön processzoron fut. Ezek a folyamatok egymásnak üzeneteket – például kiindulási adatokat, eredményeket – küldve kommunikálnak, hogy az egész alkalmazás sikeresen befejezze a munkát.

A hibadetektáló és elhárító technikákat három fontos paraméter különbözteti meg: az átlátszóság *(transparency)*, az ellenőrzőpont koordináció *(checkpoint coor-*

dination) és az üzenetek naplózása *(message logging)* [6]. Ahhoz, hogy az átlátszóság teljesüljön, az üzenettovábbító alkalmazásnak képesnek kell lennie mind futási időben az automatikus hibadetektálásra és javításra, mind a hibajavítási folyamatba becsúszó hibáról értesítést adni a programozónak, felhasználónak. Az ellenőrzőpont-állomány *(checkpoint image)* nem más, mint egy, a folyamat futása során keletkező részeredményeket tároló állomány. Ha a számítógép, amelyen a folyamat eddig futott, hiba következtében kiesik a számítógépfürtből, akkor a hibatűrő rendszer ezt a folyamatot egy olyan gépre ütemezi, amely továbbra is a fürt tagja. Amennyiben nem készült ellenőrzőpont-állomány a hiba miatt kiesett folyamatról, akkor az újraütemezés során elölről kell kezdenie a számításokat, ellenkező esetben azonban a részeredmények segítségével a legutolsó közbülső állapotból folytathatja a feldolgozást.



1. ábra
Koordinált ellenőrzőpont-állomány készítés

Az ellenőrzőpont koordinációnak két fontos típusa van. A koordinált, illetve a nem koordinált változat. A koordinált esetben, ahogy az *1. ábra* is mutatja, minden folyamatot szinkronizálni kell, vagyis be kell szüntetniük a hálózati kommunikációt, hogy ne vesszen el információ az ellenőrzőpont-állományok készítésekor. Amennyiben egy folyamatot újra kell indítani, mert kiesett az a számítógép, amelyen eddig futott, akkor mindegyik folyamat újraindul a legfrissebb ellenőrzőpontról. Sajnos ezek a tulajdonságok okozzák, hogy ez a módszer nem skálázható, mivel nem lehet csak a kiesett folyamatokat újraütemezni, hanem mindegyiket újra kell indítani az utolsó ellenőrzőpontról.

Ez nagyban növeli a rendszer sérülékenységét, hiszen ha nem túl sűrűn készítünk ellenőrzőpont-állományokat, akkor értékes processzor idők veszhetnek el hiba esetén, akár csak egy gép kiesésekor is, mivel így mindegyik számítógép munkája elvész. Ha sűrűbben készítünk ellenőrzőpont-állományokat, akkor ez kevésbé hangsúlyos, eltekintve az ehhez szükséges többlet időtől.

A nem koordinált esetben egymástól függetlenül, szinkronizálás nélkül, eltérő időpontban készíthető mindegyik folyamatról ellenőrzőpont-állomány, így a rendszer skálázható, vagyis elegendő csak a kiesett folyamatokat újraütemezni. Nem koordinált esetben a folyamatok nem szüntetik be az ellenőrzőpont-állományok elkészítésekor a hálózati kommunikációt.

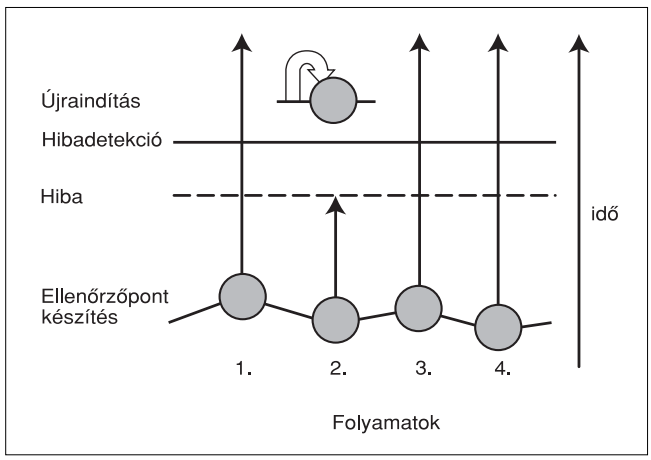
Ez azt jelenti, hogy a hálózaton levő üzeneteket naplózni kell, mivel az ellenőrzőpont-állományok nem hordoznak semmiféle információt ezekről. Vagyis, ha egy folyamat üzenetet küld egy másiknak – például egy kiindulási adatot – és a címzett kiesik, nem kapja meg az üzenetet, akkor az újraütemezett folyamat várni fogja az üzenetet, de a feladó abban a hitben él, hogy a címzett már megkapta. Ez végső soron az egész alkalmazás fennakadásához vezethet. A *2. ábra* a nem koordinált ellenőrzőpont-állomány készítésre mutat egy példát.

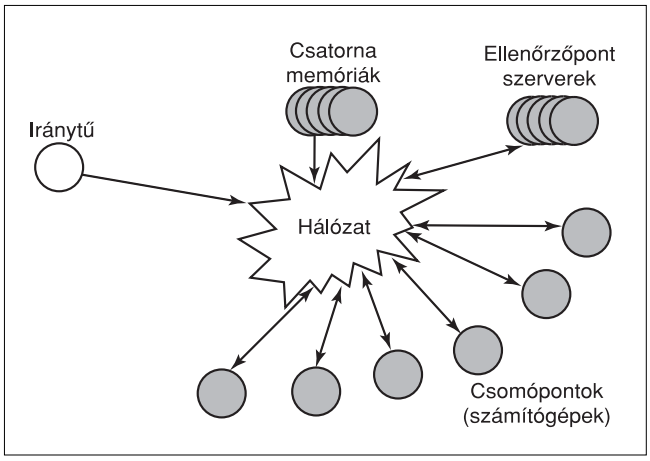
Ha a hibatűrő rendszer nem készít ellenőrzőpont-állományokat, akkor a rendszer csak a kommunikációs naplókra hagyatkozhat a kiesett folyamatok újraütemezésekor, vagyis a folyamatokat nem lehet részeredmények segítségével egy közbülső állapotból újraindítani. Az egész alkalmazást a számítás legelejétől újra kell indítani. Ebben az esetben a kommunikációs naplóknak az a haszna, hogy a folyamatoknak nem kell várniuk az üzenetekre, mert az a kiesés pillanatáig rendelkezésre áll.

Az üzenetek naplózása is többféle lehet. Létezik pesszimista és optimista naplózás. Pesszimista esetben megbízható adattároló eszközre mentik az üzeneteket, amelyeknek nagy az MTBF-je, ezért igen kicsi valószínűséggel vesznek el erről adatok. Optimista esetben nem megbízható adattárolóra mentik az üzeneteket.

Amennyiben egy számítógép tönkremegy, akkor a folyamatot más számítógépek naplóinak megfelelően indítják újra, viszont ha egynél több számítógép hibásodik meg, akkor az utolsó koherens ellenőrzőpontról történik a folyamat újraindítás, mivel ha rosszul van megtervezve a rendszer, akkor a kiesett gépek közötti kommunikáció is megszakad, amit csak úgy lehet kiküszöbölni, hogy a folyamatokat a koherens ellenőrzőpontokról indítjuk újra.

2. ábra
Nem koordinált ellenőrzőpont-állomány készítés





3. ábra Az MPICH-V rendszer felépítése

Hibatűrő megoldások, előnyeik és hátrányaik

Az alapok tisztázása után rátérek néhány gyakorlati példa részletezésére. Az első hibatűrő rendszer, amelyet bemutatok az MPICH-V [6], (Cluster&GRID group, Laboratoire de Recherche en Informatique, University of Paris South). Ez a hibatűrő rendszer azt feltételezi, hogy az MPI alkalmazás futása során keletkező hibák a számítógépek meghibásodása miatt keletkeznek. Ennek az elgondolásnak az architektúrája több elemből áll. Megbízható csatornamemóriák *(Channel Memory)*, megbízható ellenőrzőpont szerverek *(Checkpoint Server)* és egy irányító *(Dispatcher)* alkotják a csomópontokkal *(Node)* együtt a rendszert, ahogyan a *3. ábra* is mutatja.

A csatornamemóriák feladata, hogy naplózzák az MPI folyamatok közötti üzenetváltást. Az MPI folyamatok valójában nem egymással kommunikálnak, hanem egy-egy csatornamemóriával. A csomópontok csoportokba vannak szervezve, és mindegyikhez tartozik egy csatornamemória. Amennyiben egy csomópont üzenetet vár, akkor azt a saját csoportjához tartozó csatornamemóriától fogja megkapni, viszont ha üzenetet akar küldeni, akkor a címzett csoportjához tartozó csatornamemóriának kell elküldeni. A csatornamemóriák FIFO elven működnek, vagyis az először beérkező üzenet hagyja el először a memóriát.

Ezzel és a több csatornamemória felhasználásával, valamint a csomópontok csoportokba szervezésével szerették volna a tervezők elérni a koordinációs üzenetek csökkentését és a vevő számára az üzenetek teljes sorrendbe szervezését. Egy többszálú szerver végzi az esemény kezelését, vagyis a beérkező és a kimenő üzenetekkel kapcsolatos teendőket. Üzenetek nem csak a csomópontoktól érkezhetnek, hanem a csomópontokhoz csatolt ellenőrzőpont szerverektől, és az irányítótól is. Ezek többnyire vezérlő üzenetek. A többszálú szerver egy FIFO memóriába teszi az üzeneteket, ahonnan egy megbízható adattárolóra kerülnek, így abban az esetben, ha egy csomópont tönkremegy, akkor mintegy „újra lejátszható” a kommunikáció az újraindított MPI folyamattal. A legfrissebb ellenőrzőpont-állományok létrehozásának dátumánál régebbi üzeneteket törlik az adattárolóról.

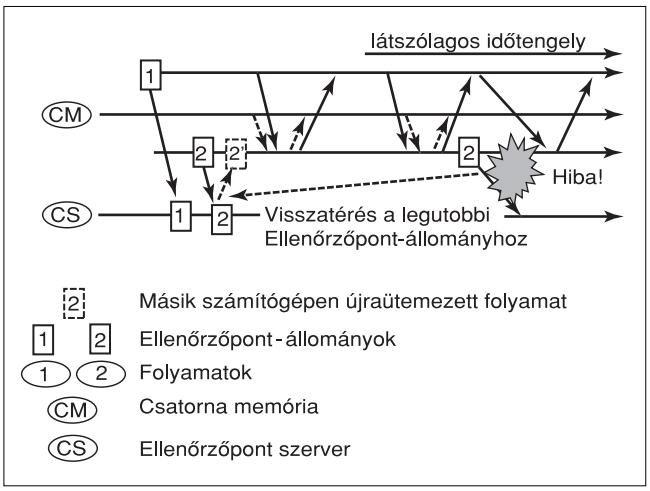
Az előző pontban tárgyaltak alapján a csatornamemóriák pesszimista típusú naplózást végeznek, mivel megbízhatóak. A megbízhatóság miatt a hardvernek szigorúbb követelményeket kell kielégítenie, így igen drága. Az ellenőrzőpont-szerverek tárolják az ellenőrzőpont-állományokat, amelyek a folyamatok egy korábbi állapotát írják le. Minden csomóponthoz egy fájl tartozik a szerveren.

Az ellenőrzőpont-állományok készítését kiváltó eseményeket nem kívülről – például az irányítótól – kapják a csomópontok, hanem lokálisan, adott időközönként érkeznek meg. Az algoritmus egy olyan (fork()) rendszerhívással kezdődik, amely az MPI folyamatról egy másolatot készít. A másolat minden hálózati kapcsolatot lezár, így minden kommunikációt megszakít, ezzel lehetővé válik az ellenőrzőpont-állomány elkészítése. Amikor elkészült a kép, a folyamat másolata befejezi a futását. Az ellenőrzőpont-állományt ezután a csomópont elküldi az ellenőrzőpont szervernek. A megoldás előnye, hogy az eredeti folyamatnak eközben nem kell megszakítania a futását. A csatornamemóriákhoz hasonlóan az ellenőrzőpont szervereknek is megbízhatónak kell lenniük, tehát ez a tulajdonság is hátrányok közé sorolható.

A következő rendszerelem az irányító. Az irányító többek között a parancsvégrehajtás inicializálását végzi, vagyis ellenőrzi, hogy a rendszerelemek készen vannak-e, csoportokba szervezi a számítást végző csomópontokat és csatornamemóriát rendel hozzájuk, továbbá figyeli a csomópontok állapotát, vagyis hogy érkezik-e a csomópontoktól „életjel”, vagy van-e időtúllépés. Emellett elindítja a megfelelő példányszámban a programokat az egyes számítógépeken, illetve ha egy MPI folyamat „halott”, akkor azt a fennmaradt csomópontok valamelyikén újraütemezi.

Ennek az összetett rendszernek a működését mutatja a *4. ábra*. Az ábrán a legrosszabb eset *(Worst Case)* látható, mivel a hálózaton levő ellenőrzőpont-állomány,

4. ábra Legrosszabb eset: üzenet és ellenőrzőpont-állomány elveszik



és az üzenet is elvész, hiszen az a számítógép, amelyiken a 2. MPI folyamat futott, tönkrement. Ezt az irányító veszi észre, mivel a számítógép nem küldött életjelet magáról. Ekkor az irányító a 2. MPI folyamatot egy másik csomópontra ütemezi úgy, hogy az „új" számítógép a 2. folyamat futtatásához szükséges ellenőrzőpont-állományt az ellenőrzőpont szervertől kapja meg. Az újraütemezett 2. folyamat (2') az ellenőrzőpont-állomány elkészítésének időpontjától az újabb kommunikációt a csatorna memóriával játssza le, mivel az 1. folyamat a köztük levő üzenetváltásnak ezen a részén már régen túl esett, vagyis a két folyamat emiatt, és a rendszer architektúrája miatt sem tud egymással közvetlenül kommunikálni.

Az ábrán a csatorna memória és a 2. folyamat, illetve a 2'. folyamat közötti kommunikációt jelző folyamatos, illetve szaggatott vonal szinte egymást fedik, de valójában időben nem egyszerre zajlanak az üzenetváltások, ezért látható az ábrán a látszólagos időtengely felirat.

A rendszer előnyei és hátrányai tehát a következők. Az irányító nem redundáns, emiatt végzetes hiba következhet be a kiesésekor. A csatornamemóriáknak és az ellenőrzőpont szervereknek megbízhatóaknak kell lenniük, ami tetemes összeggel megemeli a rendszer árát. A rendszer teljesítményét rontja, hogy a minden üzenetnek kétszer kell a hálózatra lépnie, mivel az MPI folyamatoknak a csatornamemóriákon keresztül kell kommunikálniuk. A hálózatterhelés főleg nagy méretű üzenetek esetén mutatkozik meg.

A rendszer előnyei közé sorolható az, hogy az összes MPI folyamat „halálát" túl tudja élni, mivel az ellenőrzőpont szerverek a folyamatok konzisztens ellenőrzőpont-állományainak halmazát tartalmazzák, továbbá a csatornamemóriákban a teljes rendszer kommunikációja el van mentve, ezzel lehetővé téve a rendszer gyorsabb helyreállítását. További előnyt jelent az, hogy az MPI folyamat leállása nélkül lehet ellenőrzőpont-állományt készíteni a folyamatról.

Az elmúlt években mások is foglalkoztak ezzel a témával, más szemszögből megközelítve a problémát. Az MPI/FT [7] (Mississippi State University, Department of Computer Science; MPI Software Technology, Inc.; NASA Jet Propulsion Laboratory, California Institute of Technology) módszer feltételezi, hogy a programozó által megírt MPI alkalmazás futása során keletkező hibák egy-egy csomópont meghibásodásából, továbbá véletlenszerű bithibákból eredhetnek. Tehát az előzőekben vizsgált rendszertől az MPI/FT ezzel is többre képes. Ezeket a bithibákat okozhatják a vezetékeken fellépő elektromágneses zavarok, áthallások. Feltételezi továbbá, hogy a processzor második szintű (L2) gyorsítótára mind a memória külső zavarok, mind az űrből érkező nagyenergiájú töltött részecskék ellen védve van, így a véletlen bithibák nem okozhatnak ezeken a helyeken gondot.

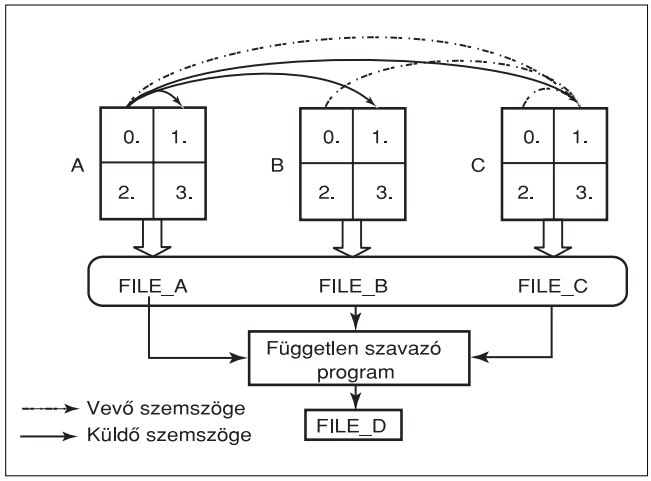
A hibadetektálásnak és javításnak több módszerét veti fel az MPI/FT. Önellenőrző szálak *(SCT – Self-Checking Thread)* használatát javasolja, amelyek különböző feladatokat töltenének be. Folyamatok globális adatstruktúráira szavaznának egyszerű többségi döntéssel, továbbá lokális adatokat több példányban tárolnának és időközönként szintén többségi szavazással eldöntenék, hogy melyikük tartalmaz helyes adatokat. Ezekre a szavazásokra főleg olyan helyeken van szükség, ahol gyakran előfordulhatnak az adatokban véletlenszerű változások, például bithibák. Ilyen környezet tipikusan a nagyszámú nagyenergiájú, illetve töltött részecskéket tartalmazó hely, például az űr. További feladatuk lehetne egy nem blokkoló kollektív függvény időnkénti meghívása, mellyel észlelni lehetne a kiesett MPI folyamatokat, mivel ezek nem hívják meg a függvényt, így az a hívó oldalon időtúllépéssel hibát fog jelezni. Feladatuk lenne még a folyamatok közötti kommunikáció és a belső dinamikus memória lefoglalás figyelése is.

A hibatűrő rendszer részét képezi a koordinátor *(Coordinator)* is, amely az előzőekben taglalt csatornamemóriához és irányítóhoz hasonlóan működik. Ez a koordinátor az SPMD *(Single Program, Multiple Data)* alkalmazásoknál egy különálló számítógép lehet, illetve a mester/szolga modellben a mester töltheti be az adott funkciót. A tudományos programok jelentős része a mester/szolga vagy az SPMD modellt követi. Az SPMD modell lényege, hogy minden processzor ugyanazt a programot hajtja végre, de a folyamatok futása minden processzoron más-más irányt vehet. Mivel ezek a modellek a legelterjedtebbek, ezért az MPI/FT is ezekkel tud a legjobban együttműködni.

A koordinátor feladata az MPI alkalmazás folyamatos ellenőrzése, a kiesett folyamat újraindítása egy ellenőrzőpontról, majd a napló alapján a kommunikáció újralejátszása a folyamattal, hogy a rendszer újra konzisztens állapotba kerüljön. A feladatai közé tartozik továbbá az is, hogy az üzenetek számára virtuális csatornaként működjön, mivel így minden kommunikációt naplózni tud. Periodikusan vezérlőüzeneteket kell küldenie az önellenőrző szálaknak, ezenkívül válaszolnia kell az általuk küldött üzenetekre.

A biztosabb végeredmény érdekében a párhuzamos nMR *(n-Modular Redundancy)* módot vezették be

5. ábra Párhuzamos nMR végrahajtás



a tervezők, amelynek a lényege, hogy minden MPI folyamatnak *n* példánya készül az MPI alkalmazás indításakor. Ezt szemlélteti az *5. ábra* [7].

Az ábrán az MPI alkalmazást 4 párhuzamos folyamattal indítjuk el, és mindegyiknek készül két másolata. Az ábrán jól látható, hogy mi történik üzenetküldéskor. Ha a nulladik folyamat az elsőnek üzenetet akar küldeni, akkor azt az első folyamat minden példánya megkapja, illetve ha az első üzenetet vár a nulladik folyamattól, akkor a nulladik folyamat összes példányától megkapja azt. Ekkor a vevő a vett üzeneteket összehasonlítva egyszerű többségi szavazással megállapíthatná, hogy melyik üzenet tartalmaz helyes adatokat. A folyamatok az eredményeket egy-egy fájlban tárolhatják és egy független szavazó program ezeket összehasonlíthatja.

Az MPI/FT hátrányai a központosított irányítás, a koordinátor használata. A koordinátor ment el minden kommunikációt, amely a folyamatok között lezajlik, ami azt jelenti, hogy a koordinátor egy létfontosságú elem (centralizált). A rendszer ezt az nMR mód segítségével szeretné kiküszöbölni, vagyis redundáns koordinátort vezet be. Ez rövid számolás után igen nagy hálózatterhelést jelent.

Tegyük fel, hogy egyetlen folyamat akar üzenetet küldeni egy másiknak. Mivel ezek a folyamatok is nMR módban futnak, ezért mindegyikből van a rendszerben *n* példány. A működési elv alapján így *n* darab folyamat fog *n* másik folyamatnak üzenetet küldeni, ami összesen eddig n^2 üzenetet jelent. Ehhez hozzá kell venni, hogy minden üzenetnek keresztül kell mennie a koordinátoron, vagyis minden üzenet kétszer kerül a hálózatra, tehát $2*n^2$ üzenetnél tartunk. Mivel a koordinátor is nMR módban fut, ez azt jelenti, hogy ugyanez az üzenetmennyiség megjelenik minden egyes koordinátor miatt a hálózaton, vagyis az eredetileg elküldeni szándékozott egy darab üzenetből $2*n^3$ üzenet keletkezett.

Hogy még inkább szemléltessem a probléma súlyát, figyelembe kell venni, hogy egyszerű többségi döntés végrehajtásához *n*-et páratlannak érdemes választani, hogy ne kerüljünk döntésképtelen helyzetbe. Ez azt jelenti, hogy *n*-nek legalább 3-nak kell lennie, vagyis a minimális hálózatterhelés esetén is 1 üzenet elküldése valójában 54 üzenetküldéssel jár. Ezek után már nem is érdemes abba belegondolni, ha az üzenet mérete nő, vagy ha nem csak két folyamat kommunikál, ahogy az előzőekben feltételeztem, hanem több.

Ezek a tények arra engednek következtetni, hogy az MPI/FT-t nem érdemes nagy számítógépfürtökben alkalmazni, hanem inkább kisebb, nagy megbízhatóságú, redundáns rendszerekben lehet hasznát venni, mint amilyenek egy űreszközön is előfordulhatnak. További lehetséges alkalmazási területe a megoldásnak az, hogy dedikált processzorokat alkalmazunk, amelyek pont-pont összeköttetéseken keresztül kommunikálnak egymással, hiszen ekkor a nagy hálózati terhelés megoszlik az összeköttetések között.

Összefoglalás

A cikkben áttekintettem a számítógépfürtökre kidolgozott hibatűrő rendszerek egy részét. Értelmeztem az alapvető fogalmakat, az ellenőrzőpont koordináció és a naplózás típusait, jelentőségüket. Bemutattam az MPICH-V és az MPI/FT hibatűrésre kidolgozott megoldások architektúráját, a hibadetektálási és javítási folyamatuk lényegét. Kifejtettem a rendszerek előnyeit, hátrányait, miszerint az MPICH-V drága, de megbízható, így nem redundáns rendszerelemeket alkalmaz, illetve túl tudja élni akár az összes MPI folyamat „halálát”.

Az MPI/FT ezzel ellentétben olcsó redundáns rendszerelemeket alkalmaz, a hibavalószínűséget a párhuzamos nMR móddal próbálja csökkenteni. Sajnos ez a megoldás a túlzottan nagy hálózatterheléssel jár, ezért nem igazán alkalmas arra, hogy nagy számítógépfürtön használjuk.

Irodalom

[1] Nemzeti Információs Infrastruktúra Fejlesztési (NIIF) Program Szuperszámítógép Központjának honlapja, http://www.iif.hu/szuper/

[2] TLTP High Performance Computing Courseware, High Performance Computing Consortium, http://www.cs.ncl.ac.uk/old/modules/2002-03/csc305/TLTP_HPC_Course/

[3] HP MPI User’s Guide, National Center for Supercomputing Applications, http://archive.ncsa.uiuc.edu/SCD/Hardware/CommonDoc/HP/MPI/1_intro.html

[4] C. J. Beckmann, D. D. McManus, G. Cybenko: ”Horizons in scientific and distributed Computing”, COMPUTING IN SCIENCE & ENGINEERING, January-February 1999, pp.23-30.

[5] ISO 7498, Information Processing Systems – Open System Interconnection – Basic Reference Model, International Standards Organization, Geneva, 1984.

[6] G. Bosilca, A. Bouteiller, F. Cappello, S. Djilali, G. Fedak, C. Germain, Th. Herault, P. Lemarinier, O. Lodygensky, F. Magniette, V. Neri, A. Selikhov: ”MPICH-V: Toward a scalable fault tolerant MPI for Volatile nodes”, SC2002

[7] R. Batchu, Jothi P. Neelamegam, Z. Cui, M. Beddhu, A. Skjellum, Y. Dandass, M. Apte: ”MPI/FTTM: Architecture and Taxonomies for Fault-Tolerant, Message-Passing Middleware for Performance-Portable Paralell Computing”, DSM 2001, May 2001, pp.26-33.

Mobil többesadás protokollok vizsgálata IPv6 hálózatokban

KIS ZOLTÁN LAJOS, KOVÁCSHÁZI ZSOLT, KERSCH PÉTER, SIMON CSABA

BME Távközlési és Médiainformatikai Tanszék, High Speed Networks (HSN) Laboratórium

kz345@hszk.bme.hu, kz365@hszk.bme.hu,
kpeti@sch.bme.hu, simon@david.tmit.bme.hu

Reviewed

Kulcsszavak: sávszélesség hasznosítása, távoli feliratkozás, otthoni ügynök, forgalomirányítás

Többesadás protokollok alkalmazásával jelentős sávszélesség megtakarítást érhetünk el a digitális műsorszórás, a videokonferenciák vagy más multimédiás alkalmazások esetén. Ez különösen fontos a szűkös erőforrásokkal rendelkező mobil környezetben. Ebben a cikkben egy a távoli feliratkozás módszerén alapuló protokoll kiegészítést mutatunk be, amellyel az IPv6-os többesadás protokollok teljesítménye jelentősen javítható mobil környezetben. A protokoll kiegészítést meg is valósítottuk és egy kísérleti hálózaton mérésekkel ellenőriztük működését.

Jelenleg telítődött a beszédátvitelre alapozó távközlési szolgáltatások piaca. Ezért a multimédia tartalom tűnik a piaci növekedés új hajtóerejének. Mivel ezek az új tartalmak nagyságrendekkel több erőforrást igényelnek, szükségessé válik a többesadás *(multicast)* alkalmazása, amelynek segítségével jelentős sávszélesség megtakarítás érhető el az egyesadás *(unicast)* alkalmazásokkal szemben.

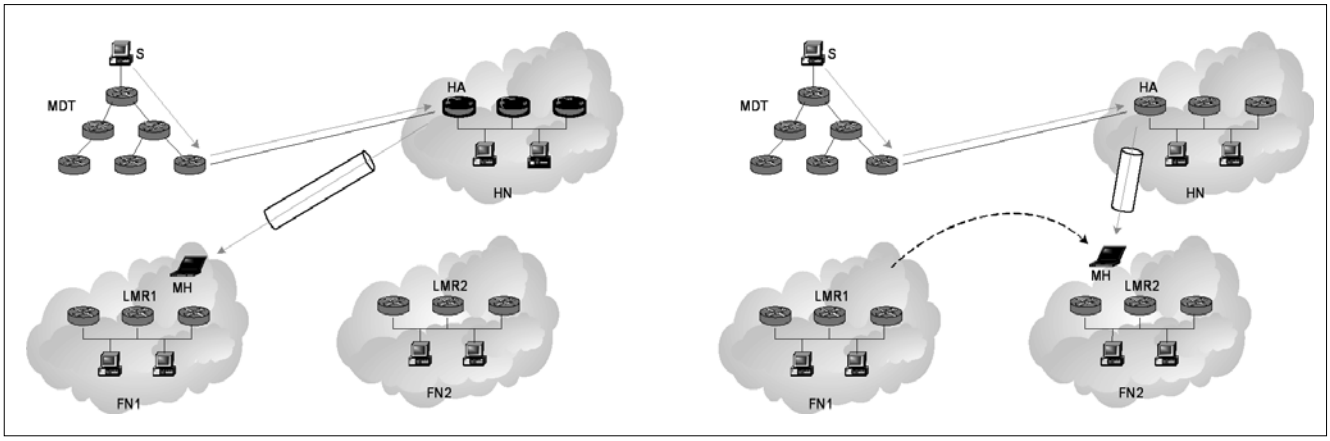
A közeljövőben várhatóan minden vállalati nagytérségi hálózat (WAN) kénytelen lesz erőforrás-optimalizáló módszereket alkalmazni [1], melyek közül jelenleg a többesadás tűnik a legalkalmasabbnak a multimédia folyam és fájl disztribúció csoportos szolgáltatások sávszélesség-hatékony megvalósítására.

Az IP alapú hálózatokban alkalmazott többesadás a közelmúlt egyik nagy kutatási területe. Az IETF számos többesadás protokollt szabványosított [2, 3]. Az elterjedőben lévő nyilvános WLAN *hotspot* és UMTS/GPRS szolgáltatóknak egyaránt érdeke a sávszélesség jobb hasznosítása. Ennek érdekében alkalmassá kell tenni a jelenleg használatos többesadás technológiákat a mobilitás kezelésére. A mobilitás kezelésére az IP alapú hálózati rétegben az IETF által kidolgozott Mobil IPv6 szabvány [4] nyújt megoldást. A Mobil IPv6 azonban csak az egyesadás forgalom mobilitásával foglalkozik. Kutatói körökben a mobil többesadásra két különböző megközelítés terjedt el: a kétirányú alagutazás *(bidirectional tunelling)* és a távoli feliratkozás *(remote subscription)* [5].

