híradástechnika

1945 VOLUME LXIII. 2008

hírközlés ▪ informatika

Elektronikus ügyintézés az NHH-ban

Logelemzés

Mérésinformatika

Wi-Fi hálózatok tervezése

2008/12

A Hírközlési és Informatikai Tudományos Egyesület folyóirata
a Nemzeti Hírközlési és Informatikai Tanács együttműködésével
és a Nemzeti Kulturális Alap támogatásával

nka

Tartalom

Címlapfotó: Dankó András

A Híradástechnika folyóirat megújulása elé

Kedves Olvasóink!

Az eddigiekben megpróbáltuk összehangolni azt a kettős cékitűzésünket, hogy lapszámainkban egyaránt helyet kapjanak az új kutatási eredményeket bemutató közlemények és a színvonalas szakmai ismeretterjesztést szolgáló áttekintő cikkek. A jövőben – figyelembe véve olvasóink érdeklődését és elvárásait – lényeges előrelépést szeretnénk elérni az áttekintő cikkek számát és minőségét illetően. Egyben megfontoltuk azt a tényt is, hogy amennyiben a kutatási jellegű cikkek csak magyarul látnak napvilágot, akkor óhatatlanul szűk olvasóközönség számára érdekesek csupán, miközben az angol számokban való publikálásuk egyrészt az adott témát művelő, jóval tágabb nemzetközi közösség számára teszik lehetővé a közzétételt, másrészt idézhetővé, referálhatóvá válnak ezek a munkák.

A fentiek alapján a szerkesztőbizottság – a HTE vezetőségének jóváhagyása és támogatása mellett – a jövőben szeretné megvalósítani azt, hogy a magyar számok döntő részben szélesebb közönségnek szóló áttekintő cikkekből álljanak, melyek mellett rendszeresen közölnénk könyvismertetőket, projektbeszámolókat, szakmai híreket, érdekességeket, interjúkat is.

A magyar folyam így jobban betölthetné azt a szerepét, hogy a szakma egyetlen magyar nyelvű, színvonalas ismeretterjesztő folyóirataként közvetítse az egyes részterületeket helyzetét, fejlődésének irányait és legújabb eredményeit a jelenleginél szélesebb olvasótábor számára és formálja, befolyásolja a magyar szaknyelvet.

Terveink szerint új rovatokkal fogjuk bővíteni lapszámainkat, azt tervezzük, hogy rendszeresen jelentkezünk könyvismertetésekkel, konferenciákról, fontos szakmai eseményekről szóló beszámolókkal, hazai és nemzetközi projektek ismertetéseivel, a HTE szakosztályok tevékenységét bemutató cikkekkel, valamint egyetemi és kutatóintézeti egységek bemutatkozásaival.

Publikációs fórumként, bírált kutatási cikkek megjelentetésére az angol nyelvű számok fognak szolgálni. Ezekben a számokban lehetnek az eredmények hozzáférhetők, idézhetők, hivatkozhatók az alapvetően nemzetközi kutató közösség számára. Fokozatosan szeretnénk megteremteni a lehetőségét annak, hogy az angol folyamot a későbbiekben bírált folyóiratként ismerje el a nemzetközi szakmai közösség. Ehhez első fontos lépésként az eddigi évi 2-ről 4-re növeljük az angol kiadások számát.

Bár az eddigiekben is törekedtünk a kutatási cikkek független bíráltatására, a fenti elképzelés sikeréhez a nemzetközi folyóiratokban szokásos bírálati procedúra általános és következetes alkalmazására lesz szükség. Kialakítunk egy állandó bírálói kört, lehetőleg minél több külföldi szakember bevonásával. A jelenlegi szerkesztőbizottságunk mellé létrehozunk egy International Advisory Committee-t, amelynek tagjai ösztönöznék saját környezetükben a lapunkban történő publikálást és közreműködnének a bírálati folyamat lebonyolításában.

Szerkesztőbizottságunk tagjai a jövőben is egy-egy fontos részterület „gazdái” maradnak és a továbbiakban is tervezzük célszámok, célszám-részek megjelentetését, többek között az alábbi területeken:

– vezetéknélküli és mobil kommunikáció,
– optikai hírközlés,
– digitális műsorszórás,
– infokommunikációs szolgáltatások,
– internet-technológiák és alkalmazások,
– médiainformatika,
– multimédia rendszerek,
– kábeltelevíziós rendszerek
– távközlési szoftverek,
– adat- és hálózatbiztonság,
– űrtávközlés,
– infokommunikáció a közlekedésben,
– gazdasági és szabályozási kérdések,
– az infokommunikáció társadalmi vonatkozásai.

Az új szerkesztési elveknek megfelelően a 2009-es évben a következőképpen alakul majd a magyar és angol számok megjelenése:

Január, április, július és október, tehát negyedévente: angol számok – „Infocommunications Journal” címmel. Február, április, június, augusztus, október és december, tehát kéthavonta: a „Híradástechnika” magyar számai.

Bízunk benne, hogy a tervezett változtatások megnyerik olvasóink tetszését és a korábbiaknál többen fogják haszonnal forgatni számainkat. Természetesen várjuk cikkeiket is, mind a magyar, mind az angol számokba!

Zombory László, a szerkesztőbizottság elnöke
és Szabó Csaba Attila főszerkesztő

Informatikai megoldások a telekommunikációban

vonderviszt.lajos@nhh.hu

A konvergencia nem csak a kommunikációs platformok integrálódásában és a határok elmosódásában figyelhető meg, hanem a hírközléssel foglalkozó tudományok és technológia más területein is, hiszen manapság már szinte elképzelhetetlen olyan hírközlési technológia vagy berendezés, amely ne venne igénybe vagy ne integrálna magába informatikai eszközöket, illetve szolgáltatásokat, a kutatástól, tervezéstől a megvalósításon át egészen a szolgáltatásnyújtásig. A közös elemek, amelyeket minden rendszerünkben megtalálhatunk; a szoftver és az utasításokat végrehajtó hardver.

Nyuli Attila a közigazgatásban használható elektronikus aláírási rendszer megvalósításának ismertetésével egy komplex informatikai rendszert mutat be, amelynek célja a biztonságos kommunikáció biztosítása távol levő felek között.

Bonyolult rendszerekben számtalan diszkrét jelenség definiálható úgy, mint esemény és ezeket a rendszerek többsége naplózni képes. A rendszerek számának és teljesítményének növekedésével az egy-egy szolgáltatással kapcsolatba hozható naplóbejegyzések száma messze túlnőtt már az emberi felfogóképesség határán, ugyanakkor az eseményeknek csak elenyésző része hordoz olyan információt, amelyből következtetés vonható le a múlt-, jelen- vagy jövőbeli rendellenes működésre. *Fábiányi Gábor, Frész Ferenc, Szabó László és Zsilinszky Sándor* a logelemzés sajátosságait tárgyalva mutatja be a hatalmas információmennyiség feldolgozásának korlátait és lehetőségeit.

A kommunikációs hálózatok tervezése olyan mérnöki tevékenység, amely szintén nem képzelhető el informatikai támogatás nélkül. *Réti Zoltán és Czucz Dávid* egy Wi-Fi hálózat tervezésének és megvalósításának informatikai eszközkészletét villantja fel egy konkrét probléma megoldása kapcsán.

A magyarországi hírközlési infrastruktúra folyamatos működtetése elképzelhetetlen a jogszabályok és előírások betartásának ellenőrzését támogató, országos kiterjedésű komplex mérőrendszer nélkül. *Gáspár Ernő és Zimmer András* cikkükben a Nemzeti Hírközlési Hatóság egységes mérésinformatikai rendszerének kialakítási elveit ismertetve engednek bepillantást egy országos mérőszolgálat „boszorkánykonyhájába".

Gál Zoltán cikkében az NGN – ami önmagában is a konvergencia „szinonimája" – VoIP szolgáltatások forgalmi kérdéseivel, azon belüli is az egyes kodekek által előállított önhasonló tulajdonságú adatfolyamok analízisével foglalkozik és megállapítja, hogy QoS szolgáltatás igénybevételével ezek jellemzői javíthatók.

Jelen számunkban még két további, beküldött kutatási cikknek adtunk helyet.

Aczél Kristóf és Vajk István cikke új módszert mutat be egycsatornás, polifonikus zenei felvételek külön szólamokra történő szétválasztására. A javasolt rendszerarchitektúrában a hiányzó információt valódi hangszermintákkal pótolja, így lehetővé téve egyes megismételhetetlen felvételek szeparációját és javítását.

Végül *Károlyi Gergely, Jakab László és Lénárt Ferenc* cikke az anyagok elektromos és mágneses anyagparamétereinek rádiófrekvenciás vizsgálatára kifejlesztett, új mérési módszerüket ismerteti. Ebben a vizsgált anyagok komplex permittivitását és permeabilitását egyidejűleg lehet megkapni egy hálózatanalizátor és egy vezérlő, adatfeldolgozó szoftver segítségével.

Vonderviszt Lajos
vendégszerkesztő

Szabó Csaba Attila
főszerkesztő

Az elektronikus ügyintézés alapjai a Nemzeti Hírközlési Hatóságnál

NYULI ATTILA

Nemzeti Hírközlési Hatóság
nyuli.attila@nhh.hu

Kulcsszavak: digitális aláírás, hitelesítés, XAdES, frekvenciagazdálkodás, NHH

A cikk az elektronikus ügyintézés bevezetésével foglalkozik a Nemzeti Hírközlési Hatóság frekvenciagazdálkodási eljárásában. Ismerteti a digitális aláírás alkalmazásával kapcsolatos kérdéseket, a megvalósított rendszer működésének folyamatát és a működtetésével kapcsolatos tapasztalatokat.