A **kétirányú alagutazás** során *(1. ábra)* a mobil állomás az otthoni hálózatán *(home network – HN)* keresztül – otthoni ügynökének *(home agent – HA)* segítségével – csatlakozik a többesadás csoportokhoz. A kommunikációhoz Mobil IPv6 kétirányú alagutazást használnak. Egy idegen hálózatba *(foreign network – FN)* kerülő mozgó állomás először egy kapcsolat frissítés üzenetet küld otthoni ügynökének, majd létrehoz egy alagutat. Ezek után ugyanúgy csatlakozhat egy többesadás csoporthoz, mintha az otthoni hálózatán lenne: MLD jelentéseit az otthoni ügynökének küldi, minek hatására az otthoni hálózat csatlakozni fog a csoporthoz. Amikor a mobil állomás egy új IPv6 alhálózatba lép, kapcsolat frissítés üzenettel informálja otthoni ügynökét új helyéről. Ennek eredményeként az alagút adatai is frissülnek, a végpontja a mobil állomás új elérési címe *(care-of address)* lesz.

A **távoli feliratkozásnál** *(2. ábra)* a mobil állomás az idegen hálózat helyi többesadás útválasztóján *(local*

1. ábra Kétirányú alagutazás



multicast router – LMR) keresztül csatlakozik egy többesadás csoporthoz. A mobil állomás MLD jelentés *(report)* üzeneteket küld a hálózatra, és minden többesadással kapcsolatos eljárást ugyanúgy hajt végre, mint az adott hálózat fix állomásai. Amikor az állomás átmegy egy másik hálózatba, újra csatlakozik a többesadás csoporthoz, itt is a helyi többesadás útválasztó segítségével. Mielőtt az állomás elhagyja a régi idegen hálózatot, jelzi, hogy elhagyja a többesadás csoportot. Amennyiben az állomás volt a csoport utolsó tagja, a többesadás fa *(multicast delivery tree – MDT)* adott útválasztóhoz kapcsolódó ága megszűnik.

Mind a kétirányú alagutazásnak, mind a távoli feliratkozásnak megvannak az előnyei és hátrányai. A kétirányú alagutazás legnagyobb előnye, hogy nincs szükség a többesadás fa újraépítésére helyváltoztatáskor, mivel a többesadás forrás és állomások mozgása teljesen rejtve marad az útválasztók elől. A módszer hátránya, hogy az otthoni ügynök sok állomás esetén szűk keresztmetszetet jelenthet, illetve, hogy az alagutazás miatt nem használja ki a többesadás nyújtotta sávszélesség-takarékos útvonalválasztást. A távoli feliratkozás előnye, hogy a többesadás fa és a hálózati forgalom szempontjából is optimális. Viszont az új ágak kiépülésének ideje alatt csomagvesztés, ezáltal szolgáltatás kiesés jelentkezhet.

A két protokoll hátrányainak kiküszöbölésére számos javaslat született [5], amelyek általában a két módszer ötvözésén alapulnak. A továbbiakban a távoli feliratkozás módszernek egy olyan továbbfejlesztését ismertetjük, amely lehetővé teszi a többesadás adatfolyamok zökkenőmentes hívásátadását, kiküszöbölve a többesadás fa újraépítésének ideje alatt tapasztalható csomagvesztést. A módszer két pontban fejleszti tovább a távoli feliratkozás koncepcióját. Egyrészről a protokoll bevezet egy ideiglenes alagutat a mobil állomás új és előző hozzáférési útválasztója között. Ezen az alagúton keresztül kapja meg a mobil állomás a többesadás csomagokat előző bázisállomásától addig, amíg az új többesadás faágak nem épültek ki az új bázisállomás felé. Másrészről a mobil állomás hívásátadáskor azonnal MLD hallgató jelentéseket küld, nem vár sem az MLD időzítőkre, sem a hálózat többesadás útválasztója által küldött MLD kérésekre *(query)*. Így azonnal megindul a többesadás fa hiányzó ágainak felépítése.

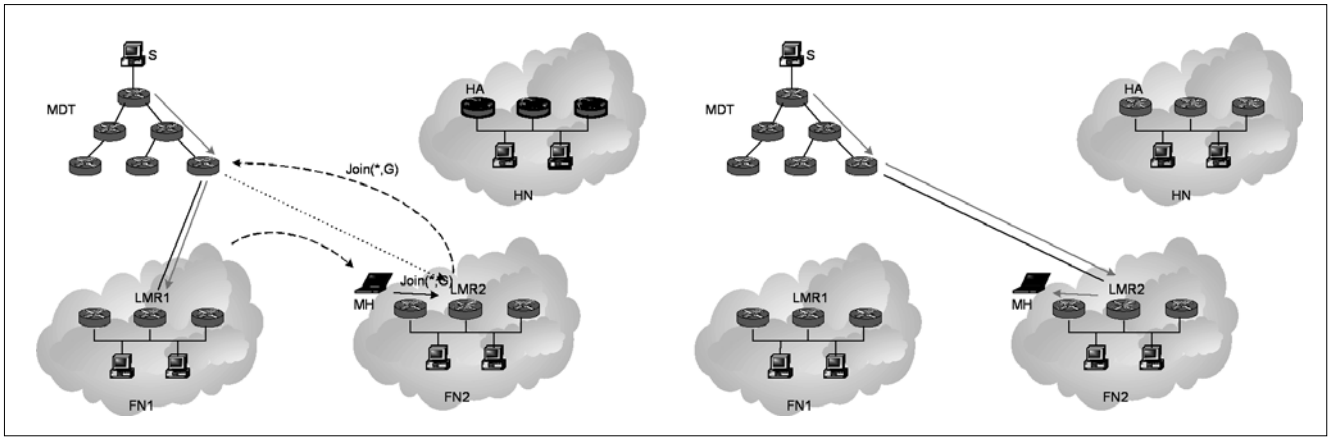
A protokoll kiegészítés tervezése során először is át kellett tekintenünk a protokoll feladatait, majd a mobilitásból fakadó, a távoli feliratkozással szemben támasztott követelményeket. A szolgáltatási modell miatt feltételeztük, hogy a forrás – a tartalom-szolgáltató *(content server)* – a fix infrastruktúrájú hálózatban található. Ezért csak a vevő oldali mobilitásra kerestünk megoldást. Továbbá feltételeztük, hogy a mobil állomás képes felmérni a lefedettségi területén belül elhelyezkedő bázisállomásokat.

Az MMCAST protokoll

A távoli feliratkozás protokollhoz készített kiegészítésünkre a továbbiakban a Mobil MultiCAST elnevezés alapján MMCAST protokoll néven hivatkozunk. Mielőtt rátérnénk a megvalósítás részletes bemutatására, röviden ismertetjük azt a hálózati architektúrát, amelyhez a protokoll megvalósítást készítettük. Hálózati architektúránkban külön egységek látják el a többesadás útválasztó, illetve a hozzáférési útválasztó feladatköröket. Ez azt jelenti, hogy a mobil állomások nem közvetlenül csatlakoznak a többesadás útválasztókhoz, hanem mindig egy bázisállomáson keresztül, ami MLD proxyként is működik [6]. Az MMCAST protokollt a hozzáférési útválasztóknak, vagy a mobil állomásoknak kell futtatniuk. Mivel a többesadás útválasztói illetve bázisállomás funkciókat kettéválasztottuk, a többesadás útválasztóknak nem kell ismerniük a protokollt.

Az MMCAST protokollban minden mobil egység egyértelműen hozzá van rendelve egy hozzáférési útválasztóhoz. Tehát egy mozgó állomás csak akkor kezdheti meg többesadás folyamok vételét, ha az MMCAST protokollal bejelentkezett egy hozzáférési hálózatba. A bejelentkezés azért kötelező, mert csak így tudjuk a mobil állomást azonosítani. Az illegális hálózathasználat ellen úgy védekezünk, hogy csak olyan állomás csomagjait fogadjuk, amelyikkel biztonsági relációban vagyunk. A prototípus validálásához nem volt szükségünk a biztonsági megoldás részletezésére, ezért prototípusunk a biztonsági protokoll üzeneteit nem tartalmazza.

2. ábra Távoli feliratkozás



Mivel mobil környezetben könnyen előfordulhat, hogy egy egység kijelentkezés nélkül lép ki a hálózatból ezért, a bázisállomások puha állapottal *(soft state)* tárolják klienseik adatait. Vagyis, ha a hozzáférési útválasztó nem kap periodikus állapot-frissítés *(REFRESH)* üzeneteket a klienseitől, akkor egy idő után automatikusan törli a mobil állomás regisztrációját az adatbázisából.

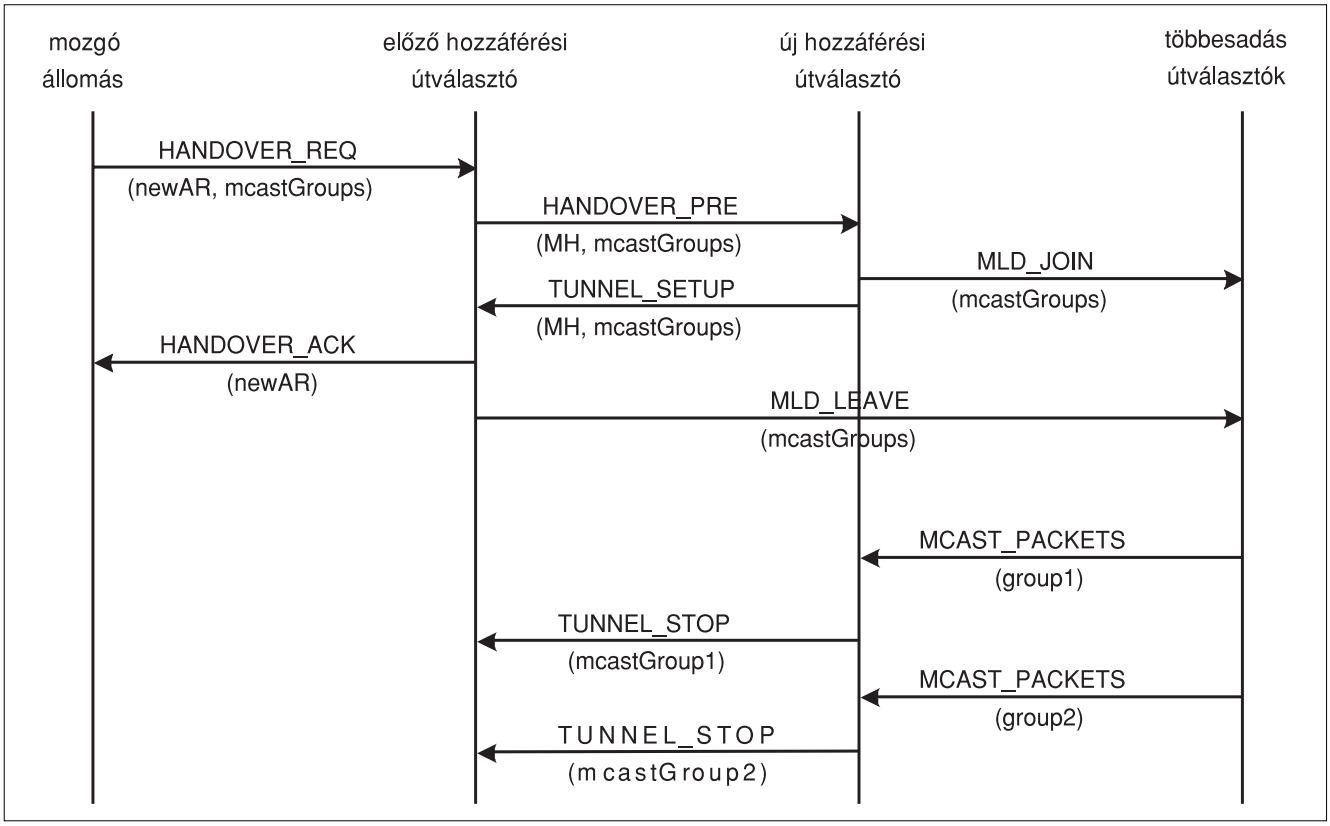
A hívásátadást a mobil állomás kezdeményezi, amikor érzékeli, hogy az aktuális állomásánál egy lényegesen jobb átviteli minőségű is rendelkezésre áll. Az elérhető elérési útválasztók listáját a mobil egység a bázisállomások által periodikusan sugárzott útválasztó-hirdető *(router advertisement)* üzenetekből tudja felépíteni (ezeket használja a Mobil IPv6 is). Az új bázisállomás kiválasztása után az állomás egy *HANDOVER_REQ* üzenetet küld bázisállomásának, ami tartalmazza az új elérési útválasztó azonosítóját (ami esetünkben az útválasztó rádiós interfészének globális IPv6-os címe), valamint az összes olyan többesadás csoport címét, amelyre a mobil egység fel van iratkozva.

Az üzenet vételét követően az aktuális bázisállomása egy *HANDOVER_PRE* üzenetet küld az új útválasztónak. Ez tartalmazza a mozgó állomás azonosítóját (ami az állomás rádiós interfészének új *link local* IPv6-os címe), valamint a *HANDOVER_REQ* üzenetben kapott többesadás címeket. Az új elérési útválasztó megnézi, hogy a kapott többesadás csoportok közül melyekre nincs még feljelentkezve. Ezeket a címeket visszaküldi az előző útválasztónak egy *TUNNEL_SETUP* üzenetben, valamint MLD jelentésekkel jelzi feliratkozási szándékát az új csoportokra. A *TUNNEL_SETUP* üzenet vételekor az előző elérési útválasztó kiépít egy ideiglenes IPv6-IPv6 alagutat az új bázisállomás felé a többesadás folyamok továbbításának céljára. Végül egy *HANDOVER_ACK* üzenettel jelzi a mobil állomás felé a hívásátadás sikeres lezajlását.

Ettől kezdve a mozgó állomást már az új elérési útválasztó szolgálja ki. Amíg a többesadás fák kiépülnek az új útválasztó felé, az előző útválasztó az alagutakon át juttat el hozzá minden szükséges adatcsomagot. Amint az első adatcsomag megérkezik az újonnan kiépült többesadás ágon, az elérési útválasztó egy *TUNNEL_STOP* üzenettel jelzi az előző útválasztónak, hogy az alagútra már nincs szükség. Ezt természetesen minden egyes többesadás-csoport esetén külön-külön meg kell tennie. Ha a hívásátadás folyamat bármely lépésében csomagvesztés történik, akkor ezt a mobil egységnek kell észlelnie (pl. időzítők segítségével), majd újra kezdeményezni a hívásátadást *(3. ábra)*.

Az MMCAST csomagot két program alkotja. A hozzáférési útválasztókon futó implementáció feladata, hogy nyilvántartsa a kiszolgált mozgó állomásokat és csoportjaikat, továbbítsa a jelzési- és a többesadás csomagokat. További feladata az ideiglenes alagutak létrehozása, megszüntetése, és a hívásátadás jelzésüzeneteinek kezelése. A mozgó állomásokon futó program végzi a hozzáférési útválasztó kiválasztását – automatikus üzemmódban az útválasztó-hirdető üzenetek jel/zaj viszonya, manuális üzemmódban pedig a grafikus felhasználói felülettől (GUI) kapott parancsok alapján. Feladata még a belépés, kilépés, hívásátadás üzene-

3. ábra A hívásátadás üzenetszekvenciája



tek generálása és küldése a hozzáférési útválasztóknak, továbbá az időzítők kezelése a bejelentkezéshez és hívásátadáshoz, valamint az ekkor esetlegesen bekövetkező csomagvesztéskor a csomagok újraküldése. A mozgó állomásokon futó GUI feladatai közé tartozik az összes elérhető hozzáférési útválasztó címének és jel/zaj viszonyának kijelzése, az aktuális hozzáférési útválasztó jelölése. Feladata még a be- és kijelentkezési szándékok jelzése a mozgó állomáson futó programnak, a hozzáférési útválasztó manuális váltásának lehetővé tétele, illetve hívásátadás-mód választás biztosítása.

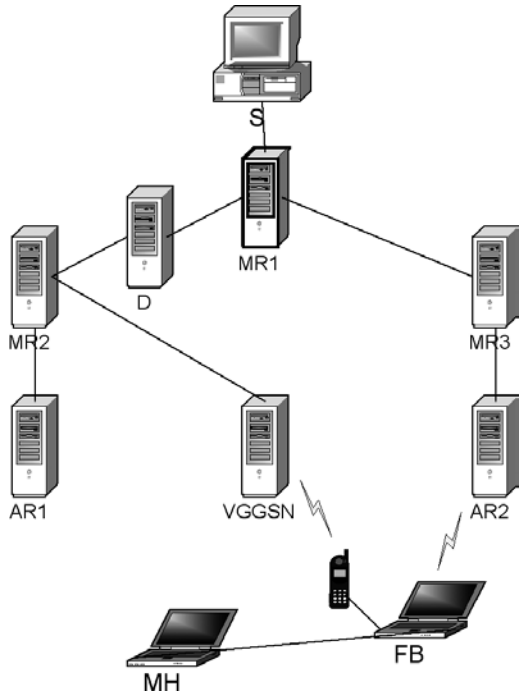
Egyre inkább általános, hogy egy mobil eszköz több hozzáférési technológiát is támogat, ezért protokoll kiegészítésünket úgy terveztük, hogy a zökkenőmentes hívásátadást különböző hozzáférési technológiák között is lehetővé tegye. Ez a gyakorlatban azt jelenti, hogy a mobil egység több különböző típusú hálózati interfésszel rendelkezhet. Az MMCAST lehetővé teszi a váltást a különböző interfészeken keresztül elérhető hozzáférési útvonalválasztók között is, és az MMCAST protokoll paraméterei (például újraadási időzítők) az interfész típusától függően (LAN, WLAN, GPRS) változnak.

A kísérleti hálózat

A megvalósított kísérleti hálózatban *(4. ábra)* két különböző hozzáférési rendszert használtunk: WLAN-t és GPRS-t. A két hozzáférési technológia egységes kezelését a közös IPv6-os hálózati réteg segítségével biztosítottuk. Ez GPRS esetén további problémákat vet fel. Jelenleg a GPRS szolgáltatók nem tudnak csatlakozni IPv6-hoz, hálózataik csak IPv4-es címeket osztanak ki a GPRS terminálóknak. Ráadásul ez sem globális cím, a mobil egységek csak lokális IP címet kapnak a hálózattól.

Ez azt eredményezi, hogy csak a terminál tudja kezdeményezni a kapcsolat felépítését, azt más viszont nem tudja kezdeményezni felé. A GPRS FrontBox architektúra feladata, hogy ezeket a korlátozásokat kiküszöbölve egy olyan virtuális GPRS interfészt valósítson meg a mobil állomáson, amely a valós rádiós interfészekkel teljesen egyenértékű, és (a kisebb sávszélességet és nagyobb késleltetést leszámítva) elrejt minden GPRS specifikus jellemzőt. Hasonló módon az IPv6-os hálózat határán egy ilyen virtuális interfész segítségével olyan virtuális hozzáférési útválasztókat valósítunk meg, amelyek a WLAN hozzáférési útválasztókkal teljesen egyenértékűen kezelhetők.

A VGGSN *(Virtual Gateway GPRS Support Node)* az IPv6-os hálózatban foglal helyet. Rendelkezik egy IPv6-os interfésszel a többesadás útválasztók felé, valamint egy IPv4-essel, ami az Internethez csatlakozik. A VGGSN egy GPRS átjáróként szolgál: a mobil állomások GPRS interfésze és az IPv6-os hálózat között továbbítja a csomagokat. Az IPv6-os hálózat illetve a FrontBox-szal ellátott mobil állomások szemszögéből a



S – többesadás forrás
MRn – többesadás útválasztó
ARn – hozzáférés útválasztó
D – késleltető elem
MH – mobil állomás
VGGSN – virtuális GGSN
FB – FrontBox

4. ábra A teszthálózat

GPRS specifikus jellemzők teljesen rejtve maradnak, a VGGSN ugyanúgy jelenik meg, mint egy közönséges WLAN bázisállomás. A GPRS FrontBox egy GPRS adatátvitelre képes mobil terminál segítségével éri el a GPRS hálózatot, s így az Internetet is. Ahhoz, hogy az IPv6-os csomagokat IPv4-es hálózatán keresztül továbbítsuk, alagutazást használunk a FrontBox és a VGGSN között.

Mivel előre nem ismerjük a dinamikusan kiosztott IP címet, mester-szolga *(master-slave)* elvű alagutat kell használnunk. Ebben az alagútban a mobil állomás és az IPv6-os hálózat csomagjait szállítjuk IPv4-es UDP csomagokban. Az alkalmazott program az alagutat egy virtuális interfészként valósítja meg. Hogy ezt az interfészt a bevezetőben említett módon a valós hálózati interfészekkel teljesen egyenértékűen kezelhessük, az alagúton átviendő csomagokat nem csupán az IPv6-os fejléccel, hanem a csomag adatkapcsolati szintű (MAC) fejlécével együtt csomagoljuk be. Így a többesadás útválasztást ugyanaz az MLD proxy funkciókat ellátó program biztosíthatja, mint a WLAN bázisállomásokon.

Mérési eredmények

A megvalósított protokoll kiegészítés validálásához méréseket végeztünk a bemutatott kísérleti hálózaton. Hogy a protokollunkat összevethessük a távoli felirat-

kozás eredeti módszerével, minden mérést megismételtünk úgy is, hogy az MMCAST alapját képező ideiglenes alagutazást kikapcsoltuk. Mivel kis méretű többesadás fák esetén a fa újraépítéséből adódó késleltetés és csomagvesztés nem jelentős, ezért a nagyobb méretű hálózatok szimulálására kísérleti hálózatunkba beépítettünk egy késleltető elemet. Ez a késleltető elem az interfészeire érkező csomagokat automatikusan továbbítja a másik interfészén, kivéve a lefelé irányuló interfészre érkező PIM (*Protocol Independent Multicast*) [3] csomagokat. Ezeket egy paraméterként megadott idő eltelte után továbbítja.

A WLAN–WLAN hívásátadás-mérés során a csomagkésleltetést és a csomagvesztést vizsgáltuk a hívásátadás különböző fázisaiban a késleltető elem késleltetésének, valamint a csomaggenerátor csomagméretének és csomagküldési periódusidejének függvényében. Amikor nem használtunk ideiglenes alagutazást meglepően nagy csomagvesztést tapasztaltunk. *Méréseink szerint a csomagvesztés mértékét nem befolyásolja sem a csomagküldési gyakoriság, sem a csomagméret. A csomagkésleltető elem késleltetésének értéke és a csomagvesztés időtartama közt viszont közel lineáris összefüggést tapasztaltunk.* A lineáris összefüggés várható volt, mivel amíg a többesadás útválasztó üzenete nem érte el a többesadás fát, nem épülhet ki a fa új ága, s így az adott többesadás csoport üzenetei sem juthatnak el a többesadás útválasztóhoz. Amikor az ideiglenes alagutazást engedélyeztük, a késleltető egység és a csomaggenerátor beállításaitól függetlenül egyáltalán nem tapasztaltunk csomagvesztést.

Érdekes viszont kicsit közelebbről megvizsgálni a csomagkésleltetés értékek alakulását a hívásátadás időpontja körül.

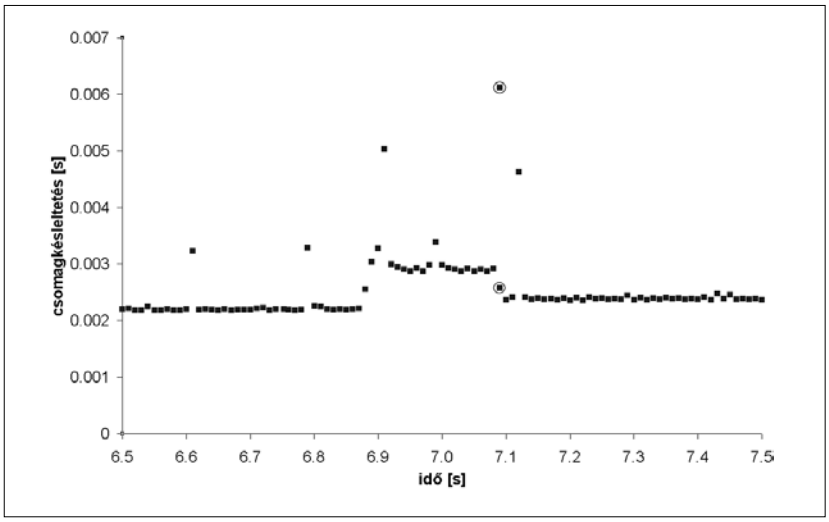
Az *5. ábrán* a csomagkésleltetés szempontjából jól elkülöníthető három fázis: Kezdetben a mobil egység az aktuális bázisállomáshoz csatlakozik, és átlagosan 2.4 ms-os késleltetéssel kapja meg a többesadás csomagokat. Ezután megtörténik a hívásátadás, a mobil állomás kapcsolata megszakad és az új bázisállomáshoz csatlakozik, ez utóbbi a hívásátadás során kiépített alagúton keresztül megkapja a többesadás csomagokat. Az alagutazás enyhén megnöveli a késleltetést, ez a növekedés azonban alig 1ms. A hívásátadást követően a késleltető elemben beállított 200ms elteltével kiépül a többesadás ág. Ekkor ismét lecsökken az átlagos késleltetés értéke, hiszen a csomagok már nem alagúton keresztül érkeznek.

Megfigyelhető, hogy ebben a harmadik fázisban kicsit nagyobb az átlagos késleltetés, mint az elsőben, mivel ez az új útvonal egy ugrással hosszabb a teszthálózatunkban. A mérés során nem volt csomagvesztés, és csupán egyetlen csomag érkezett duplikáltan (ami mind az alagúton, mind közvetlenül megérkezett, az ábrán körrel jelöltük). A duplikált csomag egyébként nem zavarja a kommunikációt, mivel a felsőbb protokoll rétegek (pl. TCP, RTP), vagy maguk az alkalmazások ezt kezelni tudják.

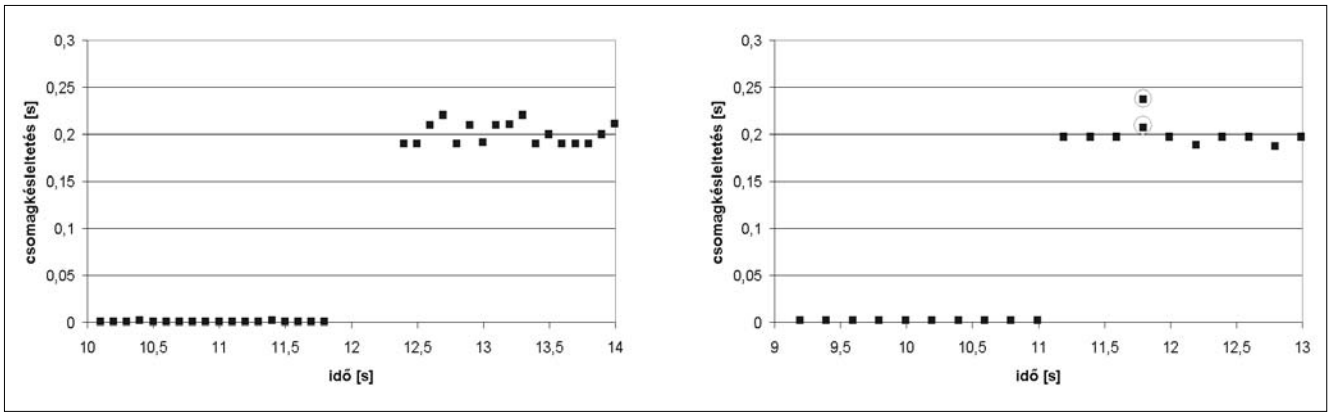
A mérést több különböző csomagméret, csomagküldési gyakoriság, illetve a késleltető elem több késleltetési értéke esetén is megismételtük. Csomagvesztés egyik esetben sem történt, és a duplikált csomagok száma is mindig egy volt. Hálózatunk ugyanis még nagy csomagküldési gyakoriság esetén is túl kicsi ahhoz, hogy az alagútban egyszerre több csomag is utazzon. A csomagkésleltetési görbe három-fázisos jellegét valamennyi esetben meg lehetett figyelni. A csomagméret növelésével lineárisan nőtt mindhárom fázisban a csomagkésleltetés értéke, hiszen egy adott sávszélességű kapcsolaton nagyobb csomag elküldéséhez több idő kell. *A csomagküldési gyakoriság egyáltalán nem befolyásolta eredményeinket. A késleltető elem időzítése pedig csupán az alagutazás időtartamát befolyásolta*, a csomagkésleltetések értékére közvetlenül nem volt hatással.

Végül végeztünk méréseket annak vizsgálatára, hogy mi történik akkor, amikor a mobil egység egyszerre több többesadás adatfolyamra is fel van iratkozva. A késleltetési érékeket ez sem befolyásolta, mivel a protokoll mobil állomásonként egyetlen hívásátadás üzenettel kezeli le az összes többesadás csoport váltását.

5. ábra Csomagkésleltetés hívásátadáskor (alagutazás engedélyezve)



Másik mérési sorozatunk során a technológiák közötti hívásátadást vizsgáltuk. A GPRS-nél felmerül az a probléma, hogy ha túl nagy sávszélességű adatfolyamot küldünk a hálózatra, akkor a szolgáltató hálózatában torlódás alakulhat ki, ami nagy csomagkésleltetést és csomagvesztést okoz. Mivel a szolgáltatói hálózat csomageldobási szabályait nem tudjuk befolyásolni, ezért ott a jelzéscsomagjaink nem élveznek előnyt, így azok is késleltetést szenvednek. Ez ahhoz vezet, hogy az állapotfrissítési üzenetek nem jutnak el a bázisállomáshoz, ezért a rendszer a mobil eszköz eltűnését feltételezi. Ezért ahhoz a megoldáshoz folyamodtunk, hogy a



6. ábra GPRS mérési eredmények

VGGSN-nél 20 kbit/s körüli értékre korlátoztuk a kiküldött többesadás folyamok sávszélességét. Továbbá a GPRS interfészre váltás esetén automatikusan megnöveli újraadási időzítők értékét, és sokkal több újraadást engedélyez, mint WLAN esetén. Ilyen beállítások mellett már sikerült GPRS alatt is átvinnünk egy kis sávszélességű adatfolyamot, és közben technológiák közötti hívásátadást végeznünk.

A hívásátadás vizsgálatához az általunk készített többesadás csomaggenerátor programot használtuk. A programmal különböző hosszúságú csomagokat küldtünk, különböző gyakoriságokkal és a hívásátadás környékén figyeltük a csomagkésleltetési időket. A méréseket elvégeztük az alagutazás engedélyezett és tiltott állapotában is *(6. ábra)*. A mérések során a késleltető elemen 500*ms* késleltetést állítottunk be.