1. Bevezetés

A Nemzeti Hírközlési Hatóság (NHH) hatáskörébe tartozó frekvenciagazdálkodás, azon belül a rádiófrekvenciák ügyfelek számára történő kijelölése illetve használatuk engedélyezése során számos technikai adatra van szükség, melyek nagy része az ügyfeleknél keletkezik. A manuális adatrögzítés kiváltása érdekében már a kilencvenes évek elején is elektronikus adatcsere folyt a nagyobb ügyfelek és az NHH jogelődje között. Az adatok először floppy lemezeken cseréltek gazdát, majd a hírközlési hálózatok növekedtével nagyobb kapacitású adathordozók váltak szükségessé.

A bevezetett megoldás ugyan elkerülhetővé tette a manuális adatrögzítést, azonban a hivatali ügyintézés (jog)alapját továbbra is a papíralapon benyújtott kérelmek képviselték, mivel az adathordozón található információk hitelessége nem volt biztosított. A probléma természetesen a hatósági munka más területein is érzékelhető volt, így az informatikai rendszerek fejlesztésével foglalkozó munkatársak fokozott érdeklődéssel várták az elektronikus aláírással foglalkozó törvény megjelenését.

2. Az első nekifutás: XMLDSIG szabvány [1] szerinti elektronikus aláírás

A *2001. évi XXXV. törvény* megjelenése az elektronikus aláírásról jelentősen inspirálta adathitelesítéssel kapcsolatos informatikai fejlesztési szándékainkat, azonban a hitelesítésszolgáltatók magyarországi megjelenéséig még évekre volt szükség.

2003. elején úgy tűnt, hogy elindulhat a régóta várt fejlesztés. A törvényi szabályozás alapjai megvannak, és az NHH nyilvántartásai szerint Magyarországon két hitelesítésszolgáltató is tud minősített elektronikus aláíró tanúsítványokat kibocsátani a nyilvántartásban szintén feltüntetett biztonságos aláírást létrehozó eszközökre (BALE). Így az ábrándozás korszakát lezárva az új technológia beépíthető a megújítás előtt álló ügyiratkezelő rendszerbe, mely ezáltal többek között képessé válik elektronikus aláírással történő kiadmányozásra, illetve a hitelesített dokumentumok iktatására is.

A közbeszerzési eljáráson keresztül kiválasztott szállító 2004. februárjában nagy meglepetést okozott: jelezte, hogy a rendszerfejlesztés határidejét jelentős mértékben veszélyezteti, hogy nem lehetséges minősített elektronikus aláíró tanúsítványokra szert tenni. Némi hitetlenkedés után az NHH egy találkozót szervezett a fejlesztő, a hitelesítésszolgáltatók és az intelligens kártya szállítóinak bevonásával.

Kiderült, hogy a hír bármennyire meghökkentő, de igaz. Magyarországon két kártya kapta meg a BALE minősítést, azonban a minősítéskor előírt feltételeket a kártyák 2004 februárjában még nem teljesítették. A hitelesítésszolgáltatók ezt követően nagy erőkkel dolgoztak a szükséges fejlesztéseken annak érdekében, hogy a fejlesztett aláíró alkalmazás számára szükséges interfészek létrejöjjenek, illetve a kártyákon futó mikrokódok a minősített működés szerinti paraméterezésűek legyenek.

Az e-aláírással hitelesített dokumentumok hatósági ügyintézés során történő kezelésére 2003-ban illetve 2004 elején még nem volt egységes szabályozás, az egyes folyamatlépésekhez tartozó intézkedések kidolgozása (például hogyan működjön egy elektronikus tértivevény) az ügyiratkezelő rendszer fejlesztésének keretein túlmutató erőfeszítéseket igényelt. Ennek volt köszönhető, hogy 2004 nyarára az elektronikus aláírási képesség megszerzésével kapcsolatos elvárások szerényebbé váltak, az ügykezelési folyamatba épülés helyett egy NHH-n belül használható elektronikus aláírást létrehozó program, illetve egy, az ügyfelek számára korlátozásmentesen átadható aláírásellenőrző alkalmazás kifejlesztése lett a cél.

Az egyszerű felhasználói felülettel rendelkező, Microsoft Windows platformon futtatható alkalmazások 2005-ben elkészültek *(1. ábra)*, miközben az NHH kiadmányozó munkakörben dolgozó munkatársai minősített elektronikus aláíró tanúsítványokat kaptak.

Éppen az alkalmazás használatára vonatkozó oktatást szerveztük, mikor számunkra teljesen váratlanul számos új jogszabály jelent meg, új alapokra helyezve az

elektronikus ügyintézést, és jó időre ellehetetlenítve az elektronikus aláírás közigazgatásbeli használatát. Az elkészült rendszert nem lehetett használatba venni.

3. Az új szabályozási környezet

A 2005 végén megjelent jogszabályok új, nagyon részletesen definiált alapokra helyezték az elektronikus ügyintézést. A legfontosabbak:

- *193/2005. (IX. 22.) Korm. rendelet* az elektronikus ügyintézés részletes szabályairól;
- *194/2005. (IX. 22.) Korm. rendelet* a közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítésszolgáltatókra vonatkozó követelményekről;
- *195/2005. (IX. 22.) Korm. rendelet* az elektronikus ügyintézést lehetővé tevő informatikai rendszerek biztonságáról, együttműködési képességéről és egységes használatáról;
- IHM ajánlások a közigazgatásban alkalmazható
  - tanúsítványokról,
  - időbélyegzésről,
  - aláírási szabályzatokról,
  - elektronikus aláírási formátumokról,
  - viszontazonosításról.

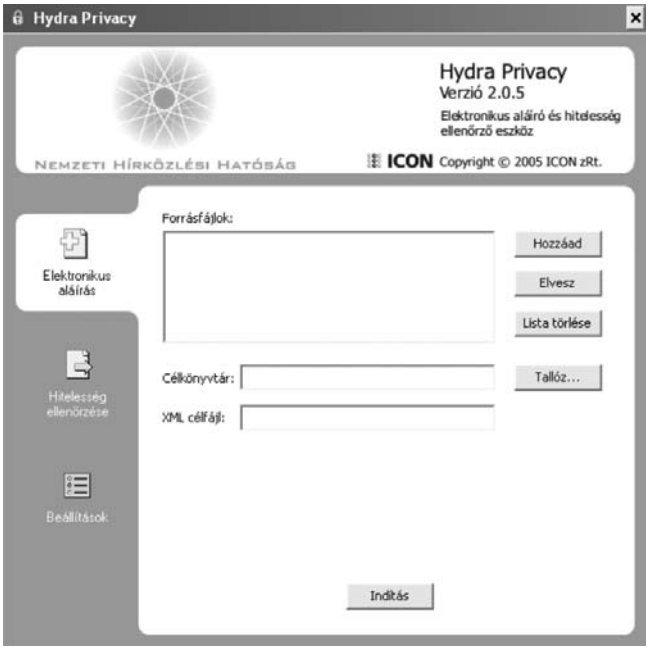
A jogszabályok által indukált főbb változások:

1. Az előírt aláírási formátum az XML Advanced Signature (XAdES) szabvány [2] módosított változata lett.
2. Ékezetes nevek is használhatóak a tanúsítványokban.
3. Csak a Közigazgatási Gyökér Hitelesítés Szolgáltató (KGYHSZ) által felülhitelesített tanúsítvány kiadók tanúsítványai alkalmazhatóak közigazgatási eljárásokban.
4. A KGYHSZ felülhitelesítéshez a hitelesítés szolgáltatóknak viszontazonosítási szolgáltatást kell nyújtaniuk a közigazgatás intézményei felé.

4. (Újra)tervezési szempontok

2006. első félévét a vonatkozó jogszabályok tanulmányozásával, értelmezésével, illetve az új informatikai rendszer tervezésével töltöttük. Megfogalmaztuk a célrendszer legfontosabb tulajdonságait:

1. Tegye lehetővé az elektronikus ügyintézést.
2. Teljeskörű megfelelés a jogszabályi elvárásoknak.
3. Infrastruktúraszerűen működjön, az NHH hatósági szakrendszereit lehető legkisebb mértékben kelljen módosítani az elektronikus ügyintézés bevezethetőségéhez.
4. Moduláris felépítésű rendszer legyen.
5. Nyílt interfészeken keresztül nyújtsa szolgáltatásait a többi (más szállító által fejlesztett) informatikai rendszer számára.



1. ábra
Aláírást létrehozó és hitelességet ellenőrző alkalmazás

6. Tanúsított elektronikus aláírást létrehozó motort használjon, miáltal szükségtelenné válik a rendszer tanúsíttatása.

7. Terjedjen ki az Ügyfélkapun keresztüli felhasználóazonosításra is.

8. A megvalósított rendszer tegye lehetővé a teljes elektronikus ügymenetet amennyiben a kapcsolódó rendszerek erre alkalmassá váltak, azonban addig is rendelkezzen olyan (átmenetileg használt) interfészekkel, melyeken keresztül humán beavatkozással a folyamat felépíthető. Ezen interfészek használhatóak a rendszer átvételi teszteléséhez is.