Az ábra első szakaszán a WLAN kapcsolaton keresztül érkeznek a csomagok. Itt körülbelül 2*ms*-os késleltetési értékeket kaptunk. A második szakaszban már a GPRS kapcsolaton keresztül érkeznek a csomagok, jól megfigyelhető a megnövekedett (átlagosan 200*ms*) csomagkésleltetés. A két szakasz közötti részben történik meg a hívásátadás. Az alagutazást nem használó esetben a hívásátadás utáni több mint fél másodperben minden csomag elveszett, az alagutazás engedélyezése esetén viszont nem volt csomagvesztés, csak egy duplikált csomag érkezett (az ábrán körrel jelöltük). Mivel a GPRS átvitel késleltetése több nagyságrenddel nagyobb az alagutazás okozta késleltetésnél, ezért itt nem figyelhető meg a hívásátadás *három fázisos* jellege.

Összefoglalás

A mérési eredmények bebizonyították, hogy a zökkenőmentes többesadás hívásátadáshoz megvalósított protokoll jól működik. Sikerült megvalósítani, hogy egy mobil állomás csomagvesztés nélkül tudjon az egyik hozzáférési útválasztóról a másikra átjelentkezni. Így elérhetjük, hogy a multimédiás alkalmazások a felhasználó számára érzékelhető megszakítás nélkül fussanak, akár mozgás közben is. A kidolgozott protokollkiegészítés a zökkenőmentes hívásátadással pontosan a jobb minőségű és megbízhatóbb szolgáltatások bevezetését teszi lehetővé, a sávszélesség takarékos (a többesadás jellege következtében) kihasználása mellett.

Köszönetnyilvánítás

Ezt a munkát az Európai Unió 5. kutatási és fejlesztési keretprogramjának IST-2001-35125 számú OverDRiVE projektjének [7] keretein belül végeztük. A projektben résztvevő szervezetek: Ericsson, RWTH, Daimler Chrysler, France Télécom, Motorola Inc., RAI, University of Bonn, University of Surrey

Irodalom

[1] Gartner:
„Network Architecture for Real-Time Performance or Cost Savings“,
Gartner Symposium ITXpo 2003,
2003. nov. 3-7., Cannes, Franciaország

[2] S. Deering:
Multicast Listener Discovery (MLD) for IPv6
(IETF RFC 1999 október)

[3] S. Deering:
Protocol Independent Multicast-Sparse Mode
(PIM-SM) (IETF RFC 1998. június)

[4] D. Johnson, C. Perkins, J. Arkko:
”Mobility support in IPv6”,
Internet-Draft, draft-ietf-mobileip-ipv6-21.txt,
(2003 február)

[5] szerk: Yu Ming Tian:
Current Approaches to IP Multicast in
a Mobile Environment,
www.comnets.rwth-aachen.de/~o_drive/index.html
(2002. november)

[6] Bill Fenner:
IGMP/MLD-based Multicast Forwarding,
draft-ietf-magma-igmp-proxy-04.txt
(Internet draft, 2003 szeptember)

[7] European Commission –
Information Technologies Programme,
http://www.ist-overdrive.org/

CCK eljárás alkalmazása a vezetéknélküli hálózatokban

JUHÁSZ ÁKOS, DR. EGED BERTALAN

BME Szélessávú Hírközlő Rendszerek és Villamosságtan Tanszék,
Vezetéknélküli Információtechnológia Laboratórium

akos.juhasz@wit.mht.bme.hu, bertalan.eged@wit.mht.bme.hu

Kulcsszavak: IEEE 802.11b fizikai réteg, CCK (Complementary Code Keying) eljárás, zavarvédelem, komplementer kódok

A világ fejlődésével a távközlés mind fontosabb szerepet kap az élet minden területén. A technikai fejlődés hatására megjelenő újítások újabb igényeket és elvárásokat gerjesztenek, melyeket a fejlődés következő lépései igyekszenek kielégíteni. Az elmúlt évek során a kommunikációs technológiák fejlődésében jelentős fordulópontot hozott a mobilitás igényének megjelenése. A jól bevált és megszokott fix összeköttetések számos feladat megvalósítására alkalmatlanná váltak. Az élet mind több területén kezdte meg térhódítását valamilyen mobil technológia, ezzel új lehetőségeket és kihívásokat állítva mind az eszközök fejlesztői, mind pedig a rendszerek tervezői elé.

Bevezetés

A mobilitás fontosságát a mai rohanó élet során nem lehet eléggé hangsúlyozni. Az élet minden területén találkozhatunk vele mikor laptopot, mobiltelefont, PDA-kat vagy egyéb hasonló eszközöket használunk. Természetesen nem elég magukat az eszközöket mobilissá tenni, hanem sok esetben biztosítani kell ezen eszközök számára a kommunikáció lehetőségét is. Ezzel eljutottunk a vezeték nélküli kommunikáció fontosságához.

A vezeték nélküli kapcsolatoknak igen sok előnye van. Sok esetben van szükség nagyobb távolságot áthidaló kapcsolatra olyan helyeken, ahol a kábelépítés különböző okokból nem megvalósítható, vagy komoly problémákba ütközne. Ilyen esetekben fix telepítésű vezeték nélküli eszközök használatára van szükség. A már említett mobil eszközökhöz azonban olyan kommunikációs technológiák alkalmazására van szükség, amelyek alkalmasak mind a vezeték nélküli átvitel, mind pedig a mozgó terminálok okozta problémák leküzdésére.

A vezeték nélküli kommunikáció legnagyobb problémája az átviteli közeg használatából adódó zavarhatóság. Zavarforrásnak tekinthetünk az átviteli közegben lévő minden olyan jelet, melynek frekvenciatartománya, irányítottsága stb. olyan, ami rendszerünk jeleit módosítani képes.

Ezek a jelek származhatnak természetes forrásokból, más elektromos eszközökből; sőt, ilyen zavarjel lehet egy másik vezeték nélküli rendszer is. Az alkalmazott modulációs eljárások és technológiák egyik legfontosabb jellemzője az ezen zavarokkal szembeni ellenálló képessége.

Az IEEE 802.11 az egyik leginkább elterjedt vezetéknélküli hálózati technológiákat definiáló szabványcsalád. Nézzük most meg, az alap szabvány által definiált fizikai réteget, valamint a használt rádiós csatornát.

Az IEEE 802.11 fizikai rétege

Az 802.11-es szabványt először 1997 szeptemberében ismertette az IEEE. Tudnunk kell, hogy a szabványcsoport több változtatáson ment át azóta, mely módosításokat különböző betűkkel jelölik (pl. 802.11a – 5GHz, OFDM; 802.11b – 2.4GHz, CCK kiegészítés; 802.11g, 2.4GHz, OFDM és CCK kompatíbilis).

A szabvány először a 2.4GHz-es frekvenciára tervezett WLAN eszközök működési paramétereit definiálta. A 2.4GHz-es ISM sáv 83.5MHz széles (2.4-2.4835GHz). Ezen frekvenciasávot a szabvány 13 egymást átfedő, egyenként 22MHz sávszélességű csatornára osztja, melyek középfrekvenciájának távolsága egyenként 5MHz. Ennek megfelelően e tartományban 3 át nem lapolódó csatornát biztosíthatunk. Párhuzamos rendszerek tervezésekor használhatunk átlapolódó csatornákat is, azonban számolnunk kell azzal, hogy így a két rendszer interferenciájából adódó zavar önmagában csökkentheti az elérhető adatátviteli sebességet.

Mivel a definiált frekvenciasáv ISM sáv, ezért a szabvány spektrumkiterjesztést (spreed spectrum) definiál a rendszer zavarhatóságának és a rendszer által keltett zavarok csökkentésére. A szabvány lehetővé teszi mind a direkt szekvenciális (DSSS), mind pedig a frekvenciaugratásos (FHSS) sávkiterjesztést is.

Az IEEE 802.11 által definiált FHSS eljárást alkalmazó eszközök GFSK modulációt alkalmaznak. Az így elérhető adatátviteli sebességek 1MB/s (2GFSK) és 2 MB/s (4GFSK). Mára a kereskedelemben kapható eszközök között a DSSS eljárást alkalmazó eszközök teljes mértékben kiszorították az FHSS eljárást, a továbbfejlesztések is a DSSS vonalon folytatódtak.

A direkt szekvenciális spektrumszórás esetében 11 chipes (a szakirodalomban a szórókód 1 bitjét nevezik chipnek) barker kódot definiáltak spektrum-kiterjesztő kódként valamennyi üzemmódban, így a chipsebesség 11MBit/s lesz minden esetben. Az alkalmazott modulációk által elérhető adatátviteli sebesség az FHSS rend-

szerekhez hasonlóan itt is 1 és 2MB/s lett. Ennek biztosításához DBPSK és DQPSK modulációt írtak elő.

A rendszerek mindkét esetben képesek az adatátviteli üzemmódok között automatán váltani, így zajosabb környezetben az átvitel stabilitása érdekében automatikusan kisebb lesz az elérhető adatátviteli sebesség. A fejléc legfontosabb részei definíciószerűen csak a legnagyobb zavartűrésű üzemmóddal továbbíthatóak (1MB/s, DBPSK), ezzel is csökkentve a csomag meghibásodásának valószínűségét. Természetesen ez magával vonja azt, hogy a rendszernek egyetlen rádiós csomag továbbítása közben is képesnek kell lennie az üzemmód változtatására!

A technológia és a követelmények szigorodásának következtében a mobil hálózatok viszonylag hamar kinőtték a rendszerek által biztosított kereteket – leginkább a korlátozott adatátviteli sebességet – így újabb fejlesztésekre volt szükség a minőség javításához. Nagyobb adatsebességű eljárás konstruálására (802.11 HR) több próbálkozás is történt.

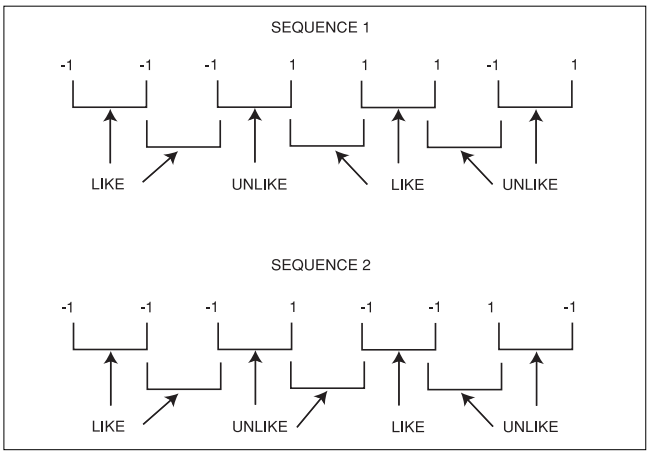
Kísérleteztek a BCPPM (Barker Code Pulse Position Modulation), MBOK (M-ary Bi-Orthogonal Keying), OFDM (Orthogonal Frequency Division Multiplex), OCDM (Orthogonal Code Division Multiplex) eljárásokkal is, azonban végül a CCK (Complementary Code Keying) eljárás váltotta be a hozzá fűzött reményeket.

Komplementer kódok

A CCK eljárás alapjait a komplementer kódok elméletében kell keresnünk. A bináris komplementer kódok egy sokkal általánosabb kódhalmazból, a többfázisú kódokból származtathatóak. (Az IEEE802.11 CCK eljárása ezeket a többfázisú kódokat alkalmazza.)

A komplementer kódokat először infravörös spektrometriában alkalmazták, de jó tulajdonságaik miatt radar applikációkban és OFDM eljárásokban is elterjedtek. Egyetlen alkalmazásban sem használták a komplementer kódokat olyan módon, ahogyan a 802.11 CCK eljárásában. Definíció szerint a komplementer kódok olyan kódpárokat jelentenek, melyek egyikében lévő hasonló bitpárok száma (bármilyen közzel véve) megegyezik a másik kódban lévő nem hasonló bitpárok számával.

Erre láthatunk egy egyszerű példát a *fenti ábrán*. Ebben a példában az első sorozatban 4 hasonló bitpár



van, míg a második sorozatban 4 nem hasonló bitpárt fedezhetünk fel. Táblázatba foglalva az egyes hasonló bitpárok számát különböző közzel véve a következő eredményt kapnánk:

Vizsgált bitek távolsága	1. Szekvencia		2. Szekvencia	
	hasonló	nem hasonló	hasonló	nem hasonló
1	4	3	3	4
2	4	3	3	4
3	1	5	5	1

Ebből tehát látható, hogy a komplementer kódokban egy erős szimmetria rejlik. Ennek nagy előnye, hogy a periódikus autókorrelációs vektora (kódszó és eltolt kódszó szorzata) ezen vektoroknak mindenhol nulla, kivéve a nulla eltolást.

Az elmondottakat matematikailag a következőképpen írhatjuk le:

$$c_j = \sum_{i=1}^{n-j} a_i a_j + j \qquad d_j = \sum_{i=1}^{n-j} b_i b_j + j$$

ahol *n* a kódszó hossza, *a* és *b* pedig a két komplementer szekvencia.

Ideális esetről akkor beszélhetünk, ha

$$c_j + d_j = 0, \quad j = 0 \quad \text{és} \quad c_0 + d_0 = 2n.$$

Az ideális esetet általában nehéz megvalósítani, de jó kódokról beszélhetünk, ha csupán egy csúcsértéke van az autókorrelációs vektornak több kis csúccsal.

A fent említett két kódsorozatot vizsgálva megállapíthatjuk, hogy ezek tökéletes komplementer kódok:

Vizsgált bitek távolsága	1. Szekvencia									2. Szekvencia									
	kód								Cj	kód								Dj	Cj+Dj
0	-1	-1	-1	1	1	1	-1	1	8	-1	-1	-1	1	-1	-1	1	-1	8	16
1	1	-1	-1	-1	1	1	1	-1	0	-1	-1	-1	-1	1	-1	-1	1	0	0
2	-1	1	-1	-1	-1	1	1	1	0	1	-1	-1	-1-	1	1	-1	-1	0	0
3	1	-1	1	-1	-1	-1	1	1	-4	-1	1	-1	-1-	1	-1	1	-1	4	0
4	1	1	-1	1	-1	-1	-1	1	0	-1	-1	1	-1	-1	-1	-1	1	0	0
5	1	1	1	-1	1	-1	-1	-1	-4	1	-1	-1	1	-1	-1	-1	-1	4	0
6	-1	1	1	1	-1	1	-1	-1	0	-1	1	-1	-1	1	-1	-1	-1	0	0
7	-1	-1	1	1	1	-1	1	-1	0	-1	-1	1	-1	-1	1	-1	-1	0	0

Többfázisú komplementer kódok

A többfázisú komplementer kódok olyan szekvenciákat tartalmaznak, melyek szintén komplementer tulajdonságokkal rendelkeznek, azonban elemeinek fázis paraméterei is vannak.

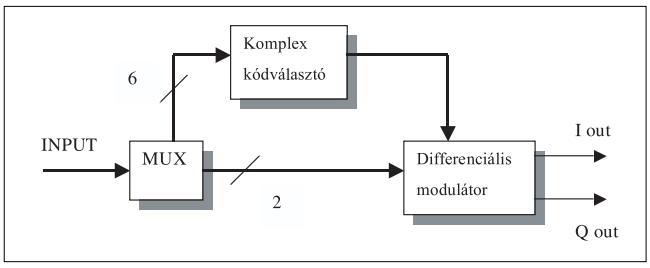
A 802.11b által definiált kódkészlet komplex komplementer kódokat tartalmaz, tehát az elemei komplex számok.

A 802.11b szabvány, CCK kiegészítés

Az átviteli sebesség növelésére tett kísérletek eredményeképpen az IEEE 1999 szeptemberében bejelentette a 802.11 szabvány 'b' kiegészítését, melyben a már meglévő adatátviteli üzemmódokat további két üzemmóddal egészítették ki, így az elérhető maximális adatátviteli sebesség 11Mb/s-ra nőtt. A két új üzemmódban CCK eljárást írtak elő, melyekben ugyan azt a chipsebességet és spektrumszélességet használja a rendszer, mint a barker kóddal történő spektrum-kiterjesztés esetén.

A CCK eljárás egy 64 elemű kódmodulációs eljárásnak is tekinthető, melyben a spektrum-kiterjesztő kód egy 64 elemű közel ortogonális vektorhalmazból kerül kiválasztásra. A kiválasztott 8 bit hosszúságú komplex (QPSK) vektor ennek megfelelően 6 bit információ átvitelére alkalmas. További 2 bit információ átvitelére ad lehetőséget a moduláció, mellyel előállítható a QPSK szimbólum.

Ennek megfelelően egy CCK adó egység elvi felépítése a következőképpen vázolható:



CCK moduláció, adó áramkör elvi felépítése

Az így kialakított szimbólum azonban mindössze 8 chip hosszúságú, így nem használja ki teljesen a 802.11 szabvány által definiált rádiós csatornát, ehhez 11 chip hosszúságú spektrum-kiterjesztő kódra lenne szükség. Ennek eléréséhez a szimbólumsebesség 1.375-szörös növelésére van szükség. A rendszerrel elérhető adatátviteli sebesség elvi maximuma tehát 11Mbit/s lett, miközben a definiált 22MHz szélességű átviteli csatornát megfelelően kihasználjuk.

Az eljárást leíró formula az alábbiak szerint alakul:

$$c=\left\{e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)},e^{j(\varphi_1+\varphi_3+\varphi_4)},e^{j(\varphi_1+\varphi_2+\varphi_4)},-e^{j(\varphi_1+\varphi_4)},e^{j(\varphi_1+\varphi_2+\varphi_3)},e^{j(\varphi_1+\varphi_3)},-e^{j(\varphi_1+\varphi_2)},e^{j\varphi_1}\right\}$$

A formulából látható, hogy az egyes chipeket 4 különböző fázistényező határozza meg. Az első mindegyik chipet modulálja, ennek megfelelően ez definiálja a QPSK forgatását az egész kódvektornak (ezt a fázistényezőt határozza meg az adatból leválasztott két bit). A második tényező minden páratlan chipet, a harmadik minden páratlan chippárt, míg a negyedik az első négy chipet modulálja.

A megfelelő fázis paraméterek kiválasztása a 8 adatbitből a következőképpen történik:

Adat	Fázis paraméter
(d_1,d_0)	φ_1
(d_3,d_2)	φ_2
(d_5,d_4)	φ_3
(d_7,d_6)	φ_4

Nézzünk most is egy példát!

Tegyük fel, hogy az átvinni kívánt adatbájtunk

d[7…0]=1,0,1,1,0,1,0,1

Ezzel a fázisértékek:

d1,d0 = 0,1 tehát φ1 = π;
d3,d2 = 0,1 tehát φ2 = π;
d5,d4 = 1,1 tehát φ3 = -π/2;
d7,d6 = 1,0 tehát φ4 = π/2;

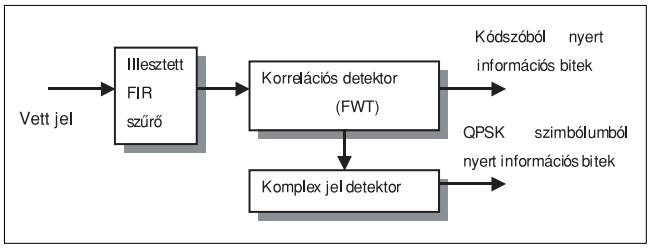
Ezeket a fázisértékeket a formulába helyettesítve a következő kódszót kapjuk:

$$c=\left\{e^{j2\pi},e^{j\pi},e^{j\frac{5\pi}{2}},-e^{j\frac{3\pi}{2}},e^{j\frac{3\pi}{2}},e^{j\frac{\pi}{2}},-e^{j2\pi},e^{j\pi}\right\}$$
$$=\{1,-1,j,j,-j,j,-1,-1\}$$

A 802.11b kiegészítés két adatátviteli sebességű üzemmóddal bővíti a szabványt. Az 5.5Mbit/s-ot az előzővel megegyező CCK eljárással éri el. A kisebb adatátviteli sebességet úgy érhetjük el, ha a már definiált CCK szimbólummal kevesebb információs bitet viszünk át. Ennek megvalósítását a komplex kódválasztó limitálásával érhetjük el. A 64 kódszóból megfelelő módon kiválasztva 4-et a szórókóddal átvihető információ 2 bitre csökken, azaz a teljes szimbólum csupán 4 bit információt fog hordozni, tehát az adatátviteli sebesség a felére csökken.

A CCK vevő áramkör felépítése egy korrelációs detektor alkalmazását igényli, azaz egyfajta Rake vevőt megvalósítva tudjuk a legegyszerűbben dekódolni a vett jelet. Az így kialakított áramkör blokkvázlata a *következő oldali ábrán* látható.

A vett jel egy illesztett FIR szűrőn átengedve egy FWT (Fast Walsh Transform) egységbe kerül. Ez az egység azért használható jól, mert ezekben kódokban WALSH tipusú struktúra rejlik. (Bár lehetséges lenne több komplementer kódszót is találni ezzel a 8 chippel,



CCK moduláció, vevő áramkör elvi felépítése

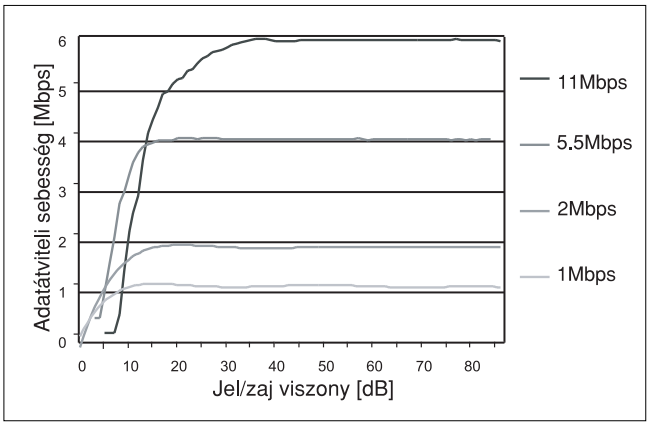
de ezeket nem lehetne FWT-vel dekódolni.) Az FWT egység két fő részre bontható funkció szerint. Az első részben annyi korrelátor kap helyet, ahány lehetséges szórókódot alkalmazhatunk, míg a második rész egy BP (Biggest Picker) áramköri egység, mely a bemenetei közül a kiválasztja a legnagyobbat.

Ennek megfelelően megérthető az egység működése is. A bejövő szimbólumot minden korrelátor megkapja egyidejűleg, így mindegyik kimenetén megjelenik egy mennyiség, mely arra utal, hogy az adott korrelátor által vizsgált szórókód mennyire hasonlít a szimbólumnál alkalmazotthoz. A BP áramkör ezek közül kiválasztja a legnagyobat, mivel ezek alapján ennek a szórókódnak volt a legnagyobb valószínűsége. Az így visszaállított QPSK szimbólum fázisának meghatározásával előállíthatjuk az adóban leválasztott 2 bitet, azaz visszaállítható az eredeti adatfolyam.

Összefoglalás

Megállapítható tehát, hogy a CCK eljárás lényegében véve egy MOK (M-ary Orthogonal Keying) szerű moduláció, melyben a használt kódok komplex szimbólum struktúrát alkotnak. A CCK használatával a 802.11 által definiált vezetéknélküli rendszer bővülhetett két nagyobb adatátviteli sebességű üzemmóddal, melyek a már definiált csatornán képesek továbbra is üzemelni, tehát a rendszer visszafelé kompatíbilis maradt.

Végezetül nézzünk meg egy Lucent Silver WLAN kártyával vizsgált adatátvitelt, melyből kiderül, hogy a CCK-t használó két újabb üzemmód valóban jelentős sebességnövekedést eredményezett. Észrevehető azonban, hogy mind az 5.5 Mbit/s, mind pedig a 11Mbit/s üzemmód adatátviteli sebessége jelentősen elmarad az elméleti határértéktől. Ennek az oka a protokollrendszerben rejlik. Mivel az eszközöket visszafelé kompatibilisen alakították ki, így sajnálatos módon az új üzemmódok biztosította gyors adatátvitelt csak a csomag tényleges adatrészénél lehet kihasználni, így hatásossága csökken.



Természetesen – ahogy az a *grafikonon* mutatott mérési eredményekből is látszik – a nagyobb adatátviteli sebességet biztosító üzemmódok és modulációs eljárások jobb jel-zaj viszonyt igényelnek a hibamentes demodulációhoz.

Irodalom

[1] Golay, Marcel J. E.:
„Complementary Series”,
IRE Transactions on Information Theory,
1961. április
[2] Sivaswamy, R.:
„Multiphase Complementary Codes”,
IEEE Transactions on Information Theory,
1978. szeptember
[3] Frank, Robert L.:
„Poliphase Complementary Codes”,
IEEE Transactions on Information Theory,
1980. november
[4] Bob Pearson:
„Complementary Code Keying Made Simple”,
Intersil, Application note, 2000. május
[5] Robert C. Dixon:
Spread Spectrum Systems with Commercial Applications
[6] Spread Spectrum Scene at www.sss-mag.com.
[7] D. Duchamp, N. F. Reynolds:
Measured performance of a wireless LAN.
In Proceedings of the 17th Conference on Local Computer Networks,
pp.494–499. IEEE, September 1992.
[8] B. Tuch:
Development of WaveLAN, an ISM band wireless LAN
AT&T Technical Journal, pp.27–37, July/Aug. 1993.
[9] Lucent Technologies, WaveLAN IEEE 802.11
PC Card User’s Guide

Kooperációra ösztönző mechanizmusok többugrásos vezeték nélküli hálózatokban

BUTTYÁN LEVENTE, HOLCZER TAMÁS, SCHAFFER PÉTER

CrySyS Laboratórium (Laboratory of Cryptography and System Security)
BME Híradástechnikai Tanszék

{buttyan, holczer, schafi}@crysys.hu

Reviewed

Kulcsszavak: díjazás, cellás hálózat, számlaalapú ösztönzés, biztonság, kriptográfia

Cikkünkben bevezetjük a kooperációra való ösztönzés problémáját, ami tipikus problémaként jelentkezik a többugrásos vezeték nélküli hálózatokban. Röviden áttekintetjük a nem-kooperatív viselkedési fajtákat, és a kooperációra ösztönző mechanizmusok típusait. Végül összefoglaljuk két általunk javasolt ösztönző mechanizmus főbb elemeit, ötleteit.

1. Bevezetés

Az elmúlt évtizedben a számítógépes technológia hatalmas fejlődésen ment keresztül. Ez a fejlődés egyrészt a hagyományos számítógépek teljesítményének növekedésével járt, másrészt olyan új számítógépes eszközök és alkalmazások létrehozásának technikai feltételét teremtette meg, melyek jelentős mértékben megváltoztatják az informatika és a távközlés ma ismert arculatát. A számítógép, mint önálló eszköz mellett megjelentek és fokozatosan túlsúlyba kerülnek az „intelligens tárgyak", melyekben a számítógép beágyazott célhardver formájában van jelen. A modern telefonkészülékekben, autókban, háztartási eszközökben, bankkártyákban már ma is megtalálható a beágyazott számítógép, és ez a kör a jövőben még tovább bővül majd. A számítógépes technológia a szó szoros értelmében mindenhol jelen lesz majd *(ubiquitous computing)*.

A mindütt jelenlevő számítástechnika víziója nagy hatást gyakorol az informatika és a távközlés területén folyó kutatás egészére. Ennek kapcsán került a kutatás előterébe többek között a többugrásos *(multi-hop)* vezeték nélküli hálózat fogalma. Ezen hálózatok reprezentáns képviselője az úgynevezett ad hoc hálózat [5], melyben a résztvevők előre telepített hálózati infrastruktúra igénybevétele nélkül, önszervező módon hozzák létre és működtetik a hálózatot. Infrastruktúra hiányában az alapvető hálózati funkciókat maguk a résztvevők látják el. Ennek megfelelően, a kommunikáció többugrásos vezetéknélküli kommunikációra épül, ahol két távoli kommunikáló fél forgalmát más, földrajzilag a két kommunikáló fél között elhelyezkedő résztvevők továbbítják. Az adatforgalom továbbításán kívül a résztvevők egyéb hálózati szolgáltatást is nyújthatnak egymásnak. Alapvető tulajdonságainál fogva – ezen belül is a fix infrastruktúrától való függetlenségének köszönhetően – az ad hoc hálózati technológia várhatóan fontos szerephez jut majd a jövőben, mint a mindenütt jelenlevő számítástechnika vízióját támogató új generációs hálózati technológia.

Az ad hoc hálózati technológia számos biztonsággal kapcsolatos problémát vet fel [3].

Ezen problémák alapvetően két csoportba sorolhatók. Egyrészt az adatbiztonság és az adatvédelem hagyományos problémáit (hitelesítés, integritás védelem, titkosság, rendelkezésre állás, anonimitás stb.) kell egy teljesen új környezetben – azaz új feltevések mellett – megoldani. Másrészt számos eredendően új biztonsági probléma is felmerül, mely a hagyományos informatikai és távközlési rendszerekben egyszerűen nem létezik, vagy csak elhanyagolható mértékben van jelen.

A BME Híradástechnikai tanszékén, a CrySyS Laboratóriumban mindkét csoport problémáit vizsgáljuk kutatási programunk keretében (részletes leírást lásd a *www.crysys.hu* oldalon). Ezen cikk keretein belül azonban csak egy speciális problémával, nevezetesen a kooperációra való ösztönzés problémájával foglalkozunk.

Az ad hoc hálózat működése – és így az általa nyújtott szolgáltatások rendelkezésreállása is – arra a feltevésre épül, hogy a hálózat résztvevői kooperatívan viselkednek, azaz hajlandóak egymás számára szolgáltatásokat nyújtani. Ezt azonban semmi nem garantálja. Éppen ellenkezőleg: mivel a kooperatív viselkedés szolgáltatások nyújtását (pl. mások csomagjainak továbbítását) jelenti, ami viszont energiafogyasztással jár, a tipikusan telepről üzemelő résztvevők telepük élettartamának növelése érdekében esetleg megtagadhatják az együttműködés. Annál is inkább, mert a kooperatív viselkedés önmagában még nem garantálja egy adott résztvevő számára, hogy a többi résztvevő is kooperativan fog viselkedni vele szemben. Valójában, egy önző résztvevő parazita módon kihasználhatja a hálózat kooperáló résztvevőit saját csomagjainak továbbítására anélkül, hogy ő maga egyetlen csomagot is továbbítana (vagy egyéb szolgáltatást nyújtana) mások számára. Ezért fontos valamilyen kooperációra ösztönző mechanimus bevezetése a hálózatba. Hasonló jellegű probléma hagyományos hálózatokban lényegében nem létezik.

Jelen cikkben először osztályozzuk a nem-kooperatív viselkedés fajtáit, majd röviden áttekintjük a kooperatív viselkedésre ösztönző megoldások típusait és azok jellemzőit. Végül összefoglaljuk két általunk javasolt megoldás főbb elemeit, ötleteit.

2. A nem-kooperatív viselkedés osztályozása

A nem-kooperatív viselkedésnek több fajtája is létezik, melyeket a következő módon osztályozhatjuk [10]:

Indokolt nem-kooperatív viselkedés.

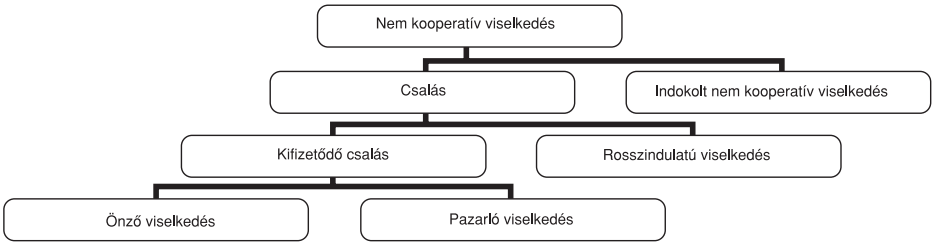
Az erőforrások szűkösségéből adódó nem-kooperatív viselkedés lehet átmeneti vagy állandó, attól függően, hogy az erőforrás hiánya átmeneti e vagy állandó. Állandó hiány akkor lép fel, ha az eszköznek nem áll rendelkezésére az erőforrás, például ha nincs elég számítási kapacitása vagy memóriája. Átmeneti hiány akkor léphet fel, ha például hirtelen nagy forgalom zúdul rá. Ezekben az esetekben az ösztönző mechanizmusnak nem szabad büntetnie az eszközt. Ehhez fel kell ismerni az indokolt nem-kooperatív viselkedést, és meg kell azt különböztetni az indokolatlan nem-kooperatív viselkedéstől.

Rosszindulatú viselkedés.

A rosszindulatú viselkedés egy nem kifizetődő viselkedési forma, ezért csak akkor fordulhat elő, ha egy magasabb rétegnek az előnyös. Például egy hírnév alapú hálózatban rágalmazó üzeneteket küldeni nem kifizetődő a hálózati réteg számára, viszont jó lehet az alkalmazási réteg számára, ha ezzel egy vetélytársát ki tudja zárni a hálózatból.

Önző és pazarló viselkedés.

Az önző és a pazarló viselkedés kifizetődő viselkedési forma. Egy forrás pazarlóan viselkedik, ha elárasztja a hálózatot fölösleges üzenetekkel, míg egy továbbító eszköz önző, ha nem továbbít csomagokat, pedig lenne rá módja.



Ebben a cikkben elsősorban az önző viselkedés megakadályozását célzó ösztönző sémákkal foglalkozunk.

3. Ösztönző sémák díjazási típusai

Az ösztönző sémák legfontosabb eleme a díjazás. A megbízó fizet a megbízottnak, hogy az számára valamilyen feladatot elvégezzen, például számításokat hajtson végre vagy csomagokat továbbítson. A díjazásnak két alapvető típusa terjedt el széles körben: a *hírnév alapú* és a *számla alapú* díjazás.

Hírnév alapú díjazás esetén a térítés mértéke függ az entitás hírnevétől. Az *A* entitás szempontjából a *B* entitás hírneve *A*-nak *B*-vel kapcsolatos tapasztalataiból és a többi entitás *B*-vel kapcsolatos tapasztalataiból ered. Az *A* entitás *B*-vel kapcsolatos bizalmát pedig *B* hírneve határozza meg dinamikus bizalmi séma alkalmazásával. Egy entitás hírneve csak a vele korábban kapcsolatba került entitások által ismert, illetve a hírnév szétárasztása által a környező entitások is ismerhetik. Ebből látható, hogy a jó hírnév csak stabil vagy lokalizált interakciós minták esetén kifizetődő. Hírnév alapú díjazási séma használata esetén a díjazásban való megegyezés fázisa kimarad, mivel a térítés mértékét a megbízó egyedül határozza meg. A hírnév valódi pénzzé konvertálása egyelőre nem megoldott, így ezen séma pénzügyi alkalmazása erősen korlátozott. Hírnév alapú ösztönzési sémákra számos példa található az irodalomban (pl. [2, 9]).

Számla alapú díjazás esetén minden entitás rendelkezik egy számlával egy virtuális banknál. A megbízó minden tranzakciónál kibocsát egy csekket, mellyel a megbízott a virtuális bank közreműködésével visszatérítést kap az elvégzett feladatokért. A bank elérhetősége előfeltétele a módszer helyes működésének, ezért szokás azt több kisebb lokális bank csomópontra partícionálni. Előfordulhat, hogy az entitás maga tárolja a saját számláját. Ehhez olyan modulokat kell az entitásokba beépíteni, melyek minden szempontból megbízhatóak. A számla alapú díjazás egy statikus bizalmi séma. Mivel minden entitás saját számlával rendelkezik, egyszerű a díjak valódi pénzzé átváltása. A probléma az lehet, hogy a számla alapú díjazás vagy megbízható hardverre, vagy a bank csomópontok elérhetőségére épít, s ez ad hoc hálózatokban külön nehézségeket jelent. Számla alapú ösztönző sémákra is számos példa található (pl. [1, 4, 6, 12]). Ezek közül kettőt részletesebben is bemutatunk a következő fejezetben.

4. Példák számla alapú ösztönzési sémákra

4.1. Csomagtovábbítás ösztönzése tiszta ad hoc hálózatokban

A [4]-ben egy olyan módszert javaslunk a kooperatív viselkedés ösztönzésére, mely számla alapú díjazásra épül és nem használ virtuális bankot (azaz az eszközök tárolják a saját számlájukat). Ehhez természetesen biztosítani kell valamilyen fizikai hozzáférésvédelmet, ami megakadályozza, hogy az eszköz gazdája hozzáférjen az eszközön tárolt számlához és manipulálni tudja azt.

Egy lehetséges megoldás az lenne, ha az egész eszköz manipulálás-ellenálló hardverre épülne, ám ez nehezen kivitelezhető és drága is. Az általunk javasolt megoldás csak annyit követel meg, hogy minden eszköz rendelkezzen egy manipulálás-ellenálló hardver modullal. Ez nem teljesíthetetlen követelemény, hiszen a mai mobil telefonokban is van ilyen modul, mégpedig a SIM kártya. A továbbiakban az eszközökben található manipulálás-ellenálló modult *biztonsági modulnak* nevezzük. A biztonsági modulról tehát azt feltételez-

zük, hogy az abban futó programok működését az eszköz gazdája nem tudja módosítani, azaz azok helyesen, az előírt protokollnak megfelelően működnek. Ugyanakkor megengedjük, hogy az eszköz gazdája az eszköz biztonsági modulon kívüli részének működését teteszőlegesen módosítsa. Az általunk javasolt megoldás azonban biztosítja, hogy az eszköz gazdájának semmi haszna nem származik az eszköz működésének módosításából, ezért feltehetően csak ritkán fog élni ezzel a lehetőséggel. Ezt a kritikus és nem kritikus funkciók körültekintő szétválasztásával és megfelelő kriptográfiai protokollok alkalmazásával érjük el.

A biztonsági modulra épülő ösztönző séma működését a következő módon foglalhatjuk össze röviden. Minden eszköznek van egy számlálója, melyet a biztonsági modul kezel, így ahhoz az eszköz gazdája nem fér hozzá. Ezt a számlálót *nuglet* számlálónak nevezzük. Mikor az eszköz egy saját csomagot szeretne küldeni, akkor azt először át kell adnia a biztonsági modulnak, ami egy kriptográfiailag védett fejlécet generál a csomag számára. Ezen kívül, a biztonsági modulban fut az útvonalválasztó algoritmus is, és így a modul meg tudja állapítani (vagy becsülni), hogy hány eszközön kell majd a csomagnak áthaladnia, amíg megérkezik a címzetthez. Jelöljük a szükséges továbbító eszközök (becsült) számát *n*-nel. Mielőtt a biztonsági modul kiadná a csomag elküldéséhez szükséges biztonsági fejlécet, ellenőrzi, hogy a nuglet számláló értéke nem kisebb-e, mint *n*. Ha igen, akkor a csomagot nem lehet elküldeni (nincs rá fedezet), és így a biztonsági modul nem adja ki a fejlécet az eszköz számára. Ha a nuglet számláló értéke nagyobb, mint *n*, akkor a biztonsági modul *n*-nel csökkenti azt, majd kiadja a fejlécet az eszköznek.

Ezek után az eszköz elküldi a csomagot a biztonsági fejléccel együtt. Minden továbbító eszköz a biztonsági fejléccel együtt átadja a csomagot a saját biztonsági moduljának. A modul csak akkor fogadja el a csomagot, ha a fejlécben található kriptográfiai ellenőrzőösszeg helyes. Ekkor a biztonsági modul új fejlécet generál a csomaghoz, melyet majd a következő továbbító eszköz biztonsági modulja fog ellenőrizni, és átadja az új fejlécet a továbbító eszköznek. Ezen kívül, a biztonsági modul feljegyzi, hogy a megelőző eszköznek (ha az nem maga a forrás volt) jár egy nuglet a csomag továbbításáért. Ezeket a feljegyzéseket minden szomszédra külön összegezve nyílvántartja a biztonsági modul, majd minden szomszéddal periodikusan futtat egy nuglet szinkronizációs protokollt, melynek segítségével a két szomszéd kiegyenlíti „tartozásait” egymás felé.

Vegyük észre, hogy egy továbbító eszköz csakis akkor kaphat fizetséget a csomag továbbításáért, ha valóban továbbította azt, hiszen mindig a következő eszköz biztonsági modulja jegyzi fel a továbbításért járó nuglet-et, ehhez azonban a csomagnak épségben meg kell érkeznie a következő eszközhöz. Azt is vegyük észre, hogy ha a csomag fejléce helytelen (vagy hiányzik), akkor a biztonsági modul nem fogadja el a csomagot, és így a továbbító eszköz nem kapja meg a továbbításért járó nuglet-et. Ezért egyetlen eszköznek sem áll érdekében fejléc nélküli vagy hibás fejlécű csomagot továbbítani. A csomag forrása tehát nem kerülheti el, hogy a csomagot elküldés előtt átadja a biztonsági moduljának (hiszen csak az tudja a megfelelő fejlécet generálni) és ezzel együtt fizessen a csomag elküldéséért.

A fent leírt ösztönző séma működését szimulációval elemeztük (a részleteket lásd [4]-ben). A szimulációban minden eszköz konstans átlagos sebességgel generál csomagokat véletlenül választott cél eszközök számára. Ha egy eszköz egy saját csomagot a nuglet számláló alacsony értéke miatt nem tud a generálás után azonnal elküldeni, akkor az eszköz eldobja a csomagot (azaz nem használ puffert a csomag ideiglenes tárolására). Minden eszköz célja az, hogy minimalizálja az eldobott saját csomagok számát. Több heurisztikus csomagtovábbítási stratégiát vizsgáltunk a fenti feltevések mellett, és a szimulációk eredménye azt mutatta, hogy a kooperatívabb stratégiák általában jobb teljesítményt értek el (a fenti cél tekintetében), mint a kevésbé kooperatívak. Más szavakkal, a javasolt eljárás valóban csomagtovábbításra ösztönzi az eszközöket, legalábbis a fenti feltevések mellett.

4.2. Csomagtovábbítás ösztönzése többugrásos celluláris hálózatokban

A többugrásos celluláris hálózat [7] abban különbözik a tiszta ad hoc hálózattól, hogy a celluláris hálózatokhoz hasonlóan bázisállomásokból, és az azokat összekötő nagy sebességű genrinchálózatból álló infrastruktúrára épül. Ugyanakkor, a mai cellás rendszerektől eltérően a mobil eszközök általában nem közvetlenül kommunikálnak a bázisállomással, hanem más mobil eszközök csomagtovábbító szolgáltatását igénybe véve, több „ugráson” keresztül érik el azt. Tipikus esetben a csomag útja a forrástól a cél eszközig a következő:

- a forrástól a forráshoz legközelebbi bázisállomásig mobil eszközök továbbítják a csomagot valamilyen, ad hoc hálózatokban is alkalmazott útvonalválasztó és csomagtovábbító technikát használva,
- a forráshoz legközelebbi bázisállomástól a célhoz legközelebbi bázisállomásig a gerinchálózaton halad a csomag,
- végül a célhoz legközelebbi bázisállomástól a célig ismét több mobil eszköz továbbítja a csomagot ismét ad hoc hálózati technológiát használva.

Látható tehát, hogy a tiszta ad hoc hálózatokhoz hasonlóan, a többugrásos celluláris hálózatok működése is feltételezi, hogy az eszközök kooperatívak, és továbbítják más eszközök csomagjait. Ezért a kooperációra való ösztönzés itt is fontos. Ebben az esetben azonban a megoldás formája annyiban módosul, hogy a résztvevők halmaza kibővül a bázisállomásokkal, pontosabban az azokat működtető hálózati szolgáltatóval, mely különböző biztonsági politikák betartatásával bizonyos mértékig kontrollálni tudja a hálózat működését. A kooperációra ösztönző eljárások természetesen

kihasználhatják a hálózati szolgáltató jelenlétét. A hálózati szolgáltató például könnyen játszhatja a virtuális bank szerepét, és ezzel olyan számla alapú díjazásra épülő ösztönző rendszer kialakítását teszi lehetővé, mely nem igényel manipulálás-ellenálló modult a mobil eszközökben.

A [6]-ban egy igen hatékony, probabilisztikus mikrofizetési sémára épülő ösztönző rendszert javasoltunk, mely többugrásos celluláris hálózatokban használható. Ez a csomagtovábbításra ösztönző eljárás azt feltételezi, hogy a mobil eszközök és a bázisállomás közötti kommunikáció aszimmetrikus abban az értelemben, hogy a mobil eszközök több ugráson keresztül érik el a bázisállomást, míg a bázisállomás közvetlenül tud forgalmazni a cellájában tartózkodó mobil eszközök felé. A javasolt eljárás a csomagtovábbítás ösztönzése mellett azt is lehetővé teszi, hogy a hálózati szolgáltató detektálja és azonosítsa a csalást megkisérlő mobil eszközöket.

A probabilisztikus mikrofiztés ötletét a következőképpen magyarázhatjuk el röviden [11]: Tegyük fel, hogy *A* szeretne *B*-nek fizetni egy kis összeget, mondjuk 1 Forintot. A hagyományos mikrofizetési sémákban *A* ezt úgy teszi meg, hogy átad *B*-nek egy 1 Forintot érő elektronikus zsetont, amit *B* valódi pénzre vált be a virtuális bank segítségével. Ezzel szemben, probabilisztikus mikrofizetés esetén *A* egy 1000 Forintot érő elektronikus lottószelvényt ad át *B*-nek, amely azonban csak 1/1000 valószínűséggel nyer. Az átadott szelvény várható monetáris értéke tehát pontosan 1 Forint.

A probabilisztikus séma előnye abból származik, hogy az átadott szelvény az esetek nagy többségében nem nyer, és így *B* nem fordul a virtuális bankhoz, hogy valódi pénzre váltsa az elektronikus szelvényt. Más szavakkal, a bank terheltsége nagy mértékben csökken. Ugyanakkor, ha *B* egy szolgáltató, aki sok felhasználóval bonyolít le a fentihez hasonló tranzakciót, akkor átlagosan ugyanannyit keres, mint a hagyományos fizetési sémát használva (feltéve, hogy az egyes lottószelvények nyerése egymástól független események). Ha *A* is sok tranzakciót bonyolít le (ami mikrofizetés esetén tipikus), akkor átlagosan ő sem veszít semmit egy hagyományos mikrofizetési séma használatához képest. Az *A*-ra eső fluktuációt (néha többet kell fizetnie, mint amennyit valójában vásárolt) ki lehet küszöbölni [8].

A [6]-ban javasolt ösztönző séma alapötlete, hogy a csomag forrása egy elektronikus lottószelvényt csatol a csomaghoz, mely egy meghatározott *p* valószínűséggel nyerő szelvény bármely továbbító eszköz számára, ahol *p* egy rendszer-paraméter, amit a hálózati szolgáltató állít be. Minden, a csomagot továbbító eszköz ellenőrzi, hogy számára a csatolt szelvény nyerő-e vagy sem. A nyerő szelvényeket a továbbító eszköz tárolja. A nyerő szelvénnyel együtt azt is megjegyzi, hogy a szelvényt tartalmazó csomagot melyik eszköztől kapta és melyik eszköznek küldte tovább.

Az összegyűjtött nyerő szelvényeket, valamint a velük együtt tárolt eszköz-azonosítókat, az eszköz egy későbbi időpontban, kötegben átadja a hálózati szolgáltatónak (például mikor az eszköz fizikailag közel kerül egy bázisállomáshoz és így közvetlenül el tudja a köteget küldeni a bázisállomásnak). A bázisállomás a köteget a hálózati szolgáltató számlázó központjába küldi.

Mikor egy csomag megérkezik a bázisállomáshoz, a bázisállomás ellenőrzi a csomaghoz csatolt lottószelvény érvényességét (a lottószelvény nem más, mint egy üzenethitelesítő kód, melyet a forrás és a hálózati szolgáltató közötti titkos kulcs segítségével számol ki a forrás és ellenőriz a bázisállomás; a továbbító eszközök számára ez a kód egy pénzfeldobás sorozat). Ha a szelvény érvényes (azaz valóban a csomag forrása generálta), akkor a csomagot a bázis állomás továbbítja a cél felé. Ellenkező esetben a bázisállomás eldobja a csomagot, hiszen annak továbbításáért nem tud megterhelni senkit.

A sikeres csomagokról a bázisállomás tájékoztatja a hálózati szolgáltató számlázási központját. A számlázási központ tehát két forrásból kap információt: egyrészt a bázisállomások tájékoztatják, hogy mely csomagok érték el sikeresen a célt, másrészt a továbbító eszközök küldik el nyerő lottószelvényeiket. A számlázási központ ezen információk összevetésével állapítja meg, hogy kit kell megterhelni, kit kell kifizetni, és hogy ki próbált meg csalni. Egészen pontosan, a sikeres csomagok forrásának számláját a központ megterheli. A terhelés mértékét a hálózati szolgáltató állapítja meg, ám az alapvetően a csomag méretétől függ.

A nyerő szelvényekre csak akkor fizet a központ, ha a szelvényhez tartozó csomagot valamely bázisállomás jelentette, azaz az sikeresen elérte a célt. Ez ösztönzi az eszközöket, hogy továbbítsák a csomagot, különben nem kapnak fizettséget, hiába rendelkeznek nyerő szelvénnyel. Ráadásul mikor egy nyereményt kifizet a központ, akkor nemcsak a nyerő szelvényt benyújtó eszköznek fizet, hanem annak eszköznek is, amelytől a szelvényt benyújtó eszköz a csomagot kapta, és annak is, akinek a csomagot továbbküldte. Ez még jobban ösztönzi az eszközöket a csomagok továbbítására, hiszen így még vesztes szelvényt tartalmazó csomagokat is van értelme továbbítani, mivel ugyanaz a szelvény a következő eszköz számára lehet nyerő, mely esetben a nem nyerő továbbító eszköz is jutalomban részesül.

A fentieken túl, a szomszédok nyerő szelvénnyel együtt történő lejelentésének van egy másik előnye: lehetővé teszi a központ számára csomagtovábbítási statisztikák készítését. Az ezen statisztikákban felfedezett inkonzisztencia pedig lehetővé teszi a csalások detektálását, majd megbüntetését. Ha például egy eszköz szisztematikusan megtagadja a csomagok továbbítását, akkor nagyobb gyakorisággal fog megjelenni csomagot fogadó szomszédként, mint csomagot küldő szomszédként. Ráadásul, minnél agresszívebben tagadja meg egy eszköz a csomagok továbbítását, annál könnyebben és hamarabb fogja ezt a számlázási központ detektálni.

Irodalom

[1] N. B. Salem, L. Buttyán, J.-P. Hubaux, M. Jakobsson: A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks, In Proceedings of the 4th ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Annapolis, Maryland, USA, 2003.

[2] S. Buchegger, J.-Y. Le Boudec: Performance Analysis of the CONFIDANT Protocol (Cooperation of Nodes: Fairness in Dynamic Ad-hoc NeTworks), In Proceedings of the Third ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Lausanne, June 2002.

[3] L. Buttyán, J.-P. Hubaux (eds.): Report on a Working Session on Security in Wireless Ad Hoc Networks, ACM Mobile Communications and Computing Reviews, 7(1), 2003.

[4] L. Buttyán, J. P. Hubaux: Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks, ACM/Kluwer Journal on Mobile Networks and Applications (MONET), to appear, October 2003.

[5] S. Corson, J. Freebersyser, A. Sastry (eds.): ACM/Kluwer Mobile Networks and Applications, Special Issue on Mobile Ad Hoc Networking, October 1999.

[6] M. Jakobsson, J.-P. Hubaux, L. Buttyán: A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks, In Proceedings of the Seventh International Financial Cryptography Conference, Guadeloupe, January 2003.

[7] Y.-D. Lin, Y.-C. Hsu: Multihop Cellular: A New Architecture for Wireless Communications, In Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom), Tel Aviv, 2000.

[8] S. Micali, R. Rivest: Micropayments Revisited. In Proceedings of the Cryptographer's Track at the RSA Conference, 2002.

[9] P. Michiardi, R. Molva: CORE: A COllaborative REputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks, In Proceedings of the IFIP Communication and Multimedia Security Conference, Portoroz, Slovenia, 2002.

[10] P. Obreiter, B. Koenig-Ries, and M. Klein: Stimulating cooperative behavior of autonomous devices – an analysis of requirements and existing approaches, In Proceedings of the Second International Workshop on Wireless Information Systems (WIS), 2003.

[11] R. Rivest: Electronic Lottery Tickets as Micropayments, In Proceedings of the Financial Cryptography Conference, 1997.

[12] S. Zhong, Y. R. Yang, and J. Chen: Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad Hoc Networks. In Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (Infocom), 2003.

Hírek

Az **Invitel Rt.** és az **Ericsson Magyarország** keretszerződést írt alá **Ethernet DSL Access** (EDA) rendszer telepítésére és rendszerintegrációs munkákra. A közelmúltban az Ericsson mérnökei olyan megoldást fejlesztettek ki, amellyel a szolgáltatók minden eddiginél olcsóbban, gyorsabban és egyszerűbben építhetik ki saját ADSL hálózartukat.
Az EDA technológia lényege, hogy nincsen szükség viszonylag drága ATM alapú felhordóhálózatra, mert helyette a már jól megszokott Ethernet hálózati elemek használhatók. Az Ethernet DSL Access technológia egészen kicsi, 10-12 előfizető kiszolgálására alkalmas dobozokból épül fel.

2003. február végétől **Axelero Internet Biztonság** néven új szolgáltatást indított az **Axelero** az **F-Secure Corporation**-nel együttműködve, amely védelmet nyújt a személyi számítógépeket érő különféle külső támadásokkal és vírusokkal szemben. Az egyedi konstrukcióban kínált szolgáltatást az Axelero minden jelenlegi és új hozzáférést vásárló előfizetője egyaránt igénybe veheti, havi nettó 1000 forintos előfizetési díj ellenében.
Az Axelero új akciója révén a február 16. és március 31. között ADSL Profi hozzáférést vásárlók ingyenesen juthattak a szolgáltatáshoz. A vállalat előjelzése szerint ez év végéig közel 7000 előfizető veszi igénybe majd az új biztonsági megoldást.

Az m-kereskedelmet kiszolgáló mobil technika

HORVÁTH GYULA *gyémántokleveles távközlési tanácsadó mérnök*

horgyul@hdsnet.hu

Kulcsszavak: tartalomszolgáltatás, szabványosítás, nyílt szoftverek

A vezető távközlési vállalatok érdeklődése folytán a nemzetközi szabványosító intézetek a mobil kereskedelmet kiszolgáló távközlő technikával, mint a műszaki fejlődés egyik soron lévő lépésével foglalkoznak. Ez az egyik gyakran alkalmazott módon úgy kezdődik, hogy a leendő új termék ajánlott közös tulajdonságait a szabványosítás folyamatában együttesen tervezik meg.

Új műszaki elképzelések értékelését mérnöki gondolkodás szerint a mű világos meghatározásával, a bevezetésekor önnálló helyzet ismertetésével és az elérendő célok rögzítésével célszerű kezdeni. Ezt követheti a kifejlesztése során megoldandó föladatok számbavétele, majd az elérhető eredmények értékelése. Az m-kereskedelemmel ez a cikk a feladatokig bezárólag foglalkozik. Előzetes értékelésre a szabványok megjelenése után kerülhet sor, a végső ítéletet a piac fogja kimondani. E cikk célja az m-kereskedelmet kiszolgáló, fejlődésben lévő távközlés állapotáról tájékoztatást adni.

Bevezetés

Meghatározás:

Előfizetők szempontjából az egyik új átfogó szolgáltatás, szolgáltatók szempontjából szolgáltatások és funkciók szervezett csoportja.

Az m-kereskedelem a születése idején még domináns vezetékes technika eszközeivel megvalósuló e-kereskedelembe a mobil távközlés bevonásával keletkezik. Lényege az, hogy üzleti ügyek intézésére mobil készülékekről adat- és videó átvitel útján nyit lehetőséget, ami hozzáférést jelent a szükséges multimédia információkhoz és módot ad gépi úton végrehajtható utasítások kiadására (pl. banki ügyek intézése). Legfontosabb eszköze az MMS *(mobil multimedia messaging service,* multimédia mobil üzenetküldő rendszer), amelynek nem egyetlen alkalmazása az m-kereskedelem.

Célkitűzés:

M-kereskedelem mindenütt, biztonságosan és gazdaságosan.

A már működő mobil adatátviteli rendszerek teljes lefedettséget még nem nyújtanak, adatbiztonság szempontjából még nem tökéletesek. Mellettük a piac részleges telítettsége miatt csak gazdaságosan használható új mobil szolgáltatás számíthat sikerre. A siker további föltétele az m-kereskedelem gazdasági oldalának kialakulása (például a vevők bizalmának elnyerése és megőrzése), amihez a csomagküldő szolgálatok és az e-kereskedelem tapasztalatai állnak rendelkezésre.

Helyzetértékelés:

Rendelkezésre áll már a WAP, az MMS és a 3G.

A WAP *(wireless access protocol,* vezetéknélküli hozzáférési protokoll) útján szerzett magának az adatátvitel helyet a mobil távközlésben, ami napjainkban a videó átvitellel bővül, elsősorban a mobilkészülék felé. A felmenő irányú forgalom nélkülözhetetlen feltételeként kaphatók már digitális fényképezőgéppel egybeépített mobil készülékek is.

A 3G mobil szabványainak megfelelő átviteli rendszeren működhet a mindenütt használható, univerzális mobil távközlő rendszer (UMTS), ami az m-kereskedelem számára hordozónak kiválóan alkalmas. A népiesen maroktelefonnak nevezett mobilkészüléknek már a nevéből is következik, hogy kicsiny a *kijelzője* és kevés nyomógombját különféle logikai fogásokkal többféle utasítás kiadására lehet fölhasználni. A kijelző mérete már az olvasást is korlátozza, a bonyolultabb vagy terjedelmesebb képek nézése kívánnivalókat hagy maga után.

A *tartalomszolgáltatás* egyoldalú, mert tartalmakat olyanok készítenek, akiknek valamilyen, legtöbbször üzleti érdekük fűződik ahhoz, hogy az adott információkhoz bárki könnyen hozzáférhessen. A mobil előfizetőket ezen kívül érdeklő témákban kevés értékes tartalmat készítenek, mert nincs általánosan alkalmazható egyszerű megoldás a hozzáférési díj utólagos beszedésére.

Mind a fix, mind a mobil előfizetők számára elmúlóban van azoknak az újdonságoknak varázsa, amelyek bármikor, jól fölépített menürendszeren keresztül nyújtanak felvilágosítást, tájékoztatást, tesznek esetleg ajánlatot. Még túl gyakran érzik annak szükségességét, hogy valamelyik részletkérdésben a menüben nem található gépi hang helyett élő hangot halljanak.

Megoldandó problémák

A leírt helyzetből látható, hogy az m-kereskedelem megvalósításához a már működő mobil távközlő hálózat jellemző tulajdonságainak fontossága megváltozik, a rendszernek nemcsak műszaki, hanem gazdasági tulajdonságait is tovább kell fejleszteni, és új képességek szükségesek.

Ezek a kölcsönös együttműködés (interoperability), a gazdaságosság, új szolgáltatások, és más további feladatok címszavai alatt csoportosíthatók.

Kölcsönös együttműködés

Az ember és munkaeszköze kezdettől fogva lazább vagy szorosabb rendszert alkotott. Az m-kereskedelem céljára használt technika elemei között kifogástalan, kölcsönös együttműködést biztosító, szoros, divatos kifejezéssel élve hézagmentes *(seamless)* kapcsolatra van szükség, főleg a biztonság és megbízhatóság érdekében. A ma rendelkezésre álló hardver- és szoftvertechnika ezen igény kielégítésére elvileg alkalmas.

Az m-kereskedelmet sokféle alrendszerben használják. Ezek a használók és szolgáltatók, gyártók, kereskedők és üzemeltetők, akiknek szoros együttműködésére van szükség, kiterjesztve az alkalmazások gyakran még csak mellékesen figyelembe vett szempontjaival is. Utóbbi annak a ma még új követelménynek a kielégítését jelenti, miszerint az ember-gép interfészeknél nemcsak az igen eltérő természetű embert és gépet kell hézagmentesen egymáshoz illeszteni, hanem a rendszer egészének működéséből az ezen interfészre háruló feladatokat is meg kell oldani. Ehhez a keretet három jelentős szervezet, a GSM Association (GSM Szövetség), a 3GPP (3. Generációs Partnerségi Program) és a GBA (Globális Számlázási Társaság) adja.