9. Legyen egy hordozható számítógépeken is alkalmazható (tehát az NHH informatikai hálózatától függetlenül is működőképes) elektronikus aláírást létrehozó illetve hitelesítést ellenőrző komponense is. Ez a modul rendelkezzen függvény- és adatkapcsolati interfésszel annak érdekében, hogy más alkalmazások (tipikusan az ügyiratkezelő rendszer) a modul által nyújtott hitelesítési funkciókat igénybe tudják venni.

5. Aláírásformátumok

Mielőtt az elkészült rendszer működési koncepcióját ismertetnénk, célszerű kitérni a közigazgatásban használható elektronikus aláírásformátumok ismertetésére. Az IHM *elektronikus aláírás formátumok műszaki specifikációja* címet viselő ajánlása négy közigazgatási formátumot különböztet meg:

- A **„pillanatnyi”** közigazgatási formátum egy olyan pillanatnyi aláírás, mely sem visszavonási információkat, sem időbélyegzést nem tartalmaz. Olyan esetekben alkalmazható, amikor az aláírt dokumentum sértetlenségének ellenőrizhetősége önmagában is elegendő. Ez a formátum a szabványos XAdES-EPES formátumnak

felel meg. Élettartama rövidebb az aláírást követő első visszavonási állapot információ kiadásánál.

• A **„rövid távú”** közigazgatási formátum egy olyan rövid távú aláírás, melyhez időbélyeg kapcsolódik, de nem tartalmaz visszavonási információkat. Olyan esetekben alkalmazható, amikor az aláírt dokumentum sértetlenségének ellenőrizhetőségén túl szükség van a dokumentum adott időpont előtti létezésének az igazolására is (de alkalmazható pillanatnyi aláírásként is). Ez a formátum megfeleltethető a szabványos XAdES-T formátumnak. Az aláírás ellenőrzése nem szükséges az aláíró tanúsítványának lejárta után.

• A **„hosszú távú”** közigazgatási formátum egy speciális hosszú távú aláírás (mely értelemszerűen alkalmazható pillanatnyi és rövid távú aláírásként is). Ez a formátum megfeleltethető a szabványos XAdES-C formátumnak. Jellemzője, hogy az elektronikus aláírás ellenőrizhetősége szükséges a tanúsítványlánc bármely elemének a lejárta után is.

• Az **„archív”** közigazgatási formátum egy speciális archív aláírás, egyúttal megfelel a szabványos XAdES-A formátumnak. Jellemzője, hogy ellenőrzése szükséges az aláírás során használt algoritmusok kriptográfiai elavulása után is.

A „hosszú távú” és „archív” közigazgatási formátum visszavonási információkat és időbélyeget egyaránt tartalmaz, így olyan esetekben is alkalmazható, amikor az első két aláírási formátummal ellentétben az aláírások utólagos letagadhatatlanságára (az aláíró kilétének harmadik fél előtti bizonyíthatóságára) is szükség van.

Az NHH elektronikus ügykezelést lehetővé tévő rendszerének működése során rövid távú és archív elektronikus aláírások keletkeznek.

6. Működési logika

A rendszer elektronikus aláírásra vonatkozó működési folyamatait a *2. ábra* szemlélteti.

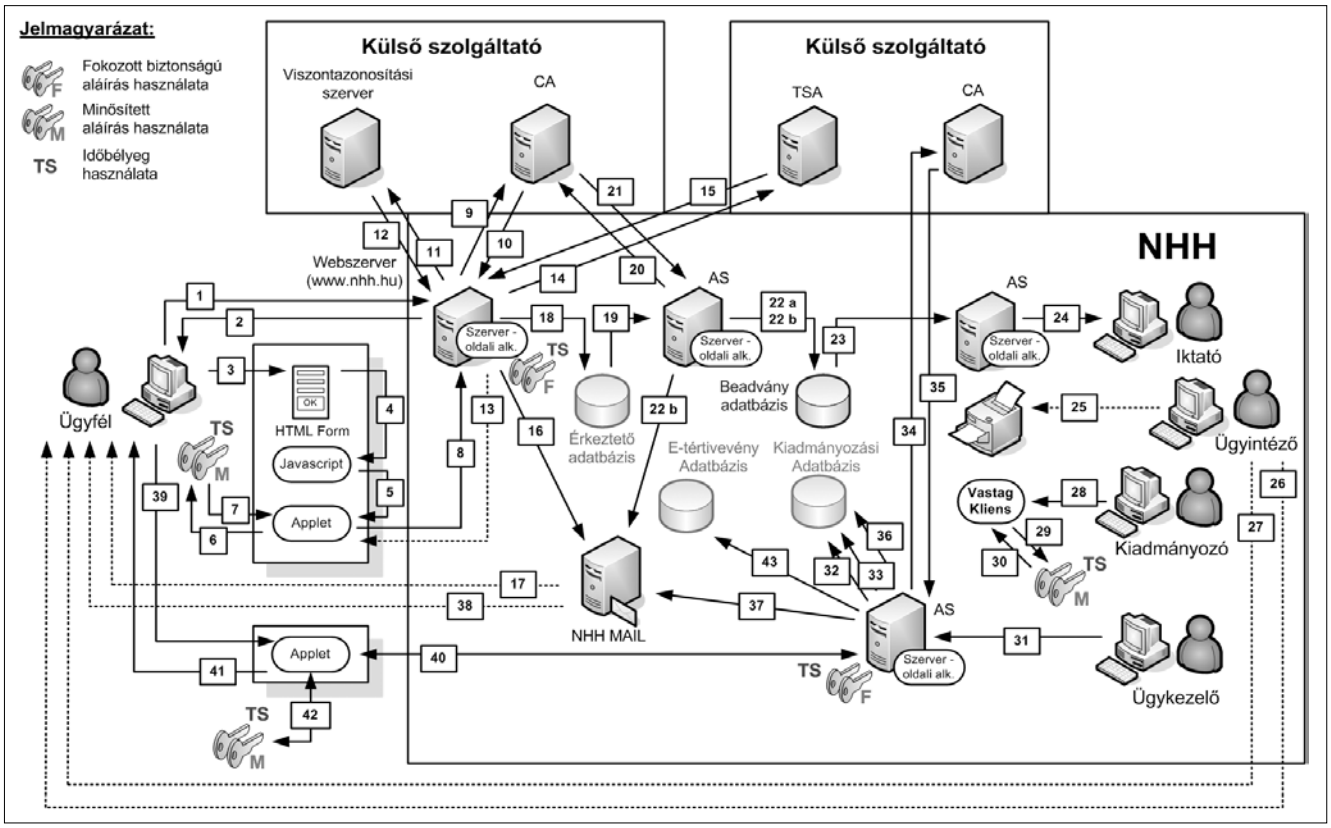
A működési folyamat a következő lépésekből épül fel:

1. Az elektronikus hatósági ügyintézést kezdeményező ügyfél az elérni kívánt szolgáltatást biztosító weblaphoz kapcsolódik. A személyes adatok és a bizalmasság megőrzése érdekében az NHH és az ügyfél közötti kapcsolat SSL protokoll felhasználásával titkosított.

2. A weblap tartalma – amely bármilyen tetszőleges kialakítású (UTF-8 kódolású) űrlap lehet –, letöltődik az ügyfél böngészőjébe. Az űrlapok a benyújtandó tényleges adatokon kívül tartalmazzák a viszontazonosításhoz és a rendeletekben megfogalmazott nyilatkozási lehetőségekhez szükséges mezőket is.

3. Az ügyfél az űrlap kitöltését és az űrlapon jelzett, elektronikus formában rendelkezésre álló és mellékelendő fájlok becsatolását követően, az űrlap tartalmának jóváhagyásaként, a weblapon található *Továbbítás elektronikus aláírással* gomb vagy a *Továbbítás ügyfélkapu azonosítóval* gomb segítségével kezdeményezi az űrlap és a kapcsolódó adatok feldolgozását. A becsatolásra kerülő fájlok tartalmát a feldolgozó alkalmazás nem vizsgálja/értelmezi (ezek akár aláírt XML állományok is lehetnek). A rendszer számára az első aláírást a bead-

2. ábra A rendszer elektronikus aláírásra vonatkozó működési folyamatai



ványt benyújtó ügyfél aláírása jelenti. Az ilymódon keletkezett állományt fogja a fogadó rendszer hitelesíteni. Amennyiben egy ügyfél egy másik személy által aláírt XML állományt kíván hiteles módon becsatolni, úgy azt kötelezően XAdES-A formátumban kell megtennie. A csatolható fájlok méretét a hosszú feldolgozási idők elkerülése érdekében a rendszer korlátozza. Az egy-egy űrlapra becsatolt állományok összmérete nem haladhatja meg a 100 MB-ot. A csatolt fájlok típusára, formátumára nincs külön megkötés, azonban a rendszer paraméterezésén keresztül űrlaponként szabályozhatóak az elfogadott MIME típusok.

4. A feldolgozás első lépéseként egy kliens-oldali Javascript program kigyűjti az űrlapot alkotó weblapból az egyes adatbeviteli mezőket és azok tartalmát. A Javascript program lehetőséget biztosít az űrlap adatbeviteli mezőinek tartalmi validálására is (tartományba esés, dátum, IP cím, e-mail cím stb.) Amennyiben vannak csatolmányok, azok alapján egy csatolmánylista készül, majd az adatokból egy XML alapú adattömböt képez.

5. A Javascript letölt egy elektronikus aláírással hitelesített Applet-et, amelynek átadja az űrlap adataiból képzett XML adattömböt.

6. Az alkalmazás az XML adatstruktúrát ismételten olvashatóvá alakítja és a csatolt fájlok listájával együtt (amennyiben ilyenek léteznek) megjeleníti az ügyfél számára az aláírás előtt. A letöltésre került Applet létrehozza a közigazgatásban elvárt XAdES alapú XML aláírási formátumot és kezdeményezi a bevitelre került adatok és a csatolt állományok ügyfél általi aláírását.

7. Az ügyfél az aláíró eszközének és az aláírásra használt kulcspárjának (tanúsítványának) kiválasztását követően fokozott biztonságú, vagy minősített elektronikus aláírással látja el a bevitelre került adatokat. (Mind a viszontazonosításra használt, mind az ügyintézési tevékenységhez szükséges adatmezők és csatolt állományok aláírásra kerülnek.)

8. Az Applet az ügyfél elektronikus aláírásával ellátott, XAdES-EPES formátumú adatokat továbbítja az NHH Webszervere felé.

9. Az NHH Webszerverén futó szerver oldali komponens az Applet által beküldött XAdES állomány részeként csatolt ügyfél tanúsítványt megvizsgálja. Amennyiben a tanúsítvány már/még érvényes, úgy a tanúsítványt kibocsátó szolgáltató (CA) rendszeréből megpróbálja letölteni a vonatkozó tanúsítvány visszavonási listát (CRL), illetve adott esetben megpróbálja lekérdezni a tanúsítvány érvényességét a szolgáltató által biztosított OCSP szolgáltatás igénybevételével.

10. A vonatkozó tanúsítvány visszavonási lista (CRL) sikeres letöltését, illetve az OCSP válasz visszaérkezését követően a szerver oldali komponens megvizsgálja, hogy az ügyfél tanúsítvány szerepel-e a CRL listán (visszavonásra került-e).

11. Amennyiben a csatolt tanúsítvány érvényes és nem került visszavonásra, úgy az ügyfél által kitöltött adatok alapján a rendszer megkísérli az ügyfél viszontazonosítását a tanúsítványt kibocsátó szolgáltató viszontazonosítási szolgáltatásának igénybevételével.

12. A viszontazonosítási válasz visszaérkezését követően a rendszer értékeli az ügyfél személyazonossága és a tanúsítvány megfelelőségét.

13. Amennyiben az ügyfél tanúsítványa még/már nem érvényes, visszavonásra került, vagy a viszontazonosítási kérelemre érkezett válasz nemleges, úgy a rendszer visszajelez az ügyfélnek, hogy ügyintézési kérelme nem került elfogadásra és mellékeli a visszautasítás okának leírását.

14. Amennyiben az ügyfél tanúsítványa érvényes, és a viszontazonosítás eredménye pozitív, valamint az ügyfél által beküldött, aláírt adatállomány hitelessége megfelelő, úgy a rendszer generál egy 26 számjegyű érkeztető számot az 193/2005. (IX. 22.) Korm. rendelet mellékletében leírtaknak megfelelően. A beküldésre került adatok érkeztetési idejének rögzítésére a rendszer időbélyeget kér az NHH-val szerződött külső szolgáltatótól (TSA).

15. Az időbélyeg sikeres fogadását követően a rendszer a fogadó szerver kulcsával aláírja a beérkezett, érkeztető számmal és időbélyeggel ellátott adatokat.

16. Az ügyfél ügyintézési kérelemének sikeres fogadásáról e-mailben kap visszajelzést a beadvány űrlapján megadott kapcsolattartási e-mail címre. A visszajelzés az ügyfél által benyújtott kérelmet, valamint a beadvány benyújtásakor csatolt dokumentumok listáját, a fogadó rendszer által generált érkeztető számot és a fogadás időpontját rögzítő időbélyeget tartalmazza a feldolgozó szerver által aláírt XML formátumban (csatolmányként) és olvasható formában a levél törzseként. Így az e-mail külön alkalmazás nélkül is olvasható.

17. Az előkészített e-mailt az NHH levelező szervere továbbítja az ügyfélnek.

18. A beérkezett, érkeztető számmal és időbélyeggel ellátott adatok az érkeztető adatbázisban kerülnek tárolásra, a későbbi feldolgozásra várva. (Az archív aláírási formátum előállításához szükséges a kivárási idő biztosítása.)

19. Az alkalmazásszerveren futó szerver oldali komponens adott időközönként megvizsgálja az érkeztető adatbázisban lévő beadványokat, hogy a beadványokon szereplő időbélyegen található időponttól számított kivárási idő eltelt-e már.

20. Amennyiben az adott beadványra vonatkozó kivárási idő már eltelt, úgy a rendszer a tanúsítványt kibocsátó szolgáltató rendszeréből megpróbálja letölteni a vonatkozó tanúsítvány-visszavonási listát (CRL), illetve adott esetben megpróbálja lekérdezni a tanúsítvány érvényességét a szolgáltató által biztosított OCSP szolgáltatás igénybevételével.

21. A vonatkozó tanúsítvány-visszavonási lista (CRL) sikeres letöltését, illetve az OCSP válasz visszaérkezését követően a szerver oldali komponens megvizsgálja, hogy az ügyfél tanúsítványa szerepel-e a CRL listán (visszavonásra került-e).

22. a) Amennyiben a kivárási idő letelt és a beadványt aláíró ügyfél tanúsítványa továbbra is érvényes, úgy a rendszer összeállítja a beadvány archiválásához szükséges információkat és létrehoz egy XAdES-A for-

mátumú állományt, amely a beadvány adatbázisba kerül eltárolásra és az érkeztető adatbázisból törlésre kerül. Az NHH egy központi e-mail címére elküldésre kerül egy e-mail, amely az iktatók felé jelzi az elkészült beadvány rendelkezésre állását és tartalmazza a beadvány letöltési link-jét. (Ez utóbbi lépés csak a teszteléshez illetve az ügyiratkezelő rendszerhez történő integrációig volt használatban).

b.) Amennyiben a kivárási idő letelt és a kérelmet aláíró ügyfél tanúsítványa nem érvényes, úgy a rendszer az ügyfél által benyújtott és aláírt XAdES formátumú beadványt érvénytelen jelöléssel látja el és automatikusan értesítő e-mailt küld az ügyfélnek (az e-mail a beadvány űrlapján megadott kapcsolattartási e-mail címre és az NHH egy központi e-mail címére is elküldésre kerül), melyben tájékoztatja, hogy beadványa nem került feldolgozásra. Az értesítő levél olvasható formában a levél törzseként a beadvány érkeztető számát és a beadvány érvénytelen aláírás miatti elutasításának tényét tartalmazza. Az érvénytelen jelöléssel ellátott beadvány is a beadvány adatbázisban kerül eltárolásra és az érkeztető adatbázisból törlésre kerül.

23. Az (ügyiratkezelő rendszerrel megvalósított integrációig) az iktatók az alkalmazásszerveren futó webes felület és egy szerver oldali komponens segítségével kaphattak lehetőséget a beérkezett beadványok megtekintésére, illetve azoknak az NHH jelenlegi elektronikus ügyviteli rendszerébe áthelyezésére. Ezen a felületen az iktatók/ügyintézők azon beadványokat is látják külön jelöléssel ellátva, amelyek aláírása a kivárási időt követően érvénytelennek bizonyult (a tárolás és megjelenítés célja, hogy esetleges reklamációk esetén előkereshető és ellenőrizhető legyen a beadvány állapota).

24. Az ügyiratkezelő rendszerrel megvalósított integrációig az iktatók egy adott kérvénnyel kapcsolatos ügyintézési tevékenységük megkezdésekor a beadványhoz egy új iktatási számot rendeltek, és az XAdES-A formátumú aláírt beadványt munkaállomásukra letöltve csatolták az NHH elektronikus ügyiratkezelő rendszerébe.

25. Az ügyintéző az ügyiratkezelő rendszerből az XAdES formátumú aláírt beadványt a munkaállomására telepített vastag kliens alkalmazás segítségével meg tudja nyitni. Így a beérkezett és feldolgozásra került kérelmet illetve a hozzá csatolt dokumentumokat bármikor meg tudja tekinteni. (Erre a lépésre csak a szakrendszerrel és a SZÜR integrációjáig van szükség).

26. Az ügyfél az ügyintézési folyamat megkezdéséről, vagyis az ügyével kapcsolatos ügyiratszámról és az ügyét kezelő ügyintézőről, e-mailben tájékoztatást kap az ügyirattal kapcsolatos dokumentumokba való betekinthetőség biztosítása érdekében. A tájékoztató e-mailben az ügyiratszám és az ügyét kezelő ügyintéző neve csatolmányként, a kiadmányozó által aláírt XAdES formátumban és az e-mail törzseként, szöveges formában kerül elküldésre.