Szabványok

Az előbb vázolt együttműködés Európában az ETSI égisze alatt, a rendszer minden elemére kiterjedő szabványosítás területén intenzíven folyik. Az m-kereskedelemmel kapcsolatban az ETSI vezetése alatt futnak az *m-kereskedelem* és a *Smart Card Platform* elnevezésű projektek. Az m-kereskedelem projekt legsürgősebb célja a biztonságos elektronikus aláírás megteremtése. Ebben ETSI szorosan együttműködik folyamatban lévő más, idevágó projektjein kívül az Európai Elektronikus Aláírást Szabványosító Kezdeményezéssel (EESSI).

A szabványosítás másik fő területe a számlázás és a fizetés problémáinak megoldása. A díjmegállapítás fő segédeszközének a SIM kártya mellett a mobil készülékbe helyezett intelligens kártyát (smart card) tartják, ami a SIM kártyához hasonlóan a díj összegének megállapításához szükséges, az előfizetőre vonatkozó állandó adatokat tartalmazza, amiket a számlázó program kérdez le. A fizetés lebonyolításakor a távközlési szolgáltató az érintett bankkal munkakapcsolatba kerül, ezért az m-kereskedelem szakbizottságaiban az Európai Banki Szabványok Bizottságának (ECBS) képviselői is tagok.

Nyílt szoftverek

A nyílt szoftverekre törekvés az m-kereskedelem területén már általános. Előnyük abban áll, hogy a – számos alkalmazást, részletmegoldást, illesztést a különböző vállalatoknál, különböző időpontokban kidolgozó – szoftverfejlesztők közös alapra támaszkodhatnak, így saját szoftverjeiket a nyílt szoftverekkel szoros összhangba hozhatják. A nyílt szoftverek ügyének fő képviselője az OMA (Nyílt Mobil Szövetség), amely több szabványosító csoportot integrál. Fő jellemzője, hogy más szervezetektől eltérően, holisztikusan közelíti meg a mobil szolgálatok és alkalmazások értékláncát. Nincs más ipari szervezet, amelyben ennyire átfogóan vesznek részt a mobil szolgáltatások egész értékláncával foglalkozó szakemberek, akik így középpontba állíthatják a piac és az ügyfelek követelményeit.

A *barangolással* kapcsolatos problémák más formában is jelentkeznek, mihelyt az egymással MMS üzeneteket váltó mobil készülékek között kettőnél több mobil szolgáltató hálózatán keresztül létesül kapcsolat. Ezek között kell ugyanis elosztani valós időben az összeköttetésért beszedett díjat. Újdonságok a mobil készülék földrajzi helyzetéhez kapcsolódó *értéknövelt szolgáltatások*. A földrajzi helyzet, mint adat egyre több értéknövelt szolgálat számára használható. A saját helyzet meghatározása a használó tájékoztatásán kívül olyan szolgáltatások alapjául is szolgálhat, mint helyi időjárás előrejelzése, bankjegy-kiadó automaták helye, a közelben lévő barátok adatai és tartózkodási helyük, valamint más, helytől függő ismeretek.

Díjelszámolás

A vezetékes technikában elterjedt gyakorlat, miszerint a beszélgetés befejezésekor a fizetendő díjra vonatkozó minden információnak – ismert okokból – már tárolva kell lennie, a mobil távközlésben sem mellőzhető. Ez azért említésre méltó, mert e célból a mobil hálózat különböző pontjai között többszöri információküldés szükséges. Felmerül az igény, hogy ezek költségét az információt felhasználó erőforrás tulajdonosa (általában a hívó előfizető szolgáltatója) megtérítse.

A mobil szolgálatok értékét növeli a segítségükkel elérhető tartalmak mennyisége, melyeknek előállítását, ha közzététele nem a készítőjének érdeke, meg kell fizetni. A mobil szolgáltatók ennek kézenfekvő megoldásától, a tartalom árának beszedésétől még idegenkednek. Mivel a többi értéknövelt szolgálat díjának megállapítása és beszedése műszakilag megoldható, a probléma gazdasági és lélektani jellegű. Az idegenkedés fő oka, hogy precízen működő számviteli és átutalási rendszert kell kiépíteni a tartalomszolgáltatást igénybevevő előfizetők, a mobil szolgáltató, a tartalomszolgáltatók és a pénzügyeiket intéző bankok között. A nélkülözhetetlen kölcsönös bizalom ennek a rendszernek pontos és hibátlan működésén alapul. Megingásakor a rendszer igénybevétele rohamosan csökken, majd a rendszer veszteségessé válik.

Ez a szolgáltatás, valamint a korábban említett, helyszínfüggő információkat nyújtó értéknövelt szolgáltatások is azt jelzik, hogy az m-kereskedelem milyen széles körben terjedhet el.

Gazdaságosság

Felmerül a kérdés: kinek kell és kinek nem?

Az őszinte válasz a mai helyzetben az, hogy elsősorban a mobil szolgáltatóknak és a munkájukat kiegé-

szítő vállalkozásoknak (beszállítók stb.) kell, akik forgalmukat növelni, abból profitot termelni akarnak. Másodsorban azoknak, akiknek az e-kereskedelem lehetőségeire esetenként távollét, mozgás vagy más ok miatt is szükségük van. Ilyenek például azok, akik fix telefontól távol, saját költségükre akarják az e-kereskedelem valamelyik szolgáltatását igénybe venni (esetleg más, fix telefon készülék használata helyett).

Nem kell azoknak, akik igényeiket az e-kereskedelem eszközeivel is kényelmesen ki tudják elégíteni és nagyon kellene azoknak, akiknek anyagi ereje elégtelen az m-kereskedelem számukra szükséges szolgáltatásai költségeinek fedezésére. Az elemzők egy része olyan gyorsan kirobbanó érdeklődésre számít, mint amit a legutóbbi időben az SMS iránt tapasztalhattunk, pedig az általuk kiragadott példák nem erre utalnak.

A *méretgazdaságosság* érdekében a mobil távközléssel továbbítható minden formájú, nemcsak az m-kereskedelmet szolgáló információ együttes átvitelére és kombinált kezelésére célszerű berendezkedni. Ez a gazdaságosságot növelő kritikus eszköz. A forgalmat növeli például a multimédiás interaktív játékok megnövekedett választéka, mert ezekkel várakozás, utazás közben sokan szórakozhatnak.

Az m-kereskedelem sikere csak a kritikus tömeg elérése után bontakozik ki. Ez a készülékek elérhető árával és a használatot serkentő díjszabás alkalmazásával siettethető.

Tökéletesített és új szolgáltatások

Érzékeny adatok biztonságos átvitele és kezelése

Az adott ügylet hibátlan lebonyolításához szükséges adatok feltétlen továbbítása eredeti alakjukban a rádiós átvitel során mutatkozó zavaró tényezők ellenére.

Globális platform, ezen belül globális architektúra

Célja az m-kereskedelem szolgáltatásainak használata helyszíntől függetlenül, kapcsolatteremtés – akár egy másik kontinensen is – a mobil készülék módosítása, vagy kezelésének megváltoztatása nélkül. Megvalósításához globális architektúra szükséges, különböző helyi rendszerek integrálása céljából.

Készülékek

A készülék-konstruktőrök elsődleges feladata jelenleg a képek élvezhetőségének javítása. Olyan különös megoldások is szóba jöhetnek, mint nagyítólencse elhelyezése a képernyő előtt és más kreatív ötletek.

Tapasztalatok szerint meglehetősen alacsonyan van az a határ, ameddig a kezelés bonyolultságát a felhasználók indokoltan elviselik. A határ túllépése a ritkábban használt szolgáltatások igénybevételének csökkenéséhez, elhalásához vezethet, ezért fontosabb a kezelés egyszerűségének fenntartása, mint újabb és újabb szolgáltatások bezsúfolása.

A virtuális eladó a kívánt árút és egyes részleteit természetben, nézőpontból rátekintve mutathatja be. Kisebb darabokat a kamera előtt forgathat, nagyobbakat körüljárhat, üzemi helyiségeket kamerával bejárhat. Lehetősége van arra, hogy az árú műszaki dokumentációjának egyes részleteit megmutassa, például diagrammokat, táblázatokat, ábrákat. A beépített digitális fényképezőgép az m-kereskedelemre alkalmas mobil készülékek nélkülözhetetlen alkotóeleme lesz. Képek átvitelekor a rádiós csatorna zajérzékenységére külön ügyelni kell.

Távlati lehetőségek

A bankkártya (hitelkártya) és a mobil készülék összevonása kívánatos, de még sok jogi, biztonsági és műszaki részletkérdés megnyugtató megoldása szükséges. Még nem általános az a szemlélet, hogy „az előfizető a király”, vagyis, hogy mindenben az előfizető szempontjaiból, elvárásaiból, érdekeiből kell kiindulni, nem technikát, hanem szolgáltatásokat kell eladni. Ritkán használják fel azt a két ősi megfigyelést, amelyek szerint távoli szakterületekről származó tapasztalatokat is meglepően jól lehet hasznosítani (profik), valamint, hogy jó hatásfokkal lehet szórakozva tanulni (használók).

Sok, türelmesen lefolytatott egyeztető tárgyalás útján a tartalommal kapcsolatos problémák sikeres megoldása nem kétséges. Ma már nem okoz gondot az angol nyelv ismeretének hiánya sem, mint az Interneten elérhető tartalom megértésének eszköze. A ma még költséges számítógépek mellett szakmai angol nyelvtudás megszerzését is támogatni kellene mindazoknak, akik az m-kereskedelem elterjesztésében sikeresen akarnak részt venni.

Összefoglalás

Az m-kereskedelem sikere már nem a technikán múlik, hanem sokkal inkább a rendszer jól működő emberi oldalán. Az MMS gyártóinak és üzemeltetőinek jelentős segítséget kell ügyfeleiknek nyújtaniuk ahhoz, hogy munkamódszereik, szemléletük átalakításával az MMS által jelentősen megnövelt mozgékonyságukat maximálisan kihasználhassák. Ebben tanfolyamokkal, tanácsadással, esetleg az IBM példáját követve a technika működtetésének, az ezzel kapcsolatos kockázatnak átvállalásával segíthetnek. A vállalkozóknak arra is figyelniük kell, hogy befektetésük megtérülése a kívánatosnál lassúbb lesz, mert mint láttuk, ez az új szolgáltatás eleinte csak korlátozott ügyfélkört fog érdekelni.

A bevezetésén gondolkodó szolgáltatók elsősorban nagyvárosok üzleti negyedében tervezik az MMS-re alkalmas mobilhálózat kiépítését. A távlati lehetőségek pontosabb fölbecsülésére a bevezetőben említett szabványok megjelenése után nyílik a következő alkalom.

Irodalom

The M-Business Agenda 2003,
Sterling Publications Ltd., társulva a következőkkel:
GSM, the wireless association (www.gsmworld.com),
3GPP, a global association (www.3gpp.org),
GBA, Global Building Association (www.globalbilling.org).

Visszhangzár a kábeltévéhez
(Dynamic Ingress Blocking™)

WEIN TIBOR, *műszaki menedzser*
HFC Technics Kft.
t.wein@hfctechnics.hu

Kulcsszavak: zajcsökkentés, reflexió, zajelnyomás, kábeltévé-minőség

A DIB™ a kábelhálózatok cikkünkben összefoglalt visszirányú problémáinak megoldására kidolgozott, szabadalmaztatott technológia. Bemutatott képességeivel a hálózat kétirányúsítása könnyebben és gyorsabban végrehajtható, lehetővé válik a kábelmodemek előfizető általi üzembehelyezése és a VoIP-hoz szükséges szolgáltatási minőség (QoS) elérése. A DIB moduláris struktúrája a szolgáltató számára lehetővé teszi a kis rendszerrel történő indulást, mely később szinte korlátlanul bővíthető. A DIB™ a kétirányú kábelhálózatok hatékony üzemeltetését és fenntartását is lényegesen megkönnyíti.

1. Visszirányú zajok

A visszirányú átviteli eszközök a szolgáltató szempontjából részben idegen birtokon belül működnek. Ez a környezet a visszirányú csatornába behatoló zajok fő forrása. A kétirányú kábelhálózatok jelútjait az *1. ábra* szemlélteti. A visszirányú jelút határfrekvenciája korszerű hálózatoknál általában 65 MHz. Elemeit az ábrán szürkítéssel különböztettük meg. Az ábra a városi hálózatok kezdeti alacsonyabb penetrációk mellett jellemző legösszetettebb esetét szemlélteti, amikor a CATV fejállomás és a CMTS telephelye közös.

A felhasználói sűrűség növekedésével a CMTS-ek (Cable Modem Terminating System) az optikai csomópontokkal közös telephelyen is létesülhetnek. A jövőben tehát a visszirányú jelút analóg fényvezetős szakasza többségüknél már elmarad. A cikkben bemutatott zaj- és átviteli kapacitás számítási példák erre az esetre vonatkoznak.

- A kábelhálózatok kétirányú alkalmazásának legjelentősebb problémái az alábbiak:
  – a zajszintek halmozódása,
  – a teljes visszirányú átvitel veszélyeztetettsége egyedi zajforrásoktól, és
  – a háztartásokba nem kielégítő zavarvédettséggel bevezetett kábelek.
- A visszirányú zajok három fő összetevője:
  – a hálózatban lévő aktív eszközök termikus zaja,
  – közösutas torzítás (Common Path Distortion – CPD),
  – és a behatoló zajok (áthallás, külső zavarok).

A zajok eredetének behatárolása idő- és munkaigényes feladat. Elhárításuk az erősen korlátozott hozzáférési lehetőségek miatt az esetek többségében nem is lehetséges. A zajok forrásai a háztartásokban

– a kábelmodemek,
– egyéb visszirányú eszközök és
– a fali csatlakozókhoz vezető kábelek.

A modemek által bevitt zaj jelentősége a penetráció növekedésével együtt nő. Tapasztalatok szerint a zajbehatolás a hálózatban az alábbiak szerint oszlik meg:

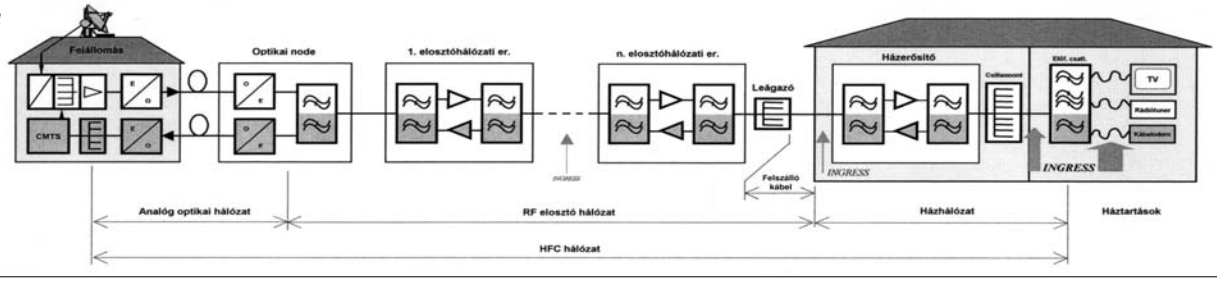
- háztartások: 50-70%
- felszálló kábelek, házhálózatok: 20-30%
- RF elosztóhálózat: 10-20%

A háztartásokból behatoló, időszakos külső zajok forrásai általában a fényerőszabályzók, TV készülékek, villanymotorok, rádiótelefonok, az amatőr rádió adó-vevők és a házi készítésű elektromos huzalozások.

A elosztóhálózatban keletkező zajok egyik összetevője a közösutas torzítás (CPD). Ennek forrása elsősorban az érintkezők szintfüggő átmeneti ellenállása. A másik összetevő a hálózat aktív eszközeinek termikus zaja, amely már könnyebben kézben tartható. A hálózat tervezési szabályainak betartásával az eredő zaj a küszöbérték alatt tartható. HFC hálózatokban a zaj nagyobbik része a visszirányú optikai szakaszon keletkezik, amely az optikai csomópontnál telepített CMTS-nél már kiesik.

Mérések szerint a zajszint a visszirányú frekvenciasáv alsó részén, főleg 10-15 MHz között kiemelkedő. Forrásai elsősorban az ipari frekvenciás zajokat kibo-

1. ábra



csátó háztartási eszközök. A mérések eredményei azt mutatják, hogy ezek használata az esti órákban a leggyakoribb, amikor a visszirányú forgalmi igény is nagy.

A zajok vizsgálatához először tekintsük át a hálózat működését, mely előre irányban a vízvezeték-hálózathoz hasonlítható, mely a vizet a háztartásokba egyre kisebb ágakra bontva juttatja. A visszirány ezzel az analógiával élve a szennyvíz hálózathoz hasonlít, amelyben a CMTS felé tartó áramlathoz valamennyi háztartás hozzájárul.

A kábelmodemekben alkalmazott visszirányú moduláció általában a QPSK, amelynek átviteli kapacitása az előre irányban alkalmazott 64QAM-énak egyharmada. Az adatforgalom, következésképpen a sávszélesség igény ugyanakkor folyamatosan növekszik (több játék, IP telefónia, e-mailek nagy mellékletekkel stb.).

A 20 MHz alatti frekvenciákon a zaj tranziens viselkedést mutat (nagy amplitúdójú keskeny tüskék). E feletti frekvenciákon a zaj inkább termikus jellegű, Gauss-eloszlású. A nagyszámú (1000-nél több) előfizetőtől felhalmozódó zajok azonban már mindenütt normál eloszlást mutatnak (központi határeloszlás-tétel).

Több mint 1000 háztartást ellátó elosztó hálózatok esetén a zaj teljesítménye a frekvencia függvényében 10-15 dB, vagyis az 5-15 MHz sávba eső zaj szintje a 40-65 MHz-esbe esőnél ennyivel magasabb. A zaj teljesítmény időbeli változást is mutat: a hajnali órákban kisebb, mint az estiekben. Az időbeli ingadozásokra 10 dB rendszertartalékot célszerű figyelembe venni és a mindenkori zajszintre ülő jelentős zajtüskék fellépésével is számolni kell.

2. A zajcsökkentés lehetőségei

Az optikai csomópont által kiszolgált előfizetőszám csökkentésével csökken a visszirányú zaj, vagyis az RF elosztóhálózat területét csökkenteni kell a fényvezetős szakaszok egyidejű növelésével. Ezzel a visszirányú átvitelt megbénító zajosodások valószínűsége is arányosan csökken. A megoldás ugyan hatékony, de igen költséges és a zaj okozta esetenkénti összeomlások kockázata, annak nagyságrendi csökkenése után sem lesz elhanyagolható.

Az alábbiakban áttekintjük a zajcsökkentés további lehetőségeit.

2.1. Szűrők alkalmazása

Felülátereszt ő szűrők beiktatásával a csillagpontnál, a visszirányú zaj csökkenthető. Segítségükkel a visszirányú kommunikációban részt nem vevő háztartásokból a csillagponthoz érkező zajok korlátozhatók, amely egyet jelent a csillagpont visszirányúsított háztartásaira eső zajhozzájárulás csökkentésével. A kétirányú átvitel növekedésével a megoldás hatása azonban folyamatosan csökken, ezért eredményesen csak az alacsony penetrációjú csillagpontos hálózatokban alkalmazható.

Sávszűrős összegzők is alkalmazhatók a jelutak egyesítési pontjaiban a szélessávú összegzők helyett, a hálózatrészek között felosztott átviteli sávokra méretezve. Ezek az összes zajösszetevőt hatékonyan csökkentik, hátrányuk azonban, hogy megfelelő minőségben rendszerint nem beszerezhetők.

2.2. Más lehetőségek

Multimédia csatlakozók alkalmazása az előfizetői csatlakozók cseréjével az ingress (visszirányú) zaj csökkentésének elterjedt megoldása. A multimédiás aljzatokat külön csatlakozókkal látják el a kommunikációs eszközök (kábelmodemek) számára. A megoldás előnye, hogy korlátozza a háztartásból eredő zajt, és nem visz többletcsillapítást a háztartás és az első visszirányú erősítő közötti jelútba. (Hátrányai a csere költségei és a háztartásokba való bejutás nehézségei.)

Kétirányú hálózatok zökkenőmentes üzemeltetése csak a hibák és zajforrások kiszűrését megfelelően biztosító *hálózat-felügyelettel* lehetséges.

A *megfelelő induló vivő-interferencia arány* (Carrier to Interferer – C/I) biztosítása rendkívül fontos. Az előfizetői végberendezések (modem) adószintjét ennek megfelelően ajánlatos minél magasabbra választani, mivel a nem megfelelő induló C/I a jelút mentén a hagyományos megoldásokkal már nemigen javítható.

3. A DIB™, mint megoldás

3.1. Működési mód

A nem kívánatos mértékű romlás úgy is megelőzhető, hogy a hálózat kizárólag a modemek által kiadott hasznos jelek célba jutását teszi lehetővé. Ehhez egy olyan eszköz beépítése szükséges, amely a hálózatban minden egyéb jel terjedését, bármely frekvencián megakadályozza. Ezt a dinamikus visszhangzár (DIB™ – Dynamic Ingress Blocker) a hálózat távoli pontjain elhelyezett zajcsökkentő egységekkel valósítja meg, ahol a C/I értéke még megfelelő. A zajcsökkentő egység a behatoló tranziens (Ingress) zajt oly módon csökkenti, hogy a visszirányt csak valós átvitel idején tartja nyitva, azaz ennek kezdetén nyit, az átvitel befejeztével pedig zár. A megoldás lényege az a működési sebesség, amelynek eredményeként a csatorna kizárólag *a jelátvitel valós időréseinek időtartama alatt nyitott*.

A zajcsökkentő egységek csak az éppen adásban lévő modemekhez (vagy egyéb interaktív eszközökhöz) tartozó zajcsökkentőkre kötött háztartások zajhozzájárulását engedik vissza az elosztóhálózatba. Az egyidejűleg nyitott zajcsökkentő egységek száma a visszirányú csatornában a visszirányú vivők, és az azok közül éppen működők számától függ. Az ingress zaj alsó sávba eső összetevőinek eredményes elnyomásához azonban a felülátereszt ő szűrőzés járulékos alkalmazása is célszerű.

A DIBTM-et a TDMA (pl. DOCSIS) alapú kábelmodemekkel való együttműködéshez tervezték. A modem és a CMTS közti kapcsolat TDMA alapú működése követ-

keztében a hálózatnak időben egyszerre mindig csak kis része kapcsolódik a hálózatra.

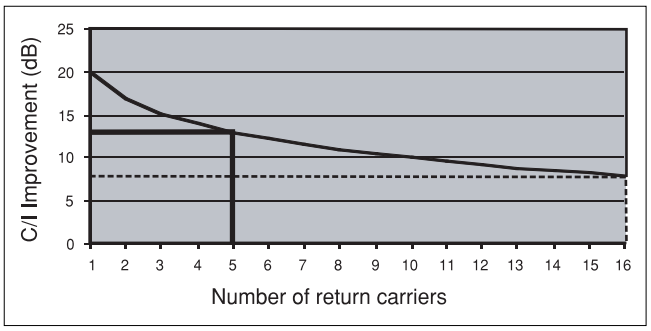
A zajcsökkentő egységek a jelutat előre meghatározott feltételek esetén nyitják. Ezek teljesülése a visszirányú jelek értékelésén és elemzésén alapszik. A zajanalízis egyúttal a zajok eredetének behatárolását, valamint az ezekkel összefüggő problémák (szabotázs, hibás csatlakozók stb.) gyors felderítését is lehetővé teszi.

3.2. Alkalmazási példa

A *2. ábra* egy 2000 lakást ellátó elosztóhálózat C/I javulását szemlélteti 20 lakás/DIB sűrűségnél. Mint az ábráról leolvasható, öt teljes terhelésű visszirányú vivő esetén (pl. két Internet, két VoIP és egy interaktív TV) a C/I=13 dB (folytonos vonal). A DIB™ még 16 visszirányú vivő esetén is (amely 160 Mb/s kapacitást jelent), 8 dB C/I javulást eredményez (szaggatott vonal).

A CMTS-nél mérhető C/I eredő értékét az alábbi tényezők befolyásolják:

– a CMTS node mérete,
– a hálózatban alkalmazott vivők száma és
– a zajcsökkentőkre eső háztartások átlagos száma.



2. ábra

3.3. A zajnyereség számítása

A visszirányú zajok jellemző értékei

Az 1,6 MHz-es modemcsatorna zajának egy háztartásra eső tipikus értéke a 20-30 MHz-es sávban 32 dBµV. 20 előfizető együttes zajhozzájárulása 13 dB (lásd 2. ábra), amely az utolsó erősítő bemenetén 32+13=45 dBµV eredőt eredményez. A kábelmodem felől érkező jel névleges szintje ezen a ponton 75 dBµV, a C/I tehát ugyanitt 75-45=30 dB. 2000 háztartás esetén 30-20=**10 dB** C/I várható.

A C/I javulása a

$$G_{C/I} = 10 * \log (K_{DIB} / K_{hh} / K_c)$$

képlettel számítható, ahol K_{DIB} a zajcsökkentő egységek száma az elosztóhálózatban, K_{hh} az egy zajcsökkentőre eső háztartások száma és K_c az egyidejűleg alkalmazott visszirányú vivők száma. Legyen az 1,6 MHz-es modemcsatorna az egy háztartásra eső tipikus zajteljesítmény (ingress zaj + CPD + alapzaj) értéke N. A háztartásokból eredő Gauss-zajok teljesítményben adódnak össze, így az összes háztartás által termelt zaj eredő értéke:

$$N_{total} = N_1 + N_2 + \ldots + N_k$$

Statisztikus alapon feltételezhető, hogy a háztartások zaj hozzájárulása egyforma, azaz

$$N_1 = N_2 = N_k .$$

Ennek megfelelően, például egy 20 háztartásból álló elosztóhálózat 20N, egy 2000-ből álló 2000N nagyságú zajt termel. 20 háztartásonként egy zajcsökkentő alkalmazásával a zajcsökkentés mértéke, például egy 2000-es node területen 2000/20=100. A C/I javulás így 20dB.

A példa egy visszirányú vivő esetére érvényes. Nagy Internet, VoIP, interaktív TV stb. sűrűség esetén az egyidőben alkalmazott vivők száma, mint az alábbiakban látni fogjuk, egynél természetesen jóval több, melyet az (1) képlet az egyidejűleg alkalmazott visszirányú vivők számának szorzótényezőjével vesz figyelembe. A képlet max. 16 vivőig ad megfelelő közelítést.

3.4. A visszirányú vivők száma

2000 háztartásra vetítve az *Internet adatforgalma* (szörfözés, mail stb.) 30% penetráció mellett 600 előfizető. Az átviteli kapacitás optimális kihasználását vivőnként kb. 10 Mb/s adatsebesség jelenti.

A hagyományos távbeszélő előfizetők átlagos hívássűrűsége 100mE körüli érték. Egy 2000 előfizetős elosztóhálózatban 30% VoIP sűrűség mellett ennek alapján 66E a forgalma. Az Erlang B formulával, 1% veszteséggel 81 trönkvonal lenne szükséges.

Ebből következik, hogy a 10Mb/s/vivő átviteli kapacitás a szolgáltatást hosszútávon is elegendő tartalékkal biztosítja.

3.5. A többvivős üzemben elérhető zajnyereség

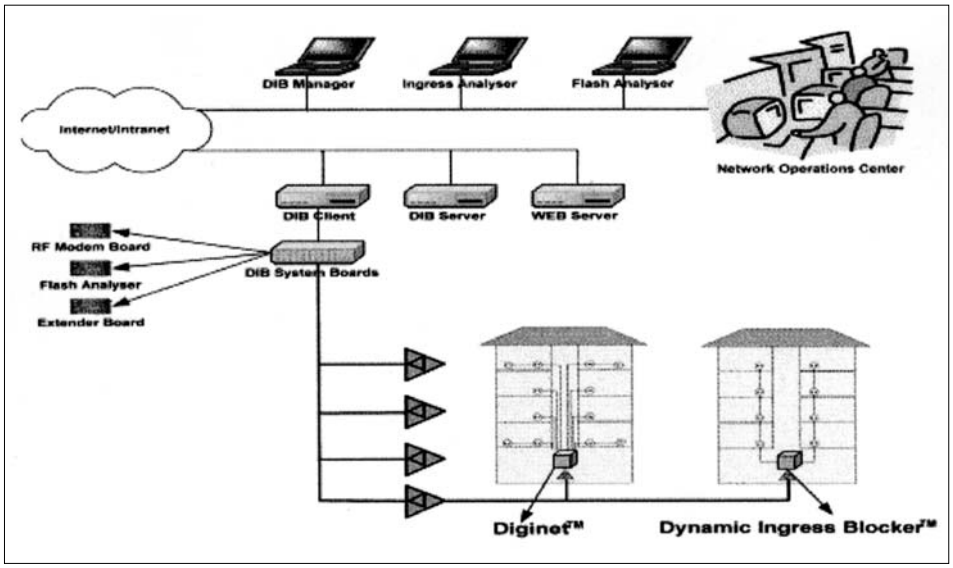
A minimálisan várható zajcsökkenés értékét egy 2000-es elosztóhálózatban, 20 háztartás/zajcsökkentő sűrűség és teljes átviteli kapacitás mellett az 2. ábrán mutattuk be. Az ábra nem veszi figyelembe, hogy egyes vivők adott időben egyazon zajcsökkentő egységen is átmehetnek. Ez a körülmény a zajelnyomást elvben tovább javítja, de a gyakorlatban nem számottevő mértékben, mivel valószínűtlen, hogy 20 vivőre 20 zajcsökkentő essen.

A visszirányú átviteli kapacitás növelésének hatékony módja tehát minél kevesebb vivő alkalmazása, minél nagyobb adatsebességekkel. Mint láttuk, a DIB™-et egy DOCSIC-t alkalmazó 2000-es elosztóhálózat területen alkalmazva megvalósítható a vivőnkénti adatsebesség növelése 10,24 Mb/s-re. Maximum 10 vivő egyidejű alkalmazásával 77 Mb/s kapacitásnövekedés érhető el, amely a nagy hálózati penetráció biztonságos megvalósításához elegendőnek látszik.

10 dB C/I a szabványos (DOCSIS/QPSK/2,56 Mb/s) kábelmodemek működésének végső határa. A megfelelő IP működéshez ajánlott rendszertartalék szintén 10 dB. A DOCSIS-ra vonatkozó ajánlásokkal összhangban ez a fejállomáson 20 dB C/I követelményt jelent.