27. Amennyiben az ügyfél által benyújtott beadvány (akár elektronikus módon, akár papíron lett indítva) nem tartalmaz minden, az ügyintézéshez feltétlenül szükséges információt, úgy a kiadmányozó egy hiánypótlási eljárást kezdeményez az ügyfél felé. A hiánypótlási eljáráson belül az ügyfél e-mailben tájékoztatást kap a hiánypótlásra vonatkozóan, és kap egy speciálisan kialakított URL-t (a link a hiánypótlási eljáráshoz kapcsolódó ügy iktatási számát/azonosítóját tartalmazza hivatkozási információként), amelyre kattintva egy webes űrlaphoz kapcsolódik. Itt a szükséges információk/adatok/dokumentumok megadhatóak, illetve pótolhatóak. A linkben megadott hivatkozási adatok az űrlapon automatikusan kitöltésre kerülnek, ezáltal elkerülve az azonosítók téves megadásából származó problémákat. A kiadmányozó a tájékoztató szöveget és a linket az e-mail törzseként, szöveges formában, illetve a vastag kliens alkalmazás segítségével elektronikusan aláírva (minősített aláírással), az e-mailhez csatolva is elküldi. A hiánypótlásra való felszólítás átvételének igazolása az ügyfél felelőssége. A hiánypótlási űrlap kezelése és feldolgozása a 2.1. ponttól leírtak szerint történik.

28. Amennyiben a beérkezett kérvénnyel kapcsolatosan dokumentum keletkezik, úgy annak hitelesítését a kiadmányozó a vastag kliens alkalmazás segítségével teheti meg.

29. Az elektronikus aláírás létrehozásához a kiadmányozónak ki kell jelölnie az aláíráshoz használt eszközt, illetve az aláírásra használt eszközön található, aláírásra használt kulcspárt (tanúsítványt).

30. A kiadmányozó a kiválasztott tanúsítvánnyal a vastagkliens-alkalmazás segítségével aláírja, és egyúttal időbélyeggel is ellátja a kiadásra kerülő dokumentumot.

31. Az aláírt dokumentum (a SZÜR integrációig) egy webes felületen keresztül feltöltésre kerül az alkalmazásszerverre az ügykezelő által.

32. A dokumentum feltöltésre került a Kiadmányozási adatbázisba.

33. Az alkalmazásszerveren futó szerver oldali komponens adott időközönként megvizsgálja a Kiadmányozási adatbázisban lévő állományokat, hogy a dokumentumon szereplő időbélyegen található időponttól számított kivárási idő eltelt-e már.

34. Amennyiben az adott dokumentumra vonatkozóan a kivárási idő eltelt, úgy a rendszer a tanúsítványt kibocsátó szolgáltató rendszeréből megpróbálja letölteni a vonatkozó tanúsítvány visszavonási listát (CRL).

35. A vonatkozó tanúsítvány visszavonási lista (CRL) sikeres letöltését követően a szerver oldali komponens megvizsgálja, hogy a tanúsítvány szerepel-e a CRL listán (visszavonásra került-e).

36. Amennyiben a kivárási idő letelt és a dokumentumot aláíró kiadmányozói tanúsítvány továbbra is érvényes, úgy a rendszer létrehoz egy XAdES-A formátumú állományt, amelyet a Kiadmányozási adatbázis másik táblájában tárol el. Amennyiben a kivárási idő letelt és a dokumentumot aláíró kiadmányozói tanúsítvány nem érvényes, úgy erről a rendszer e-mailben tájékoztatja a kiadmányozót. Ezek az érvénytelen aláírással rendelkező dokumentumok is eltárolásra kerülnek a Kiadmányozási adatbázisban. A rendszer egyúttal visszaküldi a dokumentumot a kiadmányozó vezetőnek, meg-

jelölve, hogy lejárt tanúsítvány miatt ismételt – most már az új és érvényes tanúsítvánnyal történő – kiadmányozás, aláírás szükséges. Az eljárás ebben az esetben a 28. ponttól ismétlődik.

37. A rendszer automatikusan megvizsgálja a dokumentumhoz (az NHH meglévő ügyintéző rendszere által) csatolásra kerülő címzettek listáját és mindegyik címzett számára automatikusan generál egy egyedi azonosítót (az azonosító a dokumentumhoz kapcsolódó azonosítószámból és a dokumentum sha-256 lenyomatából tevődik össze) linkként kialakítva, amelyen keresztül az adott ügyfél a számára kiadott dokumentumot átveheti.

38. A létrehozott egyedi linkek e-mail formájában kiküldésre kerülnek az ügyfelek számára. Az e-mailben a link csatolmányként, a szerver által aláírt XAdES formátumban és az e-mail törzseként, szöveges formában kerül elküldésre.

39. Az ügyféloldalon a link-re kattintva egy Applet-et töltődik le, amely felkéri az ügyfelet, hogy egy 'dokumentum letöltési kérés' aláírásával azonosítsa magát és kezdeményezze a számára kiadott dokumentum letöltését.

40. Az Applet a link-ben megadott paraméterek és az aláírt 'dokumentum letöltési kérés' alapján az alkalmazásszerveren található szerver oldali komponens segítségével megállapítja, hogy a letöltést kérelmező ügyfél a dokumentum letöltésére jogosult-e. Amennyiben a kérelmező jogosult a dokumentum letöltésére, úgy a szerver oldali komponens a Kiadmányozási adatbázis megfelelő táblájából kiolvassa az ügyfél számára kiadott dokumentumot és átadja a kapcsolódó Applet-nek. Amennyiben a kérelmező nem jogosult a dokumentum letöltésére, úgy letöltési kérését a rendszer elutasítja, amely visszajelzésre kerül a kérelmező felé az Applet segítségével.

41. Amennyiben a kérelmező jogosult a dokumentum letöltésére, úgy a dokumentum letöltése az ügyfél munkaállomásán futó Applet segítségével történik, mely integritás ellenőrzést is végez a letöltés sikerességének ellenőrzésére.

42. A dokumentum letöltésének utolsó lépéseként a letöltött állomány sikeres ellenőrzését követően, az ügyfélnek egy időbélyeggel és elektronikus aláírásával ellen kell jegyeznie a dokumentum 'kézhezvételét' (az időbélyeg kérés és az aláírás az Applet és a szerver oldali komponens segítségével történik).

Amennyiben az állomány letöltése, illetve ellenőrzése során valamilyen probléma merül fel, úgy a letöltött állomány a helyi fájlrendszerből törlésre kerül és a rendszer tájékoztatja a felhasználót a hiba okáról.

43. A kézhezvételt igazoló *„e-tértivevényt"* a rendszer e-mailben továbbítja az előre meghatározott, NHH-n belüli e-mail címekre, illetve egy adatbázisban (e-tértivevény adatbázis) helyezi el.

Amennyiben az ügyfél a kormányzati ügyfélkapus azonosításon keresztül használja a rendszert, úgy az ügyfél oldali aláírási funkciókat az ügyfélkapus felhasználó azonosítás helyettesíti, miközben a szerver oldali aláírási/időbélyegzési funkciók változatlanul működnek.

7. Hitelesítéskezelő alkalmazás

A kialakított rendszer kicsi, de fontos eleme a folyamat diagramon vastag kliensnek nevezett hitelesítéskezelő alkalmazás. A program az NHH hálózatától függetlenül is működőképes, használatához csupán internetkapcsolatra van szükség.

Az egyszerű felhasználói felületen keresztül három fő funkció indítható *(3. ábra)*.

3. ábra
A hitelesítéskezelő alkalmazás felhasználói felülete (1)

– Az *Elektronikus aláírás* menüpont segítségével pillanatnyi, illetve az időbélyeg-kérést is bekapcsolva rövidtávú elektronikus aláírás hozható létre.
– A *Kiegészítés* menüpont szolgál a rövidtávú aláírással ellátott tartalmak archív közigazgatási formátumra történő kiegészítésére.

4. ábra
A hitelesítéskezelő alkalmazás felhasználói felülete (2)

– A *Hitelesség ellenőrzése* menüpontot kiválasztva lehetséges az aláírt tartalmak ellenőrzése, illetve az eredeti tartalom visszaállítása. A felhasználói felület gondos tervezéssel úgy lett kialakítva, hogy a lehető legegyértelműbb módon mutassa az aláírás érvényességét vagy érvénytelenségét *(4. ábra)*. Érvénytelen aláírás jelzésére a ✖, hiányos (nem kiegészített) aláírás jelzésére a ! ikonok szolgálnak. Természetesen ennél részletesebb információk is megjeleníthetőek az eredményre kattintva *(5. ábra)*.

5. ábra
A hitelesítéskezelő alkalmazás felhasználói felülete (3)

Az intuitív felhasználói felületen kívül egy XML paraméter fájlon keresztül is vezérelhető az alkalmazás. Ez a tulajdonsága teszi lehetővé, hogy más – elektronikus aláíró illetve ellenőrző képességgel nem rendelkező – alkalmazások is kezdeményezzenek hitelesítéskezelést.

8. Integrációs pontok

A hitelesítési infrastruktúra közvetlenül négy rendszerrel áll kapcsolatban:

• A rendszer működéséhez szükséges az *Ügyfélkapu-kapcsolat*.

• Az NHH felé adatszolgáltatási kötelezettséggel rendelkező hírközlési szolgáltatók előzetes regisztráció után, az *Adatkapu-rendszeren* keresztül teljesíthetik adatbeadásaikat. Az adatok beadása struktúrált formában, űrlapok kitöltésén keresztül történik, a hitelesítési infrastruktúra szolgáltatásainak igénybevételével.

• A Nemzeti Hírközlési Hatóság ügyfelei számára az *e-nhh* nevű alkalmazás webes űrlapjai teremtik meg az elektronikus ügyintézés alapjait. E rendszer a cikk írásakor még átvételi tesztelés alatt áll.

• A negyedik kapcsolódó rendszer az NHH *ügyiratkezelő rendszere*. Mivel minden egyes webes űrlap egy adott szervezeti egység tevékenységéhez köthető, az ügyiratkezelő rendszer a űrlapazonosító alapján gondoskodik az információ szervezeti egységre szignálásáról. A hiteles űrlaptartalmak feldolgozását a szervezeti egység informatikai szakrendszere végezheti.

9. Működtetési tapasztalatok

A rendszer látszólagos bonyolultsága mellett is jól üzemeltethető. Ez egyrészt moduláris felépítésének, másrészt a robusztus futtató környezetnek (UNIX) köszönhető.

A rendszer gyors működéséhez elengedhetetlen, hogy az aláíró tanúsítványok érvényessége online tanúsítvány állapot szolgáltatás (OCSP) segítségével lekérdezhető legyen. Az aláíró tanúsítvány érvényességének tanúsítvány visszavonási lista (CRL) alapján megvalósított ellenőrzése esetén egy kérelem beadása és annak ügyiratkezelő rendszerbe történő megérkezése között akár 24 óra is eltelhet!

Az NHH hitelesítési infrastruktúrájával kapcsolatba kerülő felhasználók döntő többsége jelenleg még nem rendelkezik elektronikus aláíró tanúsítvánnyal, az adatbeadás többnyire az Ügyfélkapun keresztüli felhasználóazonosítás nyomán történik. Reményeink szerint a vállalati körökben biztató ütemben terjedő elektronikus aláírási technológia (2007-ben a hazai hitelesítés szolgáltatók által kibocsátott minősített tanúsítványok száma megnégyszereződött, a fokozott biztonságú tanúsítványok száma 24%-os növekedést mutatott [3]) néhány éven belül meg fogja találni az állampolgárokhoz vezető utat is, megteremtve a biztonságos és kényelmes otthoni ügyintézés lehetőségét.

A szerzőről

NYULI ATTILA 1965-ben született Székesfehérváron. A Budapesti Műszaki Egyetem Villamosmérnöki Karának Híradástechnika Szakán kitüntetéssel diplomázott 1990-ben. 1992-ben kitüntetéses szakmérnöki diplomát, 1993-ban pedig informatikai egyetemi doktori címet szerzett a BME-n. 1992-ben a Frekvenciagazdálkodási Intézetben kezdett dolgozni, ahol fő érdeklődési körét az elektromágneses hullámterjedés számítási modellek pontosságának vizsgálata és a földrajzi információs rendszerek alkalmazásának kérdései jelentették. Érdeklődési és feladatköre később az informatikai biztonságtechnikai területtel is kibővült. Jelenleg a Nemzeti Hírközlési Hatóság alkalmazásfejlesztési tevékenységeit irányítja.

Irodalom

[1] RFC 3275 XML-Signature Syntax and Processing, http://www.w3.org/TR/xmldsig-core/
[2] XML Advanced Electronic Signatures (XAdES) http://www.w3.org/TR/XAdES/
[3] Az elektronikus aláíráshoz és alkalmazásaihoz kapcsolódó monitoring felmérések, http://www.nhh.hu/dokumentum.php?cid=16013

Logelemzés
– avagy megfejthető-e emberi közreműködés nélkül az informatikai logokba kódolt intelligencia?

FABIÁNYI GÁBOR, FRÉSZ FERENC, SZABÓ LÁSZLÓ, ZSILINSZKY SÁNDOR

KÜRT Zrt.
{gabor.fabianyi, ferenc.fresz, laszlo.szabo, sandor.zsilinszky}@kurt.hu

Kulcsszavak: informatika, korrelációs logelemzés, monitoring, forensics

Mottó: „A bölcsesség egyik titka, hogy tisztában lenni azzal, mit kell figyelmen kívül hagyni."

Az adatok gyűjtése és elemzése egyidős az emberi civilizációval. Napjainkra a számítógép forradalmasította ezt a tevékenységet, de ugyanakkor önmaga is komoly problémák forrásává vált. Ezek jelentős részének megoldásához szükséges az informatikai rendszerekben lezajló folyamatokat, eseményeket rögzítő naplóbejegyzések, logok mélyreható elemzése. A logelemzés a vállalatok menedzsmentje számára nagy jelentőséggel bíró, egyéb információkat is képes szolgáltatni, segítségével jövőbeli trendekre is lehet következtetni. Az IT rendszerek azonban óriási mennyiségű logot termelnek, melyek adekvát feldolgozása a normál üzemeltetés keretei között lehetetlen. Megjelentek tehát a piacon a különböző megoldások, melyek közül a legnagyobb hozzáadott értéket a humán intelligenciával támogatott logelemző szolgáltatás adja.

1. Bevezetés

Divatos kifejezés manapság a logelemzés. Az utóbbi években a szakmai körökön túl szélesebb rétegek is megismerkedhettek a fogalommal a különböző, informatikához kötődő közéleti botrányok nyomán. Tény azonban, hogy sok félreértelmezés és tévhit kapcsolódik e témához, így hát érdemes alaposabban körüljárni, mit érdemes tudni róla, mire használható pontosan és milyen előnyöket kínál.

A logelemzésről elmondható, hogy az informatika jelenének és jövőjének egyik legnagyobb jelentőségű eszközrendszere.

A különböző adatok gyűjtése és értékelése már akkor is kritikus része volt az élet számos területének, amikor az elemzést még nem támogatta modern technológia. A historikus adatok értékelése visszatekint egészen az ókori időkre, a sumérok korára, akik például összegyűjtötték a termésmennyiség-adatokat és a termés megfelelő elosztására használták fel azokat. Egy másik példa a dél-amerikai Inka Birodalom, ahol a növényi kultúrákat analizálták bizonyos gazdálkodási trendek és minták meghatározásához, melyhez adatrögzítő módszerként a quipu névre hallgató csomóírást alkalmazták. (Érdekesség, hogy ezt az írásrendszert szokás háromdimenziós kettes számrendszernek is hívni.)

Ha kicsit ugrunk az időben, érdekes példát találunk az 1880-as USA népszámlálás idején. A népszámlálás adatainak feldolgozása és szerkesztése 9 évig tartott, ebből 7 teljes évet vett igénybe a statisztikai analízis.

Az adatfeldolgozást és elemzést a számítógép 20. századi megjelenése forradalmasította. 1952-ben az első számítógépek egyikén, az UNIVAC-on készült az első számítógépes előrejelzés az USA elnökválasztás várható kimeneteléről. A számítógép a CBS előrejelzésével ellentétben Eisenhowert jósolta a választások győztesének és igaza is lett.

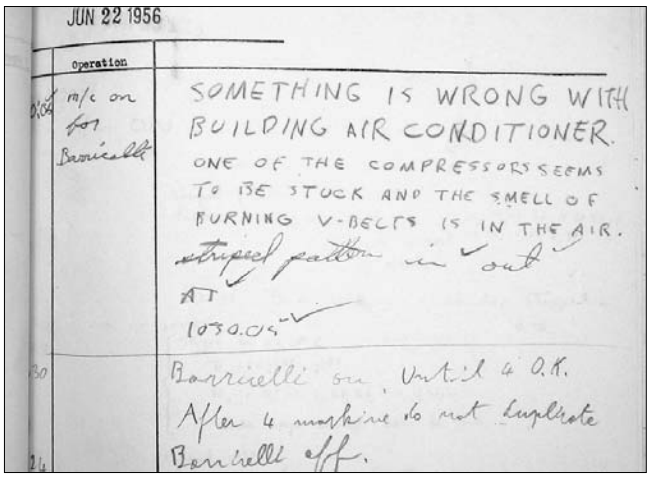
A tömeges alkalmazás elterjedésében az adatok számítógéppel végzett elemzésének üzleti célú alkalmazása, a döntéstámogatás segítése volt az igazi fegyvertény. 1989-ben nevezték el a módszert üzleti intelligenciának és írták le a koncepcióját, metodológiáját. Az üzleti intelligencia tökéletesítette a döntéshozatalt a tényalapú támogatási rendszernek köszönhetően. A prediktív analízis, vagyis az előrejelző vizsgálati módszertan 1999-ben debütált. Az üzleti életben nagy jelentősége van annak, hogy a meglévő adatokból következtetni tudjunk a jövő trendjeire, ez az egyik alapvető funkciója egy teljes értékű informatikai logelemzésnek is, mint azt a későbbiekben látni fogjuk.

A számítógép megjelenése nem csak azt eredményezte, hogy az adatfeldolgozás sebessége ugrásszerűen megnőtt, így az elemzések soha nem látott komplexitással és hatékonysággal lettek elvégezhetők, hanem egyben a számítógép maga is problémák forrásává vált, többek között a saját maga által generált, hatalmas mennyiségű adat miatt.

2. A log

A fenti példák egyértelműen igazolják, hogy az adatok összegyűjtése és elemzése minden korban rendkívül fontos szerepet játszott. Napjainkban az információs rendszerek megfelelő működésének és fejlődésének biztosításához a rendszerek naplóadatainak elemzése szolgáltat megfelelő alapot.