Mint a fenti számításokból látjuk, egy tipikus 2000 előfizetős elosztóhálózat C/I-je a CMTS-nél frekvencia-

sávonként kb. 10 dB. Ennek alapján 2,56 Mb/s-nál nagyobb sebességű QPSK alkalmazása zajcsökkentés nélkül nem ajánlatos. A DIB™ alkalmazásával várható, hogy a területről eredő C/I közel azonos lesz azzal az elosztó hálózatéval, amelyikből a kábelmodem adása érkezik. A jellemző értékek várható nagyságrendje kis kapacitású elosztóhálózatoknál 30, nagy kapacitásúaknál 20 dB. E határértékek teljesülésével a QAM-16 alkalmazása lehetséges, s ezt a próbaüzem tapasztalatai is megerősítik.



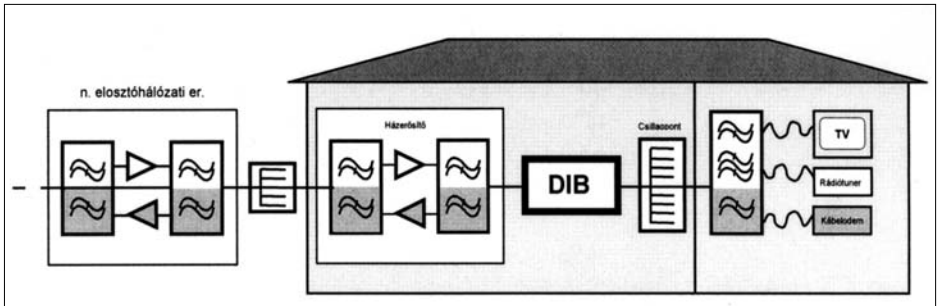
4. ábra

4. A DIB™ szolgáltatásai

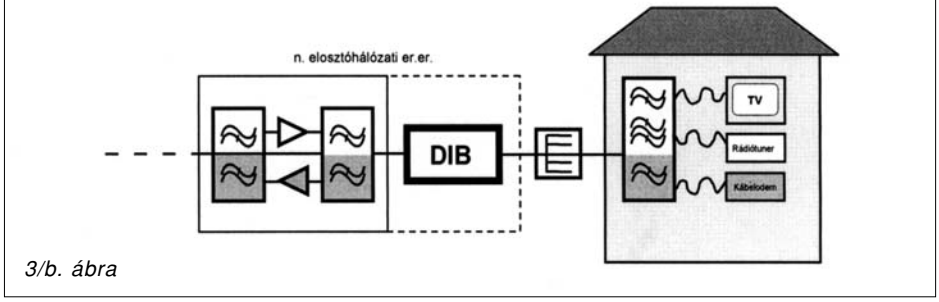
A zajelnyomás hatékonysága műszaki szempontból annál jobb, minél kisebb a zajcsökkentő egységekre eső háztartások száma. A gazdasági optimum ennek nyilvánvaló ellentéte. A megfelelő kompromisszum a 25-30 háztartás/zajcsökkentő egység, melynek alapján az egységek ésszerű beépítési pontja lakótelepi környezetben a házerősítő *(3/a. ábra)*, míg családiházas övezetben az utolsó elosztóhálózati RF erősítő *(3/b. ábra)*. Utóbbi esetben az egység az erősítő részét is képezheti.

A zajcsökkentő egységek intelligens transzponderekkel is felszerelhetők, amelyekkel a rendszer bővített szolgáltatást nyújt. Ezek az RF modem egységekkel (RF Modem Boards – RMB) a robusztus és üzembiztos HMS/DIB alapú FSK rendszerben kommunikálnak a hálózaton keresztül.

A hálózatba hatoló zaj intenzitásának, időtartamainak és frekvenciatartományainak figyelését (ingress monitoring), a problémás hálózatrészek lekapcsolását és pilotvezérlést a bővített verzió teszi lehetővé. A problémás hálózatrész lekapcsolási lehetőségével a szabotázs és meghibásodások, okozta károk csökkenthetők. A riasztási funkciók a manuális beavatkozásokhoz szükséges információkat szállítják, de a visszirány lekapcsolásának közvetlen vezérléséhez is felhasználhatók. Az erősítők előre- és visszirányú pilotokkal figyelhetők, melyeket egy gyorsidejű változáselemző egység (Flash Analyser) vizsgál. Az előre-irányú pilotot az RF Modem állítja elő és a zajcsökkentő egység méri. Az előre és visszirányú pilotok koordinációja az RMB egységben történik.



3/a. ábra

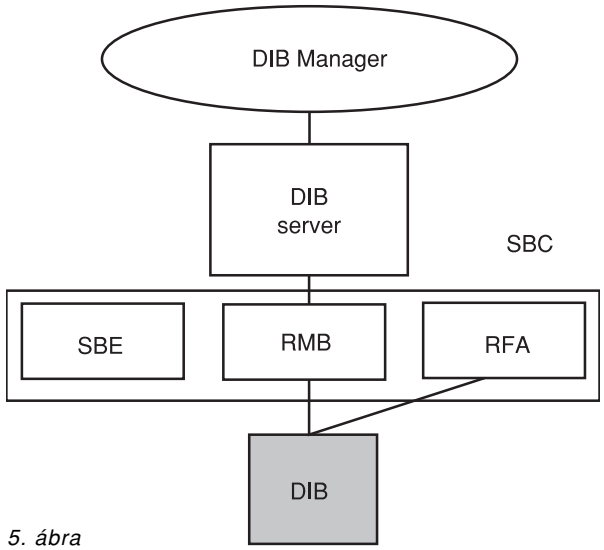


3/b. ábra

A rendszer elvi felépítését a *4. ábra* szemlélteti.

A rendszer-egységeket befogadó betét (System Board Chassis – SBC) a központi egységeket tartalmazza. A betét 4U magas standard 19” szekrénybe helyezhető. A rendszer minden adatát és kommunikációját a DIB szerver kezeli.

A rendszer Interneten/Intraneten keresztül vezérelhető. Ez bármely standard böngészővel (Internet Explorer, Netscape) használható. A bővítő egység (System Board Extender - SBE) segítségével a rendszer az SBC betétbe helyezhető további rendszer-egységekkel bővíthető *(5. ábra).*



5. ábra

5. A visszirányú zaj mérése

A behatoló visszirányú zajimpulzusokat a zajcsökkentő egységek folyamatosan mérik és az eredményeket tárolják. Ezen adatok, a behatoló zajokat elemző egységek (Ingress Analysis Tools) felé kerülnek továbbításra, melyek segítségével a hálózat minősége a telephelyen szemléltethető. Ezen információk hibabehatároláshoz, hálózatfenntartáshoz és minőségelemzéshez használhatók. A visszirányú gyorsidejű változásokat elemző egység (Return Flash Analyser – RFA) kettős feladatot lát el:

– a kis- és nagyszintű visszirányú pilotok mérése,
– a visszirány egészének,
  vagy kiválasztott részeinek mérése.

A mérést RF szinten, nagysebességű, közvetlen mintavételezéssel végzik. A specifikusan mérendő hálózatrész kiválasztásához az elemző egység mellett egy visszirányú multiplexert is alkalmazni kell.

A visszirány méréséhez középfrekvenciára (KF) keverést végeznek és az analízist itt végzik. E módszer korlátja, hogy a lekevert KF jel a visszirány teljes sávszélességét nem fogja át. A teljes sáv egyidejű megjelenítése így nem is lehetséges.

Az RF jelek közvetlen mintavételezése egy a visszirány sávszélességénél legalább kétszer nagyobb mintavételi frekvenciával (legalább 150 MHz) a visszirány teljes és korlátlan idő- és frekvenciatartomány analízisét teszi lehetővé. Az alkalmazott digitális kvantálási eljárás a jeltartalom minőségének megtartásához megfelelő felbontást biztosít. A közvetlen mintavételezés a csúcs-, átlag- és RMS analízist egyaránt lehetővé teszi úgy a frekvencia-, mint az időtartományban. A visszirányú csatornát elemző egységben (Flash Analyser) alkalmazott eljárás egy rendkívüli jelfeldolgozó kapacitásra épül.

Összefoglalva, a dinamikus visszhangzárral (DIB™ – Dynamic Ingress Blocker) a kábeltévé-hálózatok minősége nagy mértékben javítható.

Irodalom

[1] Noise in the Return Path
(Publikáció/www.spacenet.se)
[2] DYNAMIC INGRESS BLOCKING –
New Revolutionary Technology for Two-way Upgrade
(Rendszerismertető – SpaceNet Communications AB, Sweden 2003)

Hírek

Az Ericsson bevezeti Expander megoldását a fejlődő piacokon

Jelenleg a mobil-előfizetés penetrációja mindössze 21 százalékos a világon, ami összesen 1,34 milliárd előfizetőt jelent. Az előrejelzések szerint ez a szám 2008-ig további egymilliárd mobilfelhasználóval növekszik, amelynek nyolcvan százaléka a fejlődő piacokról származik majd.

Ami a hálózatüzemeltetőket illeti, az alacsonyabb költekezési hajlandóságú szegmensekben az előfizetők számának folyamatos növekedése jelentős növekedési potenciállal rendelkező, érintetlen piacot jelent, amely nyereségessé tehető. Az Ericsson Expander megoldásainak felhasználásával a fogyasztók alacsony költekezési hajlandósága többé nem akadálya a hálózatüzemeltetők nyereséges működésének. A költségcsökkentés legjobb módja a rádiótelephelyek számának csökkentése. Az Ericsson meggyőződése, hogy a telephelyek számát a lehető legkevesebbre csökkentő megoldás sokkal nagyobb megtakarítást eredményez, mint olcsó radió-bázisállomásokon alapuló megoldások alkalmazása. A jelenleg alkalmazott rádiókabinetek kapacitásának növelésével lehetővé válik a zökkenőmentes és költséghatékony bővítés, ha a megnövekedett forgalmi igények úgy kívánják.

A bevezetés első fázisa új rádiófunkciók bevezetését jelenti a meglévő berendezések legkedvezőbb kihasználásával. A megoldás egyszerre kínál nagyobb cellalefedettséget és az ugyanazon a bázisállomáson belül rugalmas kapacitásbővítést.

Távközlés a villamos hálózaton
(Power Line Telecommunication)

LÖCHER JÁNOS

Budapesti Műszaki és Gazdaságtudományi Egyetem, Villamosenergetika Tanszék

locher@vmt.bme.hu

Kulcsszavak: Internet, szélessávú csatlakozás, on-line hozzáférés, OFDM

A villamoshálózati távközlés (Power Line Telecommunication) egy új technológia, amely a meglévő kisfeszültségű villamos hálózatot használja berendezések közötti átvitelre. A villamoshálózat ilyen célú felhasználása nem új ötlet. Már régóta használják különböző kapcsolókészülékek vezérlésére, vagy telefonkapcsolat létrehozására. Ezek minősége és a rajtuk megvalósítható szolgáltatások, viszont már korántsem elegendőek napjaink megnövekedett igényeinek kielégítésére. Az Internet terjedése meghozta az igényt egy mindenki számára elérhető szélessávú adatkapcsolatra. Az új digitális modulációs eljárások pedig megteremtették annak a lehetőségét, hogy a villamos hálózatot használhassuk fel ilyen célból.

Az Internet terjedésével megnőtt az igény a szélessávú adatkapcsolat mind szélesebb körű kiépítésére. Ez az igény hozta magával azokat a megoldásokat, amelyek egy már meglévő hálózatot használnak fel a szélessávú Internet-hozzáférés biztosítására. Ilyenek az analóg telefonvonalon működő ISDN, vagy ADSL rendszerek, de ezek közé sorolhatóak a kábeltelevízió rendszert felhasználó kábelmodemes megoldások is. Ezek persze csak olyan helyeken működőképesek, ahol a felhasznált hálózat elérhető.

Létezik egy ezeknél lényegesen nagyobb hálózat, ami szinte minden olyan helyen hozzáférhető, ahol az adatátvitel egyáltalán szóba jöhet. Ez a hálózat pedig a kisfeszültségű villamosenergia elosztó rendszer.

Ebben a cikkben a villamoshálózati távközlés (Power Line Telecommunication – PLT) felhasználásának lehetőségét szeretném bemutatni szélessávú adatkapcsolatok létrehozására.

PLT rendszerek csoportosítása

A PLT-t a felhasználás szempontjából két nagy csoportra lehet bontani. Az első a tipikusan házon belüli (Indoor), a második a házon kívüli (Outdoor) hasznosítás.

Az *Indoor alkalmazás* a PLT technológia jobban elterjedt változata. Ebben az esetben a már meglévő kisfeszültségű elektromos hálózatot használják az eszközök összekötésére. Az áthidalt távolságok általában rövidek, nem érik el a 100 métert. Tipikus felhasználás, amikor az összekötni kívánt berendezések, például a számítógép és perifériái egy lakásban találhatók. Ebből adódóan, célszerű 10 Mb/s nagyságrendű adatátvitelt megvalósítani.

Az *Outdoor alkalmazás* esetében a PLT-t épületek összeköttetésére használják egymással, vagy más hálózatokkal. Az áthidalt távolságok nagyobbak, mint az Indoor felhasználás esetén, de még ekkor sem érik el általában az 500 métert. A megnövekedett távolságok miatt a sebessége legtöbbször kisebb, mint az előző esetben. Outdoor felhasználás esetén a csatornakapacitást általában nem szimmetrikusan osztják el a le és felmenő irányban.

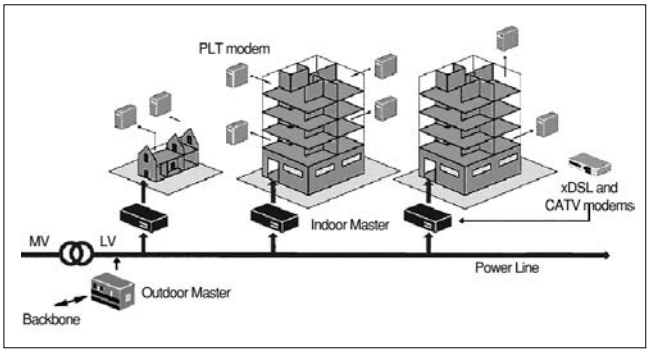
PLT hálózat felépítése

A PLT technológia nagy előnye, hogy különböző topológiájú hálózatokon is használható. A legelterjedtebb megoldások azonban a fa struktúrát alkalmazzák. Egy így felépített PLT hálózatot mutat be az *1. ábra.*

Egy hálózat általában egy transzformátorkörzetet fed le, ám semmi akadálya, hogy egy transzformátorkörzeten belül több hálózat is üzemeljen. Az ábrán látható, hogy az összeköttetés pont-multipont jellegű. Ebből adódóan kell lennie egy fejállomásnak, ami a hálózat működését vezérli. Ezt angolul Outdoor Master-nek (OM), vagy más terminológiában HeadEnd-nek (HE) hívják. Ezen az egységen keresztül kapcsolódik a PLT cella a többi hálózati részhez. Elhelyezkedését tekintve nincs kitüntetett helye. A hálózaton belül bárhol felszerelhető, ahol a működésének megfelelő feltételek biztosítva vannak.

Minden épület egy házi elosztón keresztül csatlakozik a hálózatra, ezt angolul Indoor Master-nek (IM), vagy

1. ábra PLT hálózat felépítése



másképp HomeGateway-nek nevezik. Ennek a berendezésnek a feladata, hogy összekösse az egy épületen belüli eszközöket a hálózat többi részével. A házon belüli forgalmat elválasztja a házak közötti forgalomtól, így az egyik házon belüli forgalom nem zavarja a többi ház szolgáltatásainak működését.

A felhasználók egy PLT modemen keresztül csatlakoznak a hálózathoz. Ez az egység a hálózati hozzáférés minden feladatát elvégzi, kezelést nem igényel. Minden funkciója automatikus és távolról irányítható. A felhasználó ezeket a berendezéseket a már megszokott módon kötheti hozzá a számítógépéhez, vagy telefonjához.

Felhasználási területek

A PLT legjellegzetesebb célja az Internet-hozzáférés biztosítása. Ezzel a legtöbb jelenlegi last-mile technológiánál nagyobb sebesség érhető el. Nincs szükség a betárcsázós hozzáféréseknél alkalmazott kapcsolat felépítési eljárásra, a 24 órás, folyamatos elérés könnyedén megvalósítható.

Második legelterjedtebb felhasználása a telefonbeszélgetések megvalósítása VoIP (Voice over IP) technológia segítségével. Összekötve a PSTN hálózattal lehetőség nyílik PLT-n belüli és azon kívüli hívásokra, beleértve a nemzetközi hívásokat is. A digitális átvitel következtében az átviteli utak jellemzői nem befolyásolják a hangminőséget. Titkosítási algoritmusok alkalmazásával a beszélgetések lehallgatása megnehezíthető.

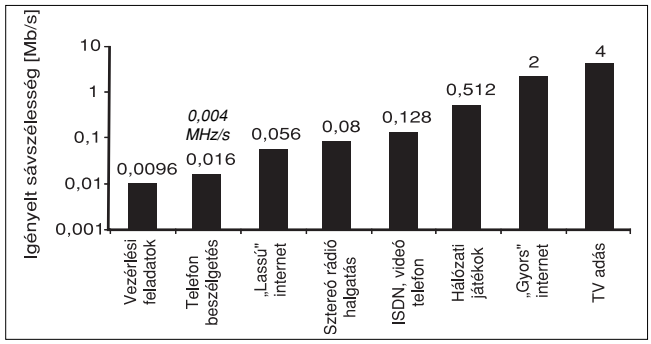
Az épületen belüli különböző informatikai, automatizálási rendszereket PLT segítségével össze lehet kötni egymással, vagy a felügyeleti rendszerrel. Lehetőség nyílik arra is, hogy eleve PLT-t használó automatizálási rendszereket telepítsünk, megtakarítva ezzel a plusz kábelezések költségét.

Az áramszolgáltatók PLT segítségével könnyedén leolvashatják a fogyasztóknál elhelyezett mérőket. A mérőkben lehetőség nyílik a napszaknak, illetve a fogyasztásnak megfelelő tarifák váltására, ezáltal a mérő a fogyasztott kWh mellett az érte fizetendő díjat is kijelezheti.

Vagyonvédelmi rendszereknél kamerák, érzékelők jeleinek továbbítása, a napi 24 órás távfelügyelet szintén megvalósítható a segítségével.

Alkalmazások által igényelt sávszélességek

A különböző alkalmazások által igényelt sávszélességeket mutatja be az *1. grafikon,* melyen látható, hogy a legkisebb sávszélességet a vezérlési funkciókat ellátó, épületinformatikai rendszerek igénylik. Következő lépcsőfok a telefonbeszélgetések és a lassú Internet. Ez a ma széles körben elterjedt betárcsázós Internet hozzáférés sávszélessége. Álló- vagy mozgóképek átviteléhez azonban már jelentősebb sávszélességek kellenek. Egy PAL rendszerű színes TV-program és a hozzá kapcsolódó sztereó hang átviteléhez a követelményektől és a kódolástól függően 1-6 Mb/s szükséges. Ennek a megvalósítására mindenféleképpen valamilyen szélessávú kapcsolatot kell igénybe venni.

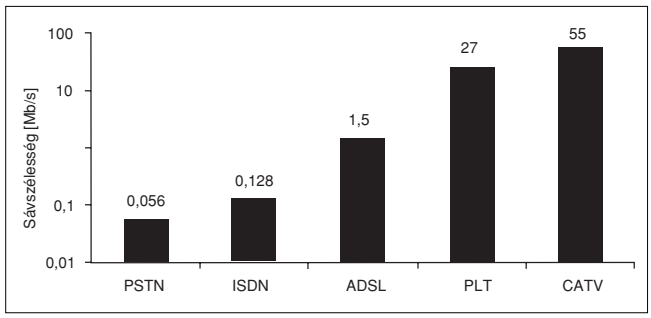


1. grafikon Alkalmazások sávszélesség igénye

Más (last-mile) technológiák által nyújtott átviteli sávszélességek

A *2. grafikonon* látható egy összeállítás más (vezetékes) last-mile technológiák által elérhető átviteli sávszélességekről. A grafikonról leolvasható, hogy a PLT által megvalósítható értéknél csak a CATV használata adhat jobb eredményt. Ennek elérésére a CATV technológia viszont speciális UHF tartományú átvitelre kifejlesztett kábeleket használ.

Itt érdemes megemlíteni, hogy mind a PLT, mind a CATV pont-multipont (busz) jellegű összeköttetést jelent, ezért a rendszer által megvalósított sávszélességen osztozik az összes rákapcsolt felhasználó.



2. grafikon
Különböző technológiák által elérhető sávszélességek

PLT átvitel megvalósításának nehézségei

A kisfeszültségű villamosenergia elosztó hálózatot nem tervezték nagyfrekvenciás működésre. Ezért ezek a kábelek nem árnyékoltak és a vezetők közötti szimmetria viszonyok sem hasonlíthatóak a sodrott érpáréhoz. Az árnyékolás hiánya miatt ezek a vezetékék antennaként viselkednek, ezáltal zavaró jeleket sugároznak a környezetükbe.

A kisfeszültségű villamosenergia elosztó hálózat csillapítása, hullámimpedanciája erősen változik a frekvencia, a hely és az idő függvényében. Ez nagymértékben megnehezíti az ilyen hálózatokat felhasználó távközlési rendszerek tervezését. A hagyományos modulációs eljárások az ellenőrizetlen terjedési utak és a reflexiók miatt nem használhatók.

A hálózat jellemzői a kapcsolat ideje alatt sokat változnak a fogyasztók gyakori ki és bekapcsolása következtében.

A meddő teljesítmény kompenzátorokban és a hálózati zavarszűrőkben alkalmazott kondenzátorok miatt a PLT jel szintje radikálisan lecsökkenhet. Ugyanezen sávot használó egyéb szolgáltatások zavarásának elkerülése érdekében viszont, a PLT átvitel szintjét nem lehet korlátlanul emelni.

Szabványosítási problémák

Európában jelenleg az EN50065/1-s szabvány vonatkozik a kisfeszültségű hálózatok másodlagos, távközlési alkalmazására. Erre a célra lehetővé teszi a 3 kHz-től 148,5 kHz-ig terjedő sáv használatát. Ez a tartomány önmagában sem elegendő a szélessávú adatátvitel megvalósítására. A problémát nehezíti még, hogy a szabvány csak a 125-140 kHz-ig terjedő részsávot engedélyezi a hozzáférési protokollt alkalmazó átvitel számára. Előírja az alkalmazható modulációs eljárásokat és protokollokat. Az így kialakított berendezések ennek következtében kompatibilisek lehetnek egymással, ám a túl „szigorú” előírások megnehezítik az újabb technológiák bevezetését.

Az európai szabványosítással foglalkozó szervezetek előtt jelenleg elfogadásra vár egy új tervezet. Ez lehetővé teszi 9 kHz-től 30 MHz-ig terjedő sáv felhasználását PLT célokra. Ennek elfogadásával mód nyílik a szélessávú adatátvitel megvalósítására kisfeszültségű hálózatokon.

Problémákat vet fel az, hogy ez a sáv már részben foglalt. Itt működnek a rövidhullámú műsorszóró rádióadók, a tengeri hajózási navigáció, a rádiócsillagászat és nem utolsósorban katonai felhasználása is van. Emiatt igen fontos, hogy mérsékelni kell a PLT zavarójel kibocsátását.

A tervezett szabvány korlátozza a vezetékektől adott távolságban mérhető mágneses térerőt, oly mértékben, ami – az eddigi tapasztalatok alapján – nem okoz zavarást a többi szolgáltatás működésében. A szabvány nem foglalkozik viszont sem a vezetett zavarok kérdésével, sem a PLT rendszer felépítésével, berendezéseinek paramétereivel. Ez meglehetősen nagy szabadságot és ezzel együtt rugalmasságot ad a gyártók kezébe. Ezáltal minden olyan megoldás, amely megfelel a kibocsátott határértékeknek, szabványosnak tekinthető, habár ezek a rendszerek legtöbbször egymással nem kompatibilisek.

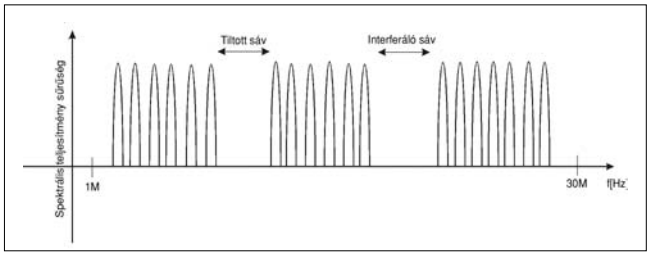
Modulációs eljárások

A hagyományos modulációs eljárások zaj és zavarérzékenysége miatt újfajta eljárásokat kellett kifejleszteni. Mivel az előírások nem kötik meg a technikai paramétereket, ezért sok megoldás született. Ezek közül az OFDM és a GMSK eljárás terjedt el a legszélesebb körben. Mindkét eljárásnak közös jellemzője, hogy megpróbálja szétszórni az átvinni kívánt információ energiáját a teljes rendelkezésre álló sávban. Az így kialakított spektrum a zajéhoz hasonlít. Ez a megoldás sokkal kedvezőbb a többi szolgáltatás zavartatása szempontjából. Növeli az átvitel impulzusszerű zavarokkal szembeni védettségét. Ilyen típusú zavarok esetén az átvitt információ kis része vész csak el, amit viszont a hibajavító kódolás alkalmazásával könnyű helyreállítani.

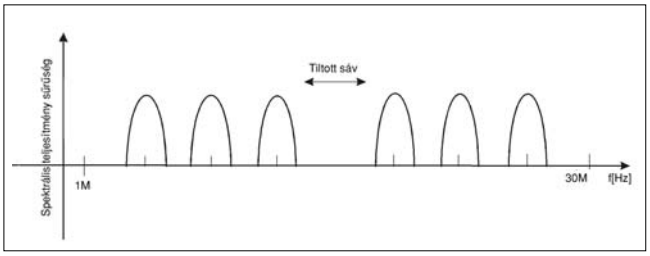
Az *OFDM (Orthogonal Frequency Division Multiplexing)* nem szoros értelemben vett moduláció, hanem egyfajta multiplexálási eljárás. Sok vivőt, tipikusan több ezret alkalmaz, néhány kHz-es raszter távolságban (2. ábra.) A vivőket legtöbbször QPSK, vagy QAM módszerrel modulálják. Ha a felhasználni kívánt sávban van olyan tartomány, aminek a használata tiltott, akkor az egyszerűen kihagyható. Ugyanez az eljárás alkalmazható, ha egy frekvenciatartományról kiderül, hogy például interferenciák miatt megengedhetetlenül nagy a zavarszintje. Ezzel a megoldással kielégítő a kompatibilitás a már meglévő szolgáltatásokkal.

A *GMSK (Gaussian filtered Minimal Shift Keying)*-t ma már az OFDM teljesen kiszorította az újonnan fejlesztett berendezéseknél, de még széles körben használatos a néhány évvel ezelőtt telepített hálózatokban. Ennél a digitális modulációs eljárásnál kevés, tipikusan 3-6 vivőt alkalmaznak. A vivők sávszélessége néhány MHz (3. ábra). Ezeket úgy kell elhelyezni a rendelkezésre álló frekvenciasávban, hogy azok ne zavarjanak egyéb szolgáltatásokat. A legkisebb zavarás a vivők frekvenciájának és amplitúdójának a helyes megválasztásával biztosítható.

2. ábra OFDM moduláció spektruma



3. ábra GMSK moduláció spektruma



	Gyártók		
Műszaki jellemzők	DS2	ASCOM	HomePlug
Adat sebesség	27 Mb/s le 18 Mb/s	4,5 Mb/s lel 4,5 Mb/s fel	14 Mb/s
Frekvencia tartomány	1-38 MHz	1,6-30 MHz	4,5-21 MHz
Vivők száma	1280	6	84
Moduláció	OFDM	GMSK	OFDM
Modulációs hatékonyság	7,25 b/s/Hz	0,75 b/s/Hz	1,16 b/s/Hz

1. táblázat Különböző PLT rendszerek összehasonlítása

Gyártók

Jelenleg a világban szinte kizárólagosan a DS2 cég által kifejlesztett lapkakészletet használják a szélessávú kapcsolatot biztosító berendezések gyártásánál. Emiatt a különböző gyárak által előállított termékek között lényegi különbség nemigen tapasztalható. A termékek közötti eltérés legtöbbször csak a hozzájuk adott szolgáltatásokban, szoftverekben és a külső megjelenésben található. A GMSK modulációt alkalmazó gyártók közül a legsikeresebb az ASCOM cég. Ők voltak Európában az elsők, akik tömeggyártásban állítottak elő PLT rendszereket. A legtöbb németországi és ausztriai rendszer a mai napig is az ő technológiájukat alkalmazza.

Említést érdemel még a HomePlug szervezet. Ez a szervezet felismerve, hogy milyen lehetőségek rejlenek a PLT házon belüli felhasználásában, létrehozott egy „ipari szabványt". Bármely gyártó szabadon kapcsolódhat a szervezethez és gyárthat HomePlug v1.0 kompatíbilis berendezéseket. Az így létrehozott termékek – köszönhetően a HomePlug aránylag „szigorú" előírásainak – általában kompatíbilisek egymással.

A különböző gyártók által létrehozott PLT rendszerek legfontosabb műszaki jellemzőit mutatja be az *1. táblázat.*

Összefoglalás

A PLT technológia műszaki szempontból ma már széles körben használhatónak tekinthető. Leküzdötte azokat a gyermekbetegségeket, melyek minden új technikákat alkalmazó rendszernél jelentkeznek Ezzel a megoldással szélessávú Internet kapcsolat biztosítható mindazon helyeken, ahol a villamos hálózat hozzáférhető.

Az EMC problémák tisztázását szolgáló szabványok és ajánlások jelenleg a kidolgozás különböző fázisaiban vannak. Megjelenésükig az adott ország frekvenciagazdálkodását végző szervezet általában „eltűri" az ilyen szolgáltatások üzemelését mindaddig, amíg bizonyítottan nem okoz zavartatást valamely engedéllyel üzemelő más rendszerben. Magyarországon még nem készültek alapos és megfontolt gazdasági számítások egy PLT eszközöket alkalmazó hálózat kiépítésének lehetőségeiről, ezért nehéz arra a kérdésre egyértelmű választ adni, hogy a hazai viszonyok között gazdaságosan üzemeltethető-e ilyen szolgáltatás. Európa számos pontján viszont sikerült ilyent megvalósítani és a levonható következtetések alapján várható, hogy ennek a technikának inkább a ritkábban lakott kisvárosi, falusi területeken van létjogosultsága.

A PLT technológia elterjedését akadályozza még a vele szemben tanúsított idegenkedés, ami valószínűleg abból ered, hogy még a szakemberek körében is kevéssé ismert ez a terület. Remélhetően a közeljövőben a rendszer elterjedésének ez nem lesz akadálya.