A naplózás alkalmas arra, hogy feltérképezzük a rendszerben felmerülő problémákat, időrendbe állítsuk azokat, megtaláljuk a lehetséges megoldásokat, kidolgozzuk az elhárítási terveket, s azok segítségével végül felülkerekedjünk a problémákon, mi több, az elemzett adatainkból következtetéseket vonjunk le a jövő fenyegetéseinek elkerülése érdekében.


JUN 22 1956

Operation

m/c on for Barnicelli

SOMETHING IS WRONG WITH BUILDING AIR CONDITIONER. ONE OF THE COMPRESSORS SEEMS TO BE STUCK AND THE SMELL OF BURNING V-BELTS IS IN THE AIR.

stripped pattern in out

AT 1030.04

Barnicelli on Until 4 O.K.

After 4 machine do not duplicate

Barnicelli off.

1. ábra Kézi naplózás az ötvenes évekből

A log a számítógép naplóbejegyzése. Amióta számítógép létezik, azóta létezik log is. Kicsit leegyszerűsítve a definíciót, a log nem más, mint a számítógép által generált naplóbejegyzés valamilyen, a számítógép működése közben megtörtént eseményről és annak fontosabb paramétereiről.

A számítógépek működése során rengeteg esemény következik be. Minden egyes esemény változást jelent az adott rendszer vagy eszköz állapotában. Számítógépes biztonsági szempontból az esemény egy tevékenység eredménye, mely egy adott cél elérésének érdekében történik.

A számítógép és a rajta futó szoftverek szimbiózisa meglehetősen bonyolult, komplex rendszer, sok beavatkozási ponttal, s persze rengeteg hibalehetőséggel. A rendszer az emberi felfogóképességhez képest rendkívül nagy sebességgel működik. Ennek köszönhetően az embernek (a számítógépkezelőnek) esélye sincs az eseményeket, esetleges hibákat, rossz működést vagy valamilyen, a működésre jellemző fontos paraméter változását valós időben, működés közben észlelni, nemhogy kezelni.

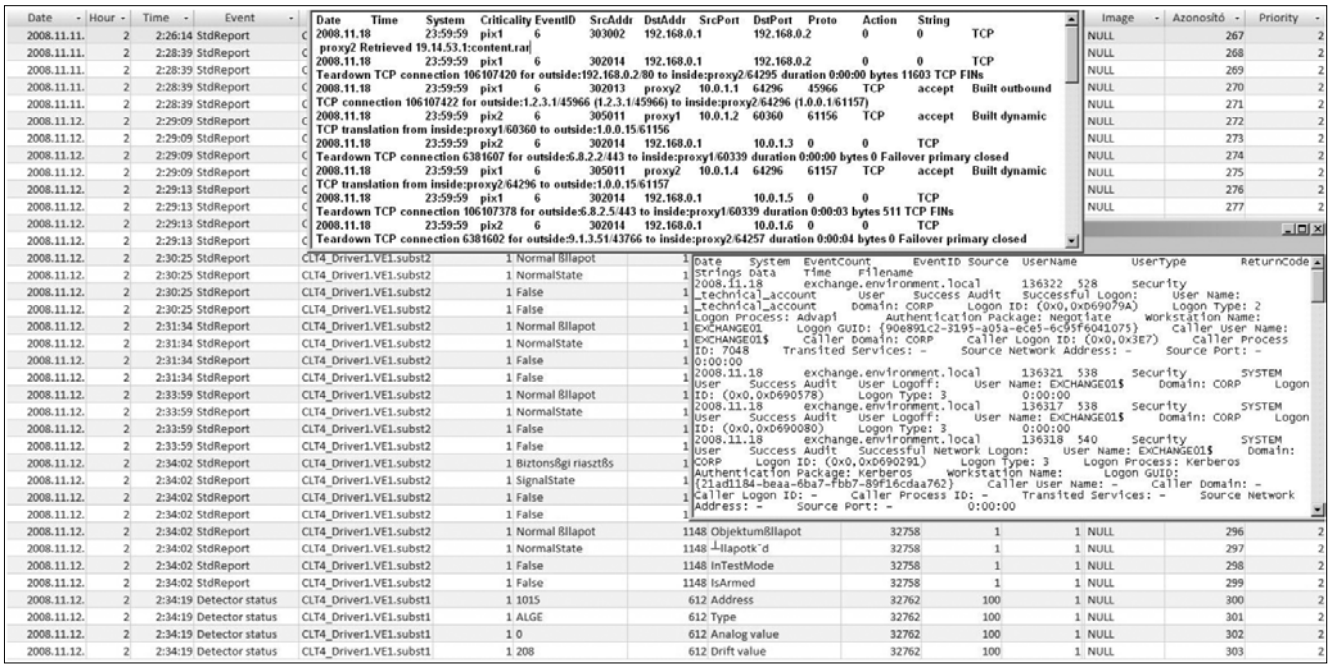
Ugyanakkor, ha ezekről az eseményekről, történésekről a számítógép vagy a rajta futó szoftverek készítenek egy-egy feljegyzést, akkor a feljegyzések alapján később visszakövethetővé, értelmezhetővé válik, hogy mi minden zajlott le a gépben, mi okozott hibát, leállást, biztonsági krízishelyzetet stb. A naplófájl a számítógépes események fontosabb paramétereit automatikusan rögzíti és olvashatóan megjeleníti, így lehetővé teszi azok utólagos ellenőrzését, elemzését.

Önmagában véve egyetlen számítógép is figyelemre méltó mennyiségű logot tud generálni, ám a számítógép-hálózatok minden korábbi várakozást felülmúló elterjedésével a szakembereknek ma már igen nagy méretű és bonyolultságú, komplex informatikai rendszerekkel kell megbirkózniuk. Ezek működése hihetetlenül összetett, így nagyságrendekkel több a hibalehetőség, a valamilyen reakciót, beavatkozást igénylő rendszerállapot-változás, amit kezelni kell. Elengedhetetlen tehát, hogy az eseményekről, hibákról, állapotváltozásokról valamiféle visszajelzést kapjunk naplóbejegyzések formájában.

Az informatikai rendszerek főbb alkotóelemei, az operációs rendszerek, alkalmazások, különféle szoftver és hardver komponensek működésük során mind, mind naplófájlokat generálnak, milliónyi naplóbejegyzéssel, loggal. Az információbiztonsági szempontok megkövetelik, hogy a felhasználók tevékenységéről, a rendszerek működéséről, a hozzáférési jogosultságok változásairól szóló bejegyzések folyamatosan követhetőek legyenek.

Az adatoknak azonban önmagukban nincs jelentésük. Az adatok az értelmezéstől, a feldolgozás módjától, alkalmazásuktól nyernek értelmet és válhatnak értékes információvá.

2. ábra „Gépi” naplózás fél évszázaddal később



Date	Hour	Time	Event	
2008.11.11.	2	2:26:14	StdReport	C
2008.11.11.	2	2:28:39	StdReport	C
2008.11.11.	2	2:28:39	StdReport	C
2008.11.11.	2	2:28:39	StdReport	C
2008.11.11.	2	2:28:39	StdReport	C
2008.11.12.	2	2:29:09	StdReport	C
2008.11.12.	2	2:29:09	StdReport	C
2008.11.12.	2	2:29:09	StdReport	C
2008.11.12.	2	2:29:09	StdReport	C
2008.11.12.	2	2:29:13	StdReport	C
2008.11.12.	2	2:29:13	StdReport	C
2008.11.12.	2	2:29:13	StdReport	C
2008.11.12.	2	2:30:25	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:30:25	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:30:25	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:30:25	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:31:34	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:31:34	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:31:34	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:31:34	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:33:59	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:33:59	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:33:59	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:33:59	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:34:02	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:34:02	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:34:02	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:34:02	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:34:02	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:34:02	StdReport	CLT4_Driver1.VE1.subst2
2008.11.12.	2	2:34:19	Detector status	CLT4_Driver1.VE1.subst1
2008.11.12.	2	2:34:19	Detector status	CLT4_Driver1.VE1.subst1
2008.11.12.	2	2:34:19	Detector status	CLT4_Driver1.VE1.subst1
2008.11.12.	2	2:34:19	Detector status	CLT4_Driver1.VE1.subst1

Image	Azonosító	Priority
NULL	267	2
NULL	268	2
NULL	269	2
NULL	270	2
NULL	271	2
NULL	272	2
NULL	273	2
NULL	274	2
NULL	275	2
NULL	276	2
NULL	277	2
NULL	296	2
NULL	297	2
NULL	298	2
NULL	299	2
NULL	300	2
NULL	301	2
NULL	302	2
NULL	303	2

A napjaink informatikai rendszereiben keletkező logok mennyisége messze meghaladja azt a mértéket, ami hagyományos rendszergazdai vagy üzemeltetői kompetenciát és erre fordítható időt feltételezve emberléptékűnek és feldolgozhatónak nevezhető, a hatékonyságot nem is említve. Pedig éppen a rendszerek komplex mivolta követelné meg még inkább a naplóadatok rendszeres, alapos elemzését. A naplófájlok vizsgálatával és értelmezésével a rendszer működése rekonstruálható, az abban előállt rendellenességek és egyéb nem várt események forrásai felkutathatóak, különös tekintettel például a rendszert érő külső és belső támadásokra. Később erről részletesebben is írunk.

Konkrét példát nézve, egy átlagos, közepesen terhelt tűzfal naponta kb. 2 és fél millió logot termel. Ebből gyakorlatilag néhányszor tíz, esetleg néhányszor száz log az, amely konkrét és releváns információt hordoz, és nagyjából egymillió a figyelmen kívül hagyható bejegyzés. Ahhoz viszont, hogy a konkrét jelzésekből trendekre, a körülményekre, az ok-okozati összefüggésekre következtetni lehessen, meg kell vizsgálni a maradék másfél millió logot is.

3. A logelemzés

A logelemzés segítségével feldolgozásra kerülnek a különböző formátumú, struktúrájú és forrású események, így lehetővé válik az informatikai rendszer állapotával kapcsolatos kép rekonstruálása és riportokba foglalása.

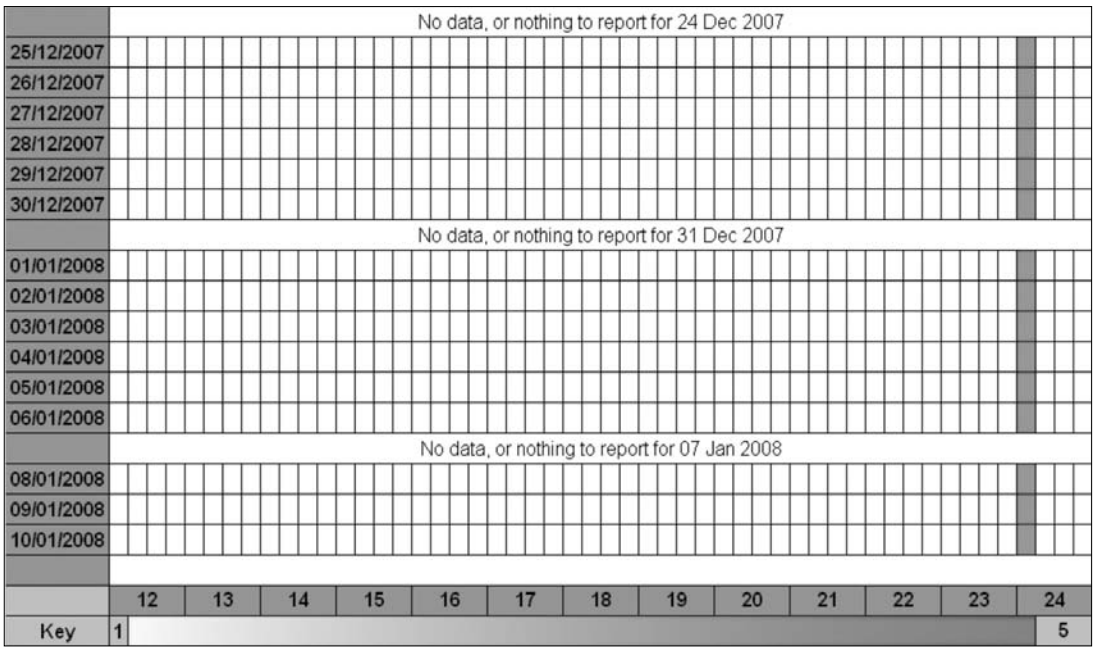
Mivel a rendszerek elképesztő mennyiségű logot generálnak, a rendszerüzemeltetők gyakran éreznek indíttatást a logok mennyiségének minimalizálása. Ezzel sok esetben halálra ítélik a feldolgozás lehetőségét, hiszen az események úgy csökkenthetőek a leghatékonyabban, ha a bejegyzések legnagyobb részét alkotó, informális üzeneteket kikapcsoljuk. Ezzel azonban elvágjuk magunkat attól a lehetőségtől, hogy egy vizsgálandó incidens esetén az azzal összefüggő, azt leíró eseményeket, körülményeket együttesen vizsgáljuk.

Az általunk incidensnek nevezett, nem kívánt események nem csak úgy „lesznek”. Nincs olyan esemény, amely egymagában képes romba dönteni jól felépített és féltve őrzött rendszereinket, hogy aztán az ismeretlenség jótékony homályába húzódva várakozzon a helyreállítási műveletek befejezéséig, hogy azt követően aztán újra lecsaphasson.

Az informatikai hálózat a komplex rendszerekre jellemző módon az elemek közötti összefüggésekkel írható le a legjobban. Ebből következően az incidenseket mindig megelőzi a rendszerkörnyezetben bekövetkező „viselkedésbeli” változás. Bizonyos események száma megnő, míg ezzel egyidőben másoké csökken. Ha csak a kritikus hibákra vagy figyelmeztető üzenetekre koncentrálunk, gyakran éppen a lényeget tévesztjük szem elől. A tettes felkutatásához kevés lesz pusztán a nyitva hagyott ablak és az üres ékszeres doboz közötti összefüggés vizsgálatára hagyatkoznunk.

Az elmúlt 5 év gyakorlati tapasztalatainak összegzéseképpen 2007-ben elkészítettük a logelemzés ökölszabályain alapuló ötlépcsős elemzési modellt, amelyben nagyvonalakban rögzítettük a logokkal kapcsolatos teendőket. Az öt lépcső: a gyűjtés, a normalizálás, az értelmezés, az elemzés és a riportolás.

Az első és legfontosabb a feldolgozandó információk összegyűjtése egy központba. Az adatokat ezután különböző tulajdonságaik alapján egységes, közös struktúrába rendezzük, ami biztosítja, hogy az adatbázis mezőiben homogén adatokat találjunk. (Ilyenek például a keletkezés dátuma, ideje, helye, típusa stb.) Az értelmezési fázisban kutatjuk a bejegyzések jelentését, melyek alapján emberi, de legalábbis elemzői fogyasztásra alkalmassá válnak. A negyedik, elemzési fázis a tényleges adatbányászat, az összefüggések és korrelációk felderítésének ideje, itt kerülnek a helyükre a kirakós elemei. Az utolsó munkafolyamat a riport elkészítése, ahol



3. ábra
Éjszakai mentés hibamintázata egy hőtérképes megjelenítőn

A hőtérkép kifejezés itt nem az eredeti jelentésével értendő, a színskála (az ábra legalján lévő csík) szerinti érték-megjelenítésre utal. A színskála színei 1-től 5-ig terjedő értékeket mutatnak, ami az adott időintervallumban bekövetkező események számát jelzi. Az ábrán a mentés hibajelzése látható, ami a 23h-ás mindennapi mentéskor megjelenik, vagyis amikor mentés történik, akkor az hibára fut.

a feltárt jelenségeket tényadatokkal és grafikonokkal alátámasztva dokumentációvá alakítjuk.

A logelemzést szakmai körökben információs hulladék-újrahasznosításnak is hívjuk, mivel a log az informatikai rendszerek működésének szükségszerű mellékterméke, ahogy a hulladék mellékterméke az emberi fogyasztásnak. Ezt a mellékterméket megfelelően kezelve értékes nyersanyagokhoz juthatunk. Az elemzési modell fázisai logikusan egymásra épülnek, pont úgy, ahogy a hulladékgyűjtő telepeken a beérkező anyagok kezelését, válogatását, továbbítását, csomagolását és elszállítását szabályozó munkafázisok.

4. Mivel elemezzünk?

Melyik a legjobb eszköz a logok elemzéséhez? Milyen szoftvert/hardvert válasszunk? Mint ahogyan az általában lenni szokott, itt sem létezik olyan univerzális termék, ami mindenben a legjobb. Vannak azonban jól bevált részmegoldások, melyeket megfelelően ötvözve hatékony gyűjtő és elemző rendszerek alakíthatóak ki.

A logelemzés egyik alapvető problémája, hogy szabványos logformátum mint olyan, egyáltalán nem létezik. Ahány rendszer, annyi féle felépítésű naplóbejegyzéssel és tárolási formátummal találkozhatunk. Vannak szövegfájlként, bináris adatfájlként és adatbázisrekordként tárolt bejegyzések, valamint teljes a skála az egyszerű egysoros jól strukturált bejegyzéstől a több sort kitöltő, dinamikusan változó tartalmúig. A naplóbejegyzések egyaránt tartalmazhatnak hagyományos alfanumerikus, vagy speciális írásjeleket, illetve a bináristól a hexadecimális skáláig terjedő numerikus értékeket is. Minél átfogóbb, teljesebb körű megoldást szeretnénk kialakítani, annál komolyabb, összetettebb problémákkal találjuk magunkat szemben.

A gyűjtés legelterjedtebb módja a syslog protokollon alapuló átirányítás, amely még a UNIX kezdeti időszakából származik és bizony mára jócskán eljárt felette az idő. Nagy előny viszont, hogy többé-kevésbé minden rendszer támogatja.

Változást jelent napjainkban, hogy egyre több gyártó és felhasználó szervezet kezdi felismerni, hogy a logok kezelése legalább annyira fontos (sőt, sok esetben fontosabb!), mint maguk a rendszerekben tárolt adatok. Emiatt a gyors, ámde nem garantált UDP protokoll helyett megjelentek a TCP protokollt és azon felül titkosítást is alkalmazó gyűjtő technológiák, de igen gyakori a fájlszintű másolás is.

Szakembereink, a komplex, elosztott terhelésű logadattárházak építését látják a leghatékonyabb megoldásnak. Ennek méretezésekor úgy kell kalkulálni, hogy a keletkező logok gyűjtésén és hosszú távú tárolásán felül az adatbányászatra is megfelelő lehetőség