Hírek

A **Linksys®, a Cisco Systems** otthoni és kis irodai (SOHO) környezetekbe szánt szélessávú, vezeték nélküli termékcsalád keretében több újdonságot jelentett be. A multimédiás termék egy felsőkategóriás DVD lejátszót ötvöz egy Wireless-G médiacsatolóval, amely a PC-n tárolt digitális videó-, kép-és zenei anyagokat képes vezeték nélküli adatátvitellel TV-re vagy Hi-Fi berendezésre továbbítani. A készülék nagyfelbontású (HD) tévéken is képes lejátszani a DVD, CD vagy Video CD lemezeket. A beépített Wireless-G médiacsatolóval négyféle digitális tartalom (digitális videó, MPEG és DivX fájlok); digitális fényképek, digitális zene (MP3 és WMA fájlok), valamint különféle élő, internetes rádióműsorok játszhatók le. A termékcsalád másik újdonsága egy önálló Wireless-B médiacsatoló, melynek segítségével a különféle típusú digitális zenefájlok házi hangrendszeren hallgathatók meg. Az analóg és digitális világot Wireless-B (802.11b) hálózati kapcsolattal összekötő eszköz a digitális hangot – például a lejátszott MP3, WMA és más zenefájlokat – képes a PC-ről eljuttatni a zenekészülékre.

MiniVideo a Digitaniatól. Január közepe óta MiniVideo néven 15-20 másodperces videók tölthetők le mobiltelefonra. Európában harmadikként, hazánkban pedig elsőként jelentek meg a piacon. A GPRS-en keresztül, emelt díjas SMS-ben és WAP-on lekérhető minivideók minden Java-képes Nokia telefonon megjeleníthetők. A szolgáltatás mindhárom mobil szolgáltató hálózatán megfelelő készülékkel igénybe vehető. Egy videó letöltésének ára: 799 Ft+áfa. A felhasználó egy emelt díjas számra elküldi a kiválasztott videó azonosító kódját, amire egy válasz SMS-ben egy könyvjelzőt kap (szolgáltatói hírüzenet névvel jelenik meg a telefonon), melynek segítségével letöltheti a videót. Cégük tervei között szerepel a kapcsolatfelvétel a magyar televíziós társaságokkal, és további együttműködési megoldások kialakítása.

Konferencia a távközlésről: GLOBECOM 2003

FRIGYES ISTVÁN

BME

istvan.frigyes@mht.bme.hu

Az IEEE GLOBECOM konferenciája (Global Telecommunication Conference), melyet minden évben az amerikai Hálaadás-ünnep utáni héten rendeznek meg – 2003-tól kezdve rendszeresen Amerikában –, legutóbb december 1-5. között, San Francisco-ban volt. A másik nagy konferencia, az ICC, ezentúl mindig Amerikán kívül kerül majd sorra a nyári hónapokban. Bizonyára ismeretes a Híradástechnika olvasói előtt, hogy ez a két rendezvény méltán tekinthető minden évben a távközlés legjelentősebb összejöveteleinek, ahol a legújabb kutatási eredményekről számolnak be (persze, amint az mindig lenni szokott, sok feleslegességgel együtt). Számos, később alapvető jelentőségűnek bizonyult eredmény is e konferenciákon jelent meg először.

A 2003-as GLOBECOM – követve az utóbbi évek gyakorlatát – úgy volt megszervezve, hogy az „Általános konferencián" kívül többé-kevésbé önálló tematikus „Szimpóziumok" alkották annak egy részét. Sőt, ezúttal az előadásoknak csak kisebbik része tartozott az általános konferenciához, leginkább azok, melyek témája egyik szimpóziumba sem tartozott, vagy inkább, melyeknek azokban nem jutott hely. Az előadások szövege ezúttal kötetben nem jelent meg, csak CD-ROM formában.

A GLOBECOMok mindig egy – összefoglaló jellegű – plenáris előadással kezdődnek. Ezúttal a Siemens egyik személyisége adta a „Keynote Address"-t, a távközlés perspektíváiról. A meglehetősen lapos, kevés újdonságot és még kevesebb meglepő előrejelzést tartalmazó előadás – e beszámoló szerzőjének véleménye szerint – messzemenően nem tartozott a legjobbak közé.

Az összes témáról beszámolni, vagy akár az „általános érdeklődő" számára a legérdekesebbekről is, meghaladná e beszámoló kereteit, de a szerző ismereteit is (az előadások száma 900-nál több volt). A szimpóziumok témáját, azok méretét érdemes azonban felsorolni, elsősorban azért, hogy áttekintsük: mely témákat tekintik különállónak valamint, hogy lássuk, melyik téma iránt milyen az érdeklődés; ez megmutatja, hogy mely témák a legfontosabbak, melyekben folyik a legintenzívebb kutatás (egy-egy szekcióban 8 előadás volt):

Vezeték nélküli távközlés –	33 szekció (!),
Optikai hálózatok és rendszerek –	8 szekció,
A hírközlés biztonsága –	8 szekció,
Hírközléselmélet –	13 szekció,
Jelfeldolgozás –	10 szekció,
Köv. generáció hálózatai, Internet –	22 szekció,
Általános konferencia –	22 szekció.

Látható, hogy messze legnépszerűbb a vezeték nélküli téma – sőt, annak arányai még a fentinél is, mondhatjuk, kedvezőbbek: számos ehhez közelálló előadás, sőt teljes szekció is szerepelt a hírközlés-elméleti, a jelfeldolgozási vagy az általános konferencia keretében. E beszámoló szerzőjét is e téma érdekelte legjobban (a Wireless Symposium programbizottságnak volt tagja) – néhány szót tehát erről. Megint statisztika: legnagyobb számban két téma szerepelt: Bluetooth és ehhez hasonló rendszerek (PAN, ad-hoc), valamint az OFDM (Orthogonal Frequency Division Multiplexing) különböző problémái (6 illetve 5 szekció, vagyis 48 illetve 40 előadás).

Legérdekesebbnek, illetve a leginkább innovatívnak tűnő téma azonban az (ugyancsak nagy számban szereplő) MIMO rendszerek voltak. E tárgykör már túljutott az alapvető ismereteken, a vizsgálatok finomabb részletekre is kiterjednek. Így az optimális kódolás, kapacitás problémák „klasszikus" kutatása után olyan vizsgálatok, mint amilyen több antenna OFDM környezetben, többfelhasználós detekció MIMO átvitelnél, a rendszerek optimalizálása és mások. Érdekességként egy előadást emelünk ki: (persze nem állítva, hogy ez volt a legfontosabb, ilyenfajta értékelést nem is lehetne csinálni): MIMO átvitel optimalizálása olyan szempontból, hogy az adóvevő teljesítmény-fogyasztása a legkisebb legyen, az adóoldali, a vevőoldali jelfeldolgozás, az adóteljesítmény, a teljesítményerősítők linearitásának figyelembevételével (Jafarkhani).

900 előadás színvonaláról egységesen természetesen nem lehet beszélni. A szervezők helyes célkitűzése volt az átlagos magas színvonal biztosítása. Ez csak adminisztratív intézkedéssel érhető el, nevezetesen úgy, hogy eleve kitűzik, hogy a beküldött előadások milyen részarányát fogadják el. Ezúttal az elutasítás arányát meglehetősen magasan, 70%-ban állapították meg. Vagyis az egyes szimpóziumok valamint az általános konferencia program bizottsága az oda küldött vagy oda utalt előadás-javaslatoknak mindössze 30%-át fogadta el, persze a legmagasabbra értékelt 30%-ot.

(Zárójelben egy nem egészen ide tartozó megjegyzés. Minthogy ezúttal, de más hasonló konferenciákon is, a döntés alapja nem rövid összefoglalás, hanem a teljes szöveg, valamint minden kéziratot hárman bírálnak el, a szerzőnek az a véleménye, hogy ilyen publikáció tudományos értéke nem kisebb egy folyóirat cik-

kénél. Talán érdemes lenne, ha a tudományos fokozatokat odaitélő szervek megfontolnák: valóban indokolte az előbbiek hátrányára megkülönböztetni e két típusú publikáció tudományos értékét, amint azt a jelen szabályzatoknak megfelelően teszik.)

A 2003-as GLOBECOM programjában újdonság volt a „Tervezők és fejlesztők fóruma". Ez összesen 28 szekcióban szemináriumokat, kerekasztal-beszélgetéseket és egyéni előadásokat tartalmazott, elsősorban nem kutatóknak, hanem a cím szerinti résztvevőknek szánva. E különválasztást az indokolja, hogy – ellentétben a mintegy 20 évvel ezelőtti hasonló konferenciákkal (a szerző, ki 1982-ben vett először részt ilyenen, maga is tapasztalta ezt a tendenciát) – az ipar érdeklődése folyamatosan csökken, gyakorlatilag teljesen átadva a helyet az egyetemeknek, kutatóintézeteknek. Az IEEE, választott hivatásának megfelelően, nem elégedett ezzel a helyzettel; a Fórumot ennek orvoslására, az ipar nagyobb érdeklődésének felkeltésére szánta. A kezdeményezés bizonyára sikerrel kecsegtet, noha a konkrét számokról a szerzőnek nincs tudomása.

Rövid tanfolyamok („Tutorials") és szakmai megbeszélések („Workshops") – e két típusú rendezvény (a konferencia megnyitása előtti és befejezése utáni napon) minden alkalommal jelentős érdeklődés mellett zajlik, ezúttal talán a megszokottnál nagyobb számban: 32 félnapos vagy egész napos tanfolyam volt, 4 Workshop mellett... Témájuk nagyrészt csatlakozott a szimpóziumok témájához. Néhány érdekesebb téma: többantennás rendszerek (3 ilyen tanfolyam is volt), Internet (3 tanfolyam), optikai hálózatok (2), érzékelő hálózatok (külön is felhívnám a figyelmet e téma jelentőségének szemmel látható növekedésére) stb.

Két magyar előadóval találkoztam, személyesen illetve a programfüzetben. Megérdemlik nevük megemlítését: Rónai Miklós és Tapolcai János.

HTE A konferencia megnyitása előtti napon tartotta az IEEE Communiction Society (ComSoc) találkozóját különböző országbeli testvér egyesületeivel (Sister Society Summit). Ebből at alkalomból került sor ilyen testvér-egyesületi megállapodás ünnepélyes aláírására a HTE és a ComSoc között. A megállapodást a két egyesület elnöke írta alá. Az együttműködés tartalmának és jelentőségének ismertetése nem része ennek a beszámolónak, arról a Híradástechnika más helyén vagy a HTE Hírlevelében bizonyára szó esik majd.

Gondolatok az „elektronikus hírközlés" szóhasználatról

JUTASI ISTVÁN

Az elektronikus hírközlésről szóló 2003. évi C. törvény szabályozza 2004. január 1-től hazánkban a távközlést. Az „elektronikus hírközlés" elnevezés az EU Irányelvekből átvett „electronic communications" tükörfordítása.

A törvény szerint az „elektronikus hírközlési tevékenység", olyan tevékenység, amely bármely értelmezhető formában előállított jel, jelzés, írás, kép, hang vagy bármely természetű egyéb közlemény elektronikus hírközlő hálózaton keresztül, egy vagy több felhasználóhoz történő eljuttatását szolgálja.

A törvény nem határozza meg, hogy mit ért elektronikus hírközlő hálózat fogalmán, de – a jelenlegi fogalmaink szerint – nem tartozik e fogalomkörbe sem az elektromos hálózat (pl. előfizetői hurok), sem az optikai kábelhálózat, vagyis a jelenlegi hálózatok 2/3-ára a törvény ebben a formában nem vonatkozik. Sőt a törvény ezt a diszkriminációt kiterjeszti a már meglévő hálózatokra is, azzal, hogy kijelenti, ahol az eddig kiadott jogszabály távközlést említ, ott elektronikus hírközlést, ahol távközlési építményt említ, ott elektronikus hírközlési építményt kell érteni.

A hazai szóhasználat pontosan tudja, mit kell érteni távközlés alatt, törvényeink (kivéve az említettet), alacsonyabb jogszabályaink, tankönyveink, cégek nevei, stb. mind-mind a távközlés kifejezést használják.

A távközlés a híradástechnikai szakma jól körülhatárolt, elismert és széleskörűen használt fogalma, amit egy kellően nem értelmezhető, divatkifejezéssel felváltani enyhén szólva értelmetlenség. A magyar nyelv az egyszerűségre törekszik és előbb utóbb kiveti az idegen eredetű szavakat (például a tükörfordításból származókat...), főleg akkor, ha egytagú helyett, két tagot használ.

A magyar nyelv védelme érdekében már törvényünk van arra, hogy az utcai feliratok magyar nyelvűek legyenek, magyar szavak, fogalmak kerüljenek kiírásra. Ezek után elvárható az is, hogy egy rendkívül nagyjelentőségű törvényben is a magyar nyelvben már elfogadott, jól meghatározott kifejezés, a távközlés maradjon meg.

Az EU-val való jogharmonizáció kapcsán különösen veszélyesek a tükörfordításból származó mesterkélt kifejezések használata, különösen akkor, amikor megfelelő magyar kifejezéssel rendelkezünk. A távközlés szó használatának fentiek szerinti mellőzése szolgáljon tanulságul és egyúttal kiindulásul az elkövetett hiba kijavítására.

Iránymérés adaptív antennarendszerrel

NÉMETH ANDRÁS

ZMNE-BJKMFK, Katonai Távközlési és Telematikai Tanszék,
anemeth@bjkmf.hu

FOLKMANN VIKTOR

Bonn Hungary Electronics Kft.
folkmannv@freemail.hu

Kulcsszavak: mobil távközlés, elektromágneses környezetszennyezés, titkosítás, hullámtan

A mobil távközlésben az előfizetők számának gyors növekedése, a szolgáltatások bővülése és a fokozódó verseny szükségessé teheti új módszerek bevezetését a rendelkezésre álló frekvenciák gazdaságosabb felhasználása érdekében. Ennek leghatékonyabb eszköze lehet az űrkutatásban, valamint a műholdas műsorszórásban már alkalmazott adaptív antennarendszerek alkalmazása. Ezek bevezetése azonban számos kérdést vet fel mind hardver mind szoftver oldalról.

Bevezetés

Az adaptív módszerekkel történő iránymeghatározás fontos szerepet tölthet be a mobil távközlés területén. A bázisállomás egy-egy tűnyalábbal követi a forgalmat bonyolító mobil készülékeket, ezáltal:

1) *A hálózat kapacitása növelhető:* A keskeny nyalábnak köszönhetően csökken az azonos frekvenciát alkalmazó cellákból érkező interferencia. Ez lehetőséget teremt adott területen a frekvenciakihasználtság javítására, ezáltal növelve a kiszolgálható felhasználók számát.

2) *A kisugárzott rádiófrekvenciás energia csökkenthető:* A sugárzás irányának jelentős korlátozásának köszönhetően lényegesen kisebb energia elegendő egy adott távolságra lévő mobilkészülékkel való kapcsolattartáshoz.

3) *Az elektromágneses környezetszennyezés* az előző pontban leírtak egyenes következményeként jelentősen csökken.

Az ilyen rendszereknek azonban nem csak polgári, hanem katonai alkalmazása is lehetséges:

A zavaró rádióadók bemérésére:
Hadszíntéren, az ellenség csapatainak kommunikációját megnehezítendő, gyakran működtetnek zavaró rádióadókat. Ezek hatása csökkenthető oly módon, hogy az antennarendszer karakterisztikájában nullhelyet illesztenek a zavaró források irányára.

Titkosítás:
A rádióforgalom lehallgatása megnehezíthető, ha az adóoldalon egy tűnyalábbal sugározunk a vevő irányába, ezáltal minimálisra csökkentve az egyéb irányokból történő vétel lehetőségét.

Célkövetés:
A hadszíntéren az egyes egységek (repülőgépek, harckocsik, hadihajók, kommandós egységek stb.) rádiócsatornákon keresztül tartják a kapcsolatot egymással és a parancsnokságokkal, azaz rádiófrekvenciás teljesítményt sugároznak ki. Megfelelő adaptív antennarendszerek alkalmazásával mozgásuk követhetővé válik…

A várható eredmények tükrében belátható, hogy az adaptív antennarendszerek kutatása fontos lehet, hiszen alkalmazási lehetőségei – egyéb technológiákat is bevonva (pl. mikrosztrip antennák) – szinte határtalanok, miközben a várható gazdasági és társadalmi hatásai sem elhanyagolhatók…

Mivel a témával foglalkozó szakirodalmakban és az Interneten sem találkoztunk hasonlóval, úgy döntöttünk, hogy építünk egy kísérleti adaptív iránymérő rendszert a GSM sávra, melynek segítségével a valóságban is vizsgálhatóvá válik az elv alkalmazhatósága, az algoritmusok hatékonysága, továbbá a hullámterjedés tulajdonságaiból adódó anomáliák hatásai. Ez segítséget nyújthat továbbá a felmerülő nehézségek megoldásában, új algoritmusok kidolgozásában és kipróbálásában, korábbi módszerek finomításában…

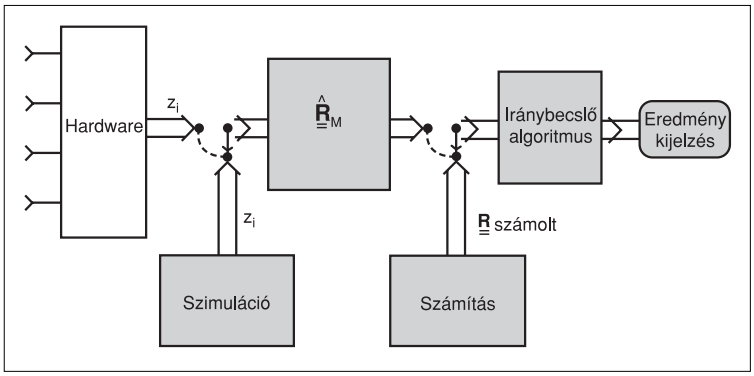
Cikkünkben kapcsolódni kívánunk a Híradástechnika folyóiratban megjelent [6] azonos témájú elméleti áttekintést adó írásához, ezáltal nem kívánunk foglalkozni elméleti alapozással, csak a működés szempontjából fontos, a megértéshez szükséges összefüggésekre hívjuk fel a figyelmet.

Szó lesz a rendszert alkotó, adatokat feldolgozó szoftver működéséről, valamint a mérést végző hardver felépítéséről és működéséről továbbá, az elkészült rendszerrel végzett mérések eredményeiről és további lehetőségekről.

Rendszer felépítése és működése

Az általunk készített rendszer esetén a térbeli mintavételezést a 900MHz-es sávban egy négyelemű antennasor végzi, ahol az elemek távolsága $\lambda/2$. (A Shannon féle mintavételi tétel térbeli adaptációjának megfelelően ez a maximális távolság, amelynél a spektrumban nem jön létre átlapolódás (időbeli frekvencia – térbeli frekvencia analógia)).

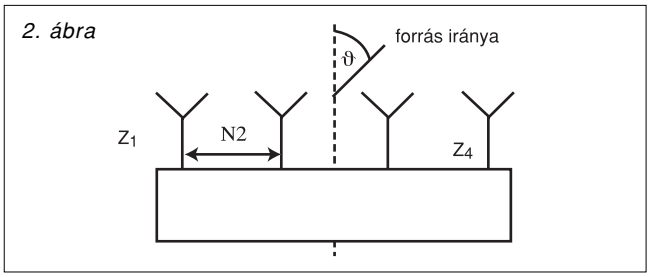
A rendszer blokkvázlata a következő oldalon, az *1. ábrán* látható.



1. ábra A rendszer blokkvázlata

Az első blokk tartalmazza a hardvert, melynek kimentén a mintavételi frekvenciának megfelelő időközönként rendelkezésre állnak az antennarendszer által vett vektorok.

Ezek soros porton keresztül jutnak a PC-be, ahol a szoftver a feldolgozás után grafikusan megjeleníti az eredményt. Az ábrán szürkével jelölt blokkokat szoftveresen valósítottuk meg. A program alkalmas iránymeghatározást végezni számítási modellek, szimuláció valamint valós mérések alapján (a hardver által előállított adatok fogadása, feldolgozása, megjelenítése). Az antennarendszerek elméletének megfelelően egy N-elemű sor irányténye zője felírható egy (N-1)-ed fokú polinommal, ami N-1 nullhelyet jelent a függvényben. Ebből következőleg a négyelemű sor maximálisan három irány becslésére alkalmas. A fázisközéppont, az antennarendszer geometriai közepe, míg a mért irány, az ebbe a pontba állított merőlegeshez képesti szögeltérés *(2. ábra)*.



Elsődleges feladatunk mindhárom esetben az autokorrelációs mátrix előállítása, ami definíciószerűen:

$$\mathrm{R} = E\{\mathbf{z}\mathbf{z}^{\mathbf{H}}\} = \lim_{k\to\infty} \frac{1}{k}\sum_{i=1}^{k} \mathbf{z}(t_i)\mathbf{z}(t_i)^{\mathrm{H}}$$

ahol $\mathbf{z}^{\mathrm{T}}=[z_1\ z_2\ z_3\ \ z_4]$ az antennarendszer mintavett vektora, *E* pedig a halmazátlag jelölése.

Számítási modellel végzett iránymeghatározáskor nem foglalkozunk olyan problémákkal, mint például az egyes források közötti fáziskülönbség, a zaj okozta torzítások, valamint egyéb, terjedésből adódó nehézségek. Úgy tekintjük, hogy az egyes források között nincs fáziskülönbség. A Gaussi zajt csak a teljesítményével vesszük figyelembe, vagyis úgy, mintha végtelen minta alapján lenne átlagolva (szórásnégyzet). Ekkor megtehetjük, hogy a forrásokat külön, egymástól függetlenül kezeljük és így végezzük a számításokat. A végén ezeket összegezve kapjuk a tényleges autokorrelációs mátrixot:

$$\mathrm{R} = \sum_{i=1}^{3} p_i \mathbf{z}_i \mathbf{z}_i^{\mathbf{H}} + \sigma^2 \mathrm{I}$$

ahol $\mathbf{p_i}$ az i-edik forrás által előállított teljesítmény a mérés helyén.

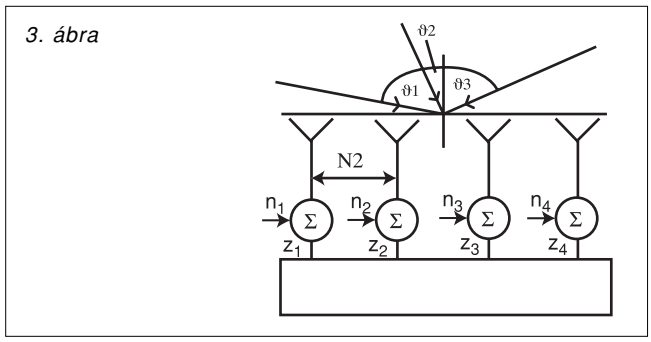
Egyetlen forrásra az autokorrelációs mátrix:

$$\mathbf{R} = \mathrm{p}\cdot\mathbf{z}\mathbf{z}^{\mathrm{H}}$$

ahol a **z,** négyelemű vektor tartalmazza az egyes antennákon jelenlévő fázist:

$$\mathbf{z}^{\mathrm{H}}=[\mathbf{e}^{-\mathrm{j}\pi\cos\theta(1-2.5)}\ \ \mathbf{e}^{-\mathrm{j}\pi\cos\theta(2-2.5)}\ \ \mathbf{e}^{-\mathrm{j}\pi\cos\theta(3-2.5)}\ \ \mathbf{e}^{-\mathrm{j}\pi\cos\theta(4-2.5)}]$$

Szimuláció esetén figyelembe kell venni az additív zajt, valamint azt hogy a gyakorlatban a különböző források jelei nem azonos fázisban érkeznek az antennákra. A rádióadók modulált jelet sugároznak, így a moduláció okozta fáziseltéréssel is számolni kell. Ezen tényezők modellezéséhez rendeljünk minden forráshoz a [–π,π] tartományon egyenletes eloszlású véletlen fázist, valamint minden antennán jelenlévő jelhez additív eloszlású Gaussi zajt *(3. ábra)*.



A fentiek alapján, három forrás esetén a mintavett vektor az alábbiak szerint alakul:

$$z_1 = \sqrt{p_1}\, e^{-j(\pi\sin\theta_1(1-2.5)+\phi_1)} + \sqrt{p_2}\, e^{-j(\pi\sin\theta_2(1-2.5)+\phi_2)} + \sqrt{p_3}\, e^{-j(\pi\sin\theta_3(1-2.5)+\phi_3)} + \sqrt{n_1}$$

$$z_2 = \sqrt{p_1}\, e^{-j(\pi\sin\theta_1(2-2.5)+\phi_1)} + \sqrt{p_2}\, e^{-j(\pi\sin\theta_2(2-2.5)+\phi_2)} + \sqrt{p_3}\, e^{-j(\pi\sin\theta_3(2-2.5)+\phi_3)} + \sqrt{n_2}$$

$$z_3 = \sqrt{p_1}\, e^{-j(\pi\sin\theta_1(3-2.5)+\phi_1)} + \sqrt{p_2}\, e^{-j(\pi\sin\theta_2(3-2.5)+\phi_2)} + \sqrt{p_3}\, e^{-j(\pi\sin\theta_3(3-2.5)+\phi_3)} + \sqrt{n_3}$$

$$z_4 = \sqrt{p_1}\, e^{-j(\pi\sin\theta_1(4-2.5)+\phi_1)} + \sqrt{p_2}\, e^{-j(\pi\sin\theta_2(4-2.5)+\phi_2)} + \sqrt{p_3}\, e^{-j(\pi\sin\theta_3(4-2.5)+\phi_3)} + \sqrt{n_4}$$

ahol: $\mathbf{p_i}$ az i-edik forrás teljesítménye, $\theta_\mathbf{i}$ az i-edik forrás beesési szöge, $\phi_\mathbf{i}$ az i-edik forrás véletlen fázisa, **n** az additív zaj teljesítménye.

Adott mintavételi időpontban az egyes antennákon lévő jelek, csak az útkülönbségből adódó fáziskülönbséggel térnek el egymástól. Ehhez szükség van arra a feltevésre, hogy ezen útkülönbség alatt modulációból származó fáziseltérés nincsen.

Ezek alapján az adott mintavételi időponthoz tartozó autokorrelációs mátrix a mintavett vektorból számít-

ható, míg a fázishiba átlagolással ejthető ki. A mintaszám növelésének a folyamat változási sebessége szab határt, hiszen a mérés eredményességének feltétele, hogy a mintavételezett folyamat adott stacioner, vagy legalább a mérési folyamat alatt stacionernek tekinthető, azaz kvázi stacioner legyen.

Az *M* minta alapján becsült autokorrelációs mátrix tehát a következő:

$$\hat{R}_{\mathbf{M}} = \frac{1}{M}\sum_{i=1}^{M} \mathbf{z_{ti}} \mathbf{z_{ti}^H}$$

Mérés esetén a mintavett vektort a hardver állítja elő, amelyből a mátrix meghatározása a fenti módon történik.

Az autokorrelációs mátrixot kiindulási paraméternek tekintve az iránymeghatározást különböző algoritmusok végzik, melyek pontosságban, dinamikatartományban, felbontásban, zavarállóságban térnek el egymástól. Az általunk használt három módszer által becsült spektrum:

$$S_{BARTLETT}(\omega) = E\{|\mathbf{s}^H\mathbf{z}|^2\} = \mathbf{s}^H(\theta)R\,\mathbf{s}(\theta)$$

$$S_{CAPON}(\omega) = \frac{1}{\mathbf{s}^T(\omega)R^{-1}\mathbf{s}^*(\omega)}$$

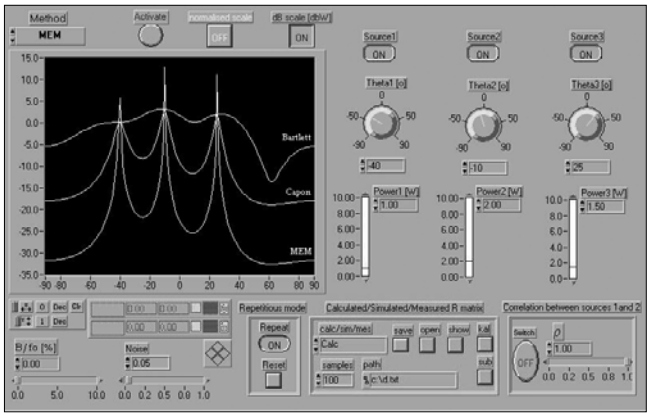
$$S_{MEM}(\omega) = \frac{1}{|\mathbf{s}^H(\omega)R^{-1}\delta|^2} \quad \text{ahol } \delta = [1\,0\,\ldots\,0]$$

Az első konvencionális módszer (Bartlett-becslés vagy Fourier-módszer), míg a második és harmadik adaptív algoritmus (Capon vagy MSINR, azaz maximális jel/zaj viszony módszer és MEM, azaz maximális entrópia módszer). Az adaptivitás leegyszerűsítve azt jelenti, hogy az antennarendszer karakterisztikája követi a vizsgált tér változásait. Az algoritmusok tulajdonságairól a későbbiekben még lesz szó.

A szoftver

Szoftverünk tehát a bemutatott rendszerben alkalmas számításon, szimuláción és mérésen alapuló iránybecsléshez szükséges számítások végzésére, az eredmények grafikus megjelenítésére. A kezelőfelület a *4. ábrán* látható.

4. ábra



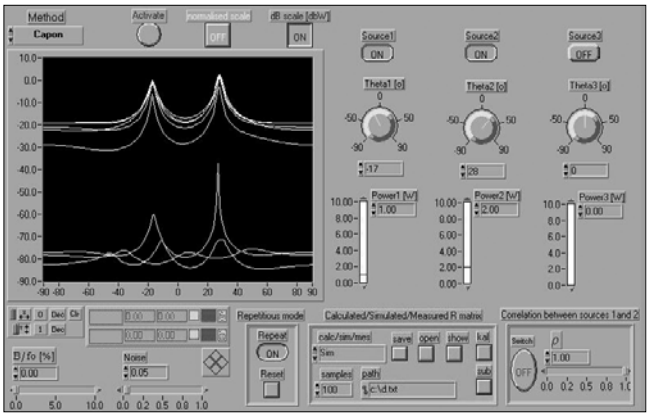
A felhasználó megjelenítheti az eredményeket lineáris, logaritmikus vagy normalizált skálán, továbbá lehetősége van összehasonlítás céljából a görbék egymásra rajzolására, a pontosabb leolvasás elősegítése érdekében pedig markerek használatára. Négy antennából álló rendszer, legfeljebb három irány becslésére alkalmas, így ennyi áll rendelkezésünkre számítás és szimuláció esetén. Ezek iránya és teljesítménye egymástól függetlenül folyamatosan, lineáris skálán beállítható. Szimuláció esetén tetszőlegesen beállíthatjuk a mintaszámot, zajt adhatunk a jelekhez, beállíthatjuk a sávszélességüket, valamint az első és második forrást korrelálttá tehetjük. Mindhárom üzemmódban (számítás, szimuláció, mérés) a korábban említett algoritmusokkal dolgozhatunk, a kapott eredményeket tárolhatjuk, majd később ismételten megjeleníthetjük. A 4. ábrán ezek alapján a következő beállításokat eszközöltük: számítási üzemmód, a források tulajdonságai sorrendben:

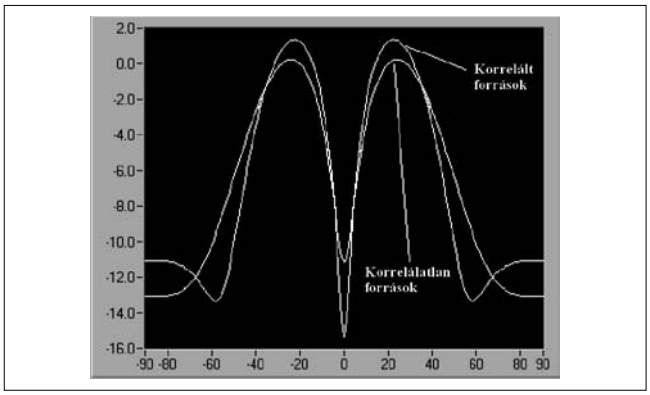
-40°, 1W; -10°, 2W; 25°, 1.5W, mindhárom módszer megjelenítése. A kijelzőn látható a különböző algoritmusok két legalapvetőbb tulajdonsága a dinamika és felbontás. Steril körülmények között tehát az adaptív modellek messze fölülmúlják mindkét paraméterben a konvencionális módszert. Csekély zavaráló képességük miatt azonban gyakorlati körülmények között kevésbé meggyőző eredményt adnak. Az *5. ábra* a mintaszám növelésének hatását mutatja be Capon módszer esetén (lentről fölfelé a mintaszám nő). Megállapítható, hogy a megbízható méréshez 100 minta már elegendő. (A mintaszám az átlagolt mérések számát jelenti.)

A korrelált források hatása a *6. és 7. ábrákon* figyelhető meg (Bartlett – balra, Capon – jobbra). Megállapítható, hogy míg a Bartlett becslés esetében alig befolyásolja a mérést, addig az adaptív algoritmusok pontossága és dinamikája jelentősen romlik.

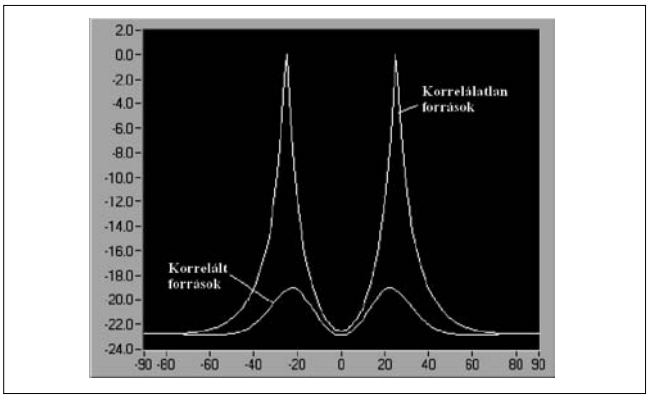
A *8. és 9. ábrán* a sávszélesség hatása vizsgálható (B/f_0 = 0% és B/f_0 = 10%). Ez alapján szintén az adaptív algoritmusok gyengesége látszik: a Bartlett becsléssel kapott eredmény gyakorlatilag érzéketlen a spektrum kiszélesedésére, a Capon módszer esetén viszont jelentősen csökken a dinamika (6dB).

5. ábra

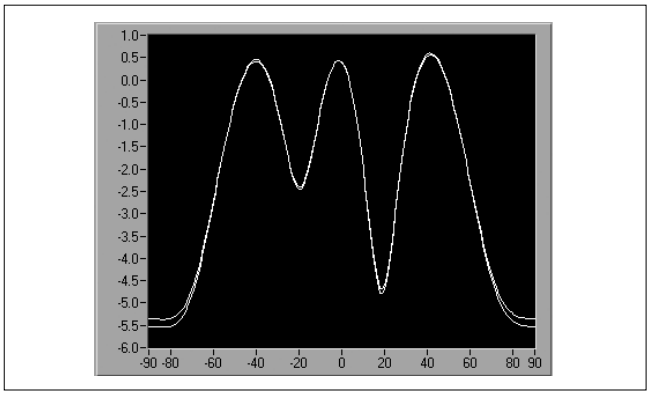




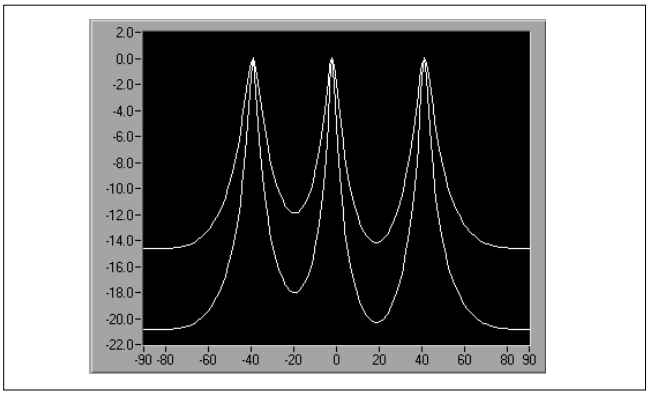
6. ábra: Bartlett



7. ábra: Capon



8. ábra: Bartlett



9. ábra: Capon

Összességében belátható, hogy az adaptív algoritmusok ideális esetben messze felülmúlják a Bartlett becslést, a valós körülmények azonban jelentősen rontják azok hatékonyságát.

Természetesen végtelen azoknak a beállításoknak a száma, melyek a fenti módon megvizsgálhatóak. Célunk ebben a fejezetben csupán az volt, hogy a program működését néhány fontosabb esetet kiragadva bemutassuk.

Hardver

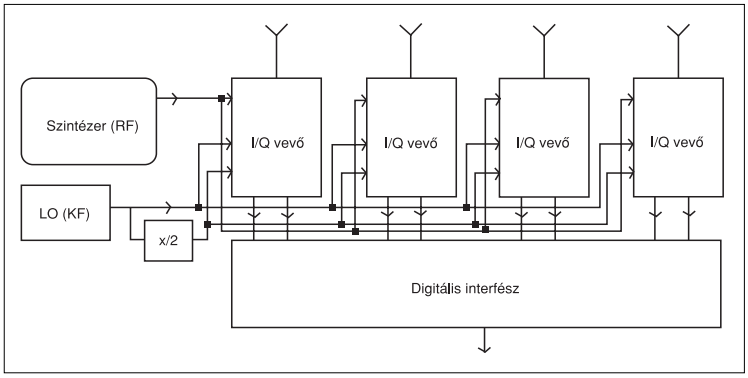
Valós mérések végzéséhez szükségessé vált a mérést végző eszköz megépítése, melynek blokkvázlata a *10. ábrán* látható.

A tervezés alapvető szempontja a programhoz való illeszthetőség volt, tehát négyelemű, lineáris struktúrájú antennarendszert kellet tervezni, ahol az elemek távolsága λ/2 a 900MHz-es GSM uplink sávban.

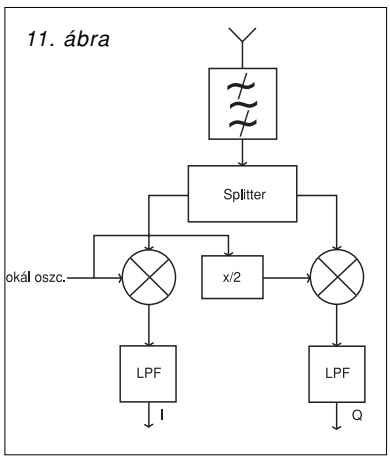
A rendszer működése leegyszerűsítve így írható le: az antennák térben mintavételezik az elektromágneses teret, amely valamilyen amplitúdó és fázisképet hoz létre. Ideális esetet feltételezve az egyes antennák kimenetein megjelenő jelek csak fázisban fognak eltérni (úthosszkülönbségből adódó fáziskülönbség). A jeleket a vevők erősítik, keverik, szűrik, előállítják az I és Q csatornákat, melyeket a digitális interfész mintavételez és továbbít a számítógépnek. A szoftver a hardvertől kapott minták átlagolása után meghatározza a kívánt források irányát. Ez alapján szükségünk volt négy I-Q vevőre, egy lokáljel és egy digitalizáló áramkörre, valamint egy RF szintézerre.

A rendszer alapeleme tehát az I-Q vevő, melynek elméleti felépítése a *11. ábrán,* az I és Q jelek jelentése pedig a *12. ábrán* látható.

10. ábra: A hardver felépítése



11. ábra



Működéséről csak annyit, hogy a kimeneten megjelenő I és Q értékek által meghatározott vektor eredőjének hossza a tér nagyságával lesz arányos, míg az I tengellyel bezárt szöge a forrás által előállított tér adott pontbeli fázisát jelenti a lokáloszcillátorhoz képest.

A keverést a valóságban, két fokozatban oldottuk meg, hiszen középfrekvencián a csatornaszűrés és erősítésszabályozás egyszerűbben megvalósítható, továbbá így nyílhat lehetőségünk a RF szintézer segítségével a sáv különböző vivőire történő ráhangolásra.

A második fokozatban a jelet az alapsávba keverjük a digitalizáló áramkör számára. A KF lokáljel előállítása, szétosztása, valamint az RF szintézer jelének szétosztása, egy nyomtatott áramköri lapon valósult meg.

A digitális interfész végzi a nyolc csatorna egyidejű mintavételezését és az adatok továbbítását soros porton keresztül a számítógépbe.

A hardver megépítéséről és beméréséről sok oldalt tele lehetne írni, ehelyett azonban most megelégszünk néhány fénykép közlésével.

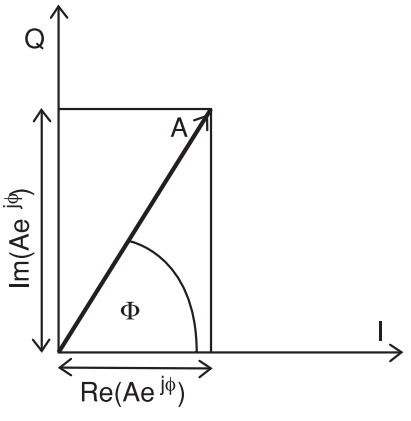
Mérések

A hardver elkészülte és bemérése után megkezdődtek a mérések. A forrás szerepét egy monopol antenna töltötte be, melyet jelgenerátorral gerjesztettünk.

Az első méréseket zárt térben (épületen belül) végeztük, de ezek csupán a rendszer működésének nagyléptékű vizsgálatára voltak alkalmasak. Hiteles mérések csak reflexiómentes környezetben végezhetők, ezért (kvázi) szabadtéri mérést végeztünk. Az így kapott eredmények már jóval meggyőzőbbek voltak, mint az épületen belüli mérések.

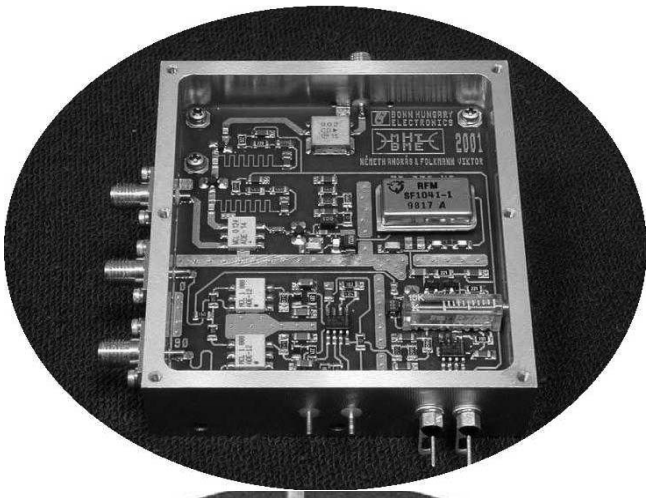
Az adóantennát először egy tisztán szinuszos jellel gerjesztettük, majd elvégeztük a méréseket modulált adójellel is. Az eredmények a *13. ábrán* láthatók. Az elméletnek megfelelően tapasztalható, hogy moduláció esetén a B/f_0 arány növelésével a mérés dinamikája csökken. FM moduláció esetén a szintcsökkenés annak tudható be, hogy SAW szűrő által meghatározott 200kHzes sávba a jelteljesítmények csak egy része jut. A hatás itt is a Bartlett-becslésnél érvényesül a legkevésbé, az adaptív módszerek a modulációra is érzékenyebbek.

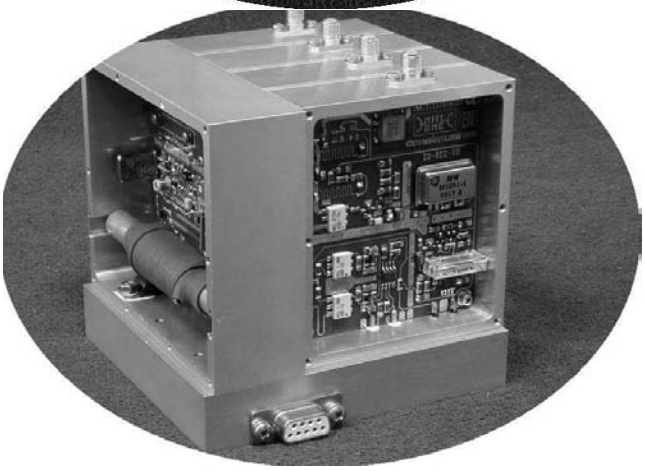
12. ábra

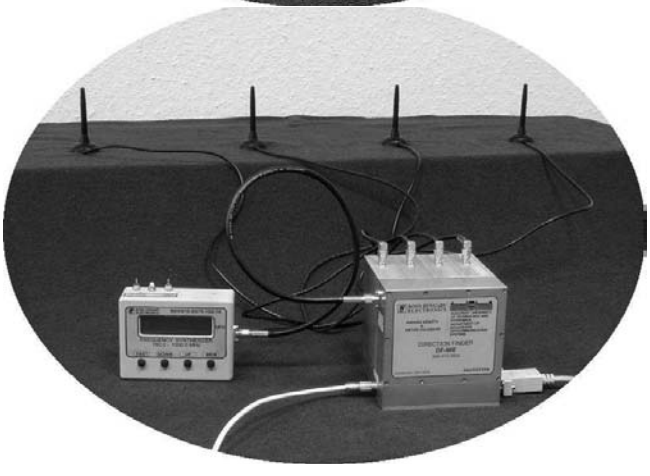


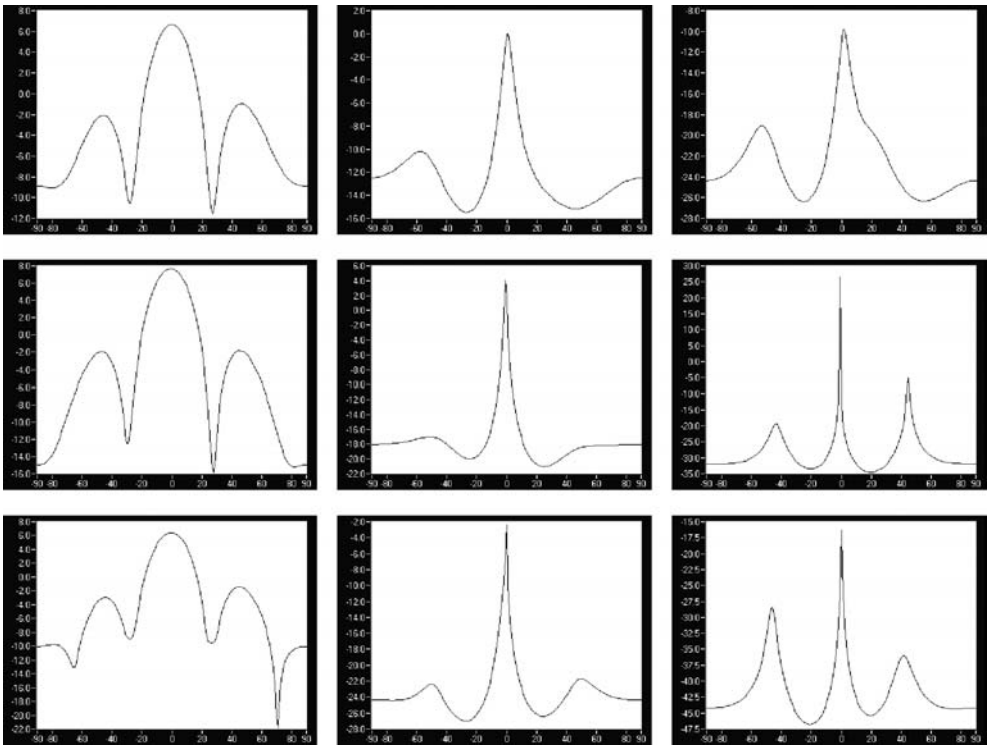
$I = Re(A \cdot e^{j\phi})$

$Q = Im(A \cdot e^{j\phi})$









13. ábra

Az itt megfigyelhető melléknyalábok valószínűleg a még mindig nem ideális mérési körülményeknek köszönhetők (reflexiók: fák bokrok, egyéb tereptárgyak, interferencia: a mérést a GSM sávban végeztük).

A mérések igazolták az egyes algoritmusok elméletben leírt tulajdonságait. Egyértelműen látszik, hogy az adaptív módszerek igen érzékenyek a valós körülmények közt általában jelenlévő zavaró tényezőkre (elsősorban a reflexiók miatt létrejövő korrelációra). Ezen a későbbiekben úgynevezett korrelációromboló algoritmusokkal lehet segíteni. Az adaptív algoritmusok hatékonyságát szintén nagymértékben befolyásolja a hardver precizitása (az I és Q csatornák közti szint- és fáziskülönbség stb.).

Konklúzió

Cikkünk célja egy, az általunk készített kísérleti iránymérő rendszer bemutatása volt, amely a későbbiekben felmerülő igényekhez igazodva továbbfejleszthető. A rendszer a szakirodalomban és szaksajtóban széleskörűen megtalálható elméleti alapokra épül, ezért a cikk csak minimális elméletanyagot közöl, és megpróbál a rendszer felépítésére, valamint a szimulációs és mérési eredményekre koncentrálni. Az iránymérő rendszerrel eredetileg mobiltelefonok irányát szerettük volna mérni, ez azonban olyan problémákat vetett fel, melyek megoldása meghaladta a rendelkezésre álló lehetőségeinket.

A rendszer a fentiek alapján jelenlegi állapotában kiválóan alkalmas további kísérletek elvégzésére, új algoritmusok kidolgozására, hatékonyságuk vizsgálatára, korlátaik behatárolására, több ilyen rendszer esetén pedig azok együttműködésének vizsgálatára. A valós alkalmazásokat tekintve az adaptivitásból adódóan az ilyen antennarendszerek felhasználhatóságának elsősorban csak a képzelet szab határt. Technikai korlát az egyes algoritmusok számításigényének jelentős növekedése az alkalmazott antenna elemszám függvényében, illetve az, hogy az adaptív antennasorok csak $\Theta = \pm 60°$-os tartományban (a színusz függvény kvázi-lineáris tartományában) adnak helyes becslést, ezáltal a teljes 360°-os tartomány lefedéséhez három ilyen (pl. mikrosztrip kivitelű) antennasorra lenne szükség. A számításigény növekedése kiváltképp akkor válik jelentőssé, ha a lineáris antennarendszerek mellett elkezdünk gondolkodni a kettő-, netán háromdimenziós elrendezések alkalmazásának lehetőségén. Összefoglalásként megállapíthatjuk, hogy számtalan olyan terület van, ahol sikerrel lehetne alkalmazni ilyen antennarendszereket, illetve az ezekből felépülő komplexumokat – például mobil bázisállomásként, vagy különböző rádióelektronikai felderítő rendszerekben.

Itt jegyezzük meg, hogy a rendszer önálló laboratórium és diplomatervezés keretében készült a Budapesti Műszaki és Gazdaságtudományi Egyetem Szélessávú Hírközlő Rendszerek Tanszékén. A hardver megvalósításához a BONN MAGYARORSZÁG Kft. nyújtott támogatást, melyért ezúton is köszönetet mondunk.

Irodalom

[1] Alfonso Farina: Antenna-Based Signal Processing Techniques for Systems
Artech House, Norwood, 1992.
[2] Szekeres Béla, Nagy Lajos, Petre Péter:
Antennák és hullámterjedés, jegyzet (BME)
[3] Varga Zoltán: Rádió iránymérés (Diplomaterv)
Budapesti Műszaki Egyetem 1999.
[4] Simonyi Károly, Zombori László:
Elméleti villamosságtan
Műszaki Könyvkiadó 2000.
[5] Istvánffy Edvin:
Tápvonalak, antennák és hullámterjedés
Műegyetemi kiadó 1997.
[6] Németh Zoltán, Imre Sándor, Balázs Ferenc:
Adaptív antennarendszerek
Híradástechnika, 2002/5. pp.21–27.

100 éve született Ocskay Szilárd

LAJTHA GYÖRGY

lajtha.gyorgy@ln.matav.hu

Ocskay Szilárd 1926-ban kezdte postai pályafutását. Mint fiatal mérnök több postai munkahelyen megfordult. Dolgozott a Vezérigazgatóság Távíró- és távbeszélő üzemi osztályán, majd amikor 1936-ban felismerték kiváló szervező és alkotó készségét, a Vezérigazgatóságon beruházói feladatokkal bízták meg.

Jelentős feladata volt a miskolci Ericsson telefonközpont telepítése. Ez a hazai hálózatban akkor sok problémát okozott, hiszen addig 7A1 központok voltak csak üzemben, melyek revertív impulzusokkal állították be a választógépeket a kapcsolat létrehozásához szükséges pozícióba. A konstrukciójában és jelzéstechnikájában eltérő Ericsson központtal az együttműködés nehéz feladat volt. Bár akkor még a helyközi hívások kizárólag kezelő segítségével voltak létrehozhatók, de az Ericsson központtal egyidejűleg felmerült a távhívás lehetősége is. Az alkotószellemű fiatal mérnök felmérve a problémákat, azt a megoldást találta a legjobbnak, hogy 12 beszédátviteli csatornából 1-et leválaszt, és azt kizárólag jelzésátvitelre használja. Elképzelése bevált és 1940-ben megvalósult Magyarországon az első közös csatornás jelzésrendszer.

Ennek jelentőségét akkor látjuk igazán, ha tudjuk, hogy ezt az 1960-as évek vége felé a hasonló elveken működő nemzetközileg szabályozott No6 és No7 jelzésrendszer valósította meg. Mérnöki szemlélete segítségével 20 évvel a világ nagyjai előtt kidolgozta ennek a perspektivikus rendszernek elveit, és elképzeléseit igazolta a gyakorlat.

Az első rurál körzet forgalomtechnikai tervezésével szintén megelőzte korát. A szentendrei rurál körzetben a különböző irányú hívások várható gyakoriságának felmérésével gazdaságos hálózatot tervezett. A forgalomelmélet gyakorlati felhasználása alkalmassá tette Ocskay Szilárdot arra, hogy gondolatait a postamérnököknek átadja. Ennek érdekében tanfolyamokat szervezett, melyeken ő maga is előadott. Tapasztalatait „Távbeszélő üzemtechnika“ és „Távbeszélő forgalmi méretezés“ könyveiben foglalta össze.

A II. világháború után politikai okokból úgy látták, hogy központi államigazgatási szervben nem alkalmazhatják, ezért áthelyezték a Posta Kísérleti Állomásra. Gyorsan beilleszkedett új munkakörébe, ahol munkatársai nagy hasznát vették innovatív szemléletének. 1951-ben kinevezték az Állomás Elektromos osztályának vezetőjévé, ahol valamennyi vezetékes távközlési feladat összefogója és irányítója volt. Hozzátartozott az erősáramú befolyásolás, és az áramellátás kérdése is.

1964-ig vezette osztályát, ahol minden kérdésben a haladás, a műszaki szemlélet és a tudományos alaposság vezérelte. Emiatt voltak összetűzései a konzervatív Vezérigazgatósággal, de jogászi alapossággal megírt jelentései mindig az ő igazát igazolták, és jelentették egyben a haladást is. A távközlő berendezések tranzisztorizálása során munkatársait tapasztalataival támogatta és az eredmények terjesztését – minden nehézség ellenére – keresztülvitte. Forgalomelméleti tudása segítségével az aktuális problémákat megoldotta és kialakított olyan hálózattervező csapatot, mely nemcsak a hazai, hanem a külföldről érkező megbízásoknak is eleget tudott tenni.

A fiatalok nevelését elsőrendű feladatának tekintette. Bár akkor nem volt népszerű a nyelvtanulás és az önálló munka, de nagy súlyt helyezett ezekre. Elérte, hogy minden munkatársa érezte a rábízott feladat fontosságát és felelősségét annak minőségéért. Sok esetben, ahogy elkészültek a tanulmányok, úgy engedte azokat tovább, de később a szerzőkkel részletesen megvitatta milyen hibákat, kétértelműségeket, vagy támadható felületeket hagytak a szövegben. Az ilyen beszélgetések tanulságai tartósan megmaradtak.

Vezetői munkája mai divatos szóval a „csapatépítésre“ is kiterjedt. Prémiumából néha elvitte vacsorázni az osztályát, majd amikor sikerült a Vezérigazgatóságtól néhány vitorlás hajót szereznie, létrehozta a Posta Kísérleti Intézet Vitorlás szakosztályát, ahol számos fiatal tanulhatott meg vitorlázni, és tölthette együtt kellemesen a hétvégéket.

Bár az idők változtak, a munka üteme felgyorsult, az együttműködési szabályok is kötöttebbek lettek, mégis érdemes innovatív személyiségét felidézni, és a módosult körülmények között is az újért, az igazért az ő stílusában küzdeni.

SECURITY TESTING OF NETWORK PROTOCOLS
Keywords: security, traffic re-routing, conformance
This article focuses on security testing of protocol implementations. A new security testing method is proposed with highlighting its scope of application. Finally a software framework is introduced with some practical examples of use.

DEVICES FOR CONFORMANCE TESTING OF TRAFFIC ANALYZERS
Keywords: reliability, application terms, optimization
Voice, video and other types of data which have been using dedicated networks are turning now more and more to Internet Protocol. This means that quality parameters of networks need to be continually monitored. Monitoring of live traffic is also important for the operation, maintenance and rapid fault clearance of networks. Network traffic analyzers offer answer to these problems.

FAULT-TOLERANT RUNNING OF PROCESSES ON COMPUTER CLUSTER
Keywords: programs requiring high capacity, MPI, co-working faults
In the article two fail-tolerant clusters are introduced which were developed for clusters of computers with one or two processors. The most important requirement toward fault-tolerant systems is to prevent the need of re-starting computing power consuming applications running for several weeks or months. These systems have to ensure the trouble-free running of the application by early fault detection or by preventing them.

ANALYSIS OF MOBILE BROADCASTING IN IPV6 NETWORKS
Keywords: bandwidth usage, remote log-on, home agent, traffic management
The use of broadcasting protocols can result in considerable saving in bandwidth in the field of digital broadcasting, videoconferencing or other multimedia applications. This is especially important in mobile environment with limited resources. The article proposes a protocol add-on using the remote log-on method which can considerably improve the performance of IPv6 based broadcasting protocols in mobile environment.

ON THE USE OF COMPLEMENTARY CODE KEYING PROCEDURES IN WIRELESS NETWORKS
Keywords: IEEE 802.11b physical layer, CCK procedure, interference protection
During the past few years the emerging need for mobility has brought about considerable changes in the development of communications technologies. The proved and well-known fixed connections turned out to be inadequate for many jobs. The penetration of mobile technologies can be observed in increasingly more areas, providing new opportunities and posing new challenges for the development and system engineering community.

MECHANISMS MOTIVATING CO-OPERATION IN MULTI-HOP WIRELESS NETWORKS
Keywords: charging, cellular network, bill based motivation, security, cryptography
This article introduces the problem of motivation for co-operation which is a typical phenomenon in multi-hop wireless networks. After a short overview of non-cooperative behaviour patterns and the types of mechanisms motivating co-operation, some basic elements and ideas of the two proposed motivating mechanisms is depicted.

MOBILE TECHNOLOGY SERVING M-COMMERCE
Keywords: content provision, standardization
The interest of leading telecommunications companies in m-commerce has led international standardization organizations, such as ETSI, to deal with the underlying technology as one of the next steps in technical development. The point of one of the often used method lies in the joint development of proposed features of the emerging product already in the process of standardization.

ECHO SUPPRESSOR OF CABLE TELEVISION (DYNAMIC INGRESS BLOCKING™)
Keywords: noise reduction, reflexion, CATV quality
The DIB™ technology has been developed and patented for the solution of backward problems of CATV networks which are characterized in the article. The proposed capability allows for an easy and rapid setup of a bi-directional network, putting cable modems into operation by customers as well as the achievement of QoS required for VoIP.

POWER LINE TELECOMMUNICATION
Keywords: Internet, broadband connection, on-line access, OFDM
Power Line Telecommunication is a new technology which uses existing low-power electric network for data transmission between devices. One the one hand, the development of the Internet has created the necessity for a broadband data connection available for everyone. On the other hand, new digital modulation techniques have created the possibility of using electric power network for this purpose.

DIRECTION MEASUREMENT WITH ADAPTIVE ANTENNA SYSTEMS
Keywords: mobile communications, electromagnetic environment pollution, cryptography, wave theory
The rapid growth of the subscriber base, the extension of services as well as the increasing competition in mobile communications can require the introduction of new methods for the more economical use of the available frequency band. The most efficient way could be the application of adaptive antenna systems which have already been widely used in space research and satellite broadcasting.

Summaries • of the papers published in this issue

Contents

Cover: How long will mobile boom last?

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

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

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

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

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

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

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

HU ISSN 0018-2028

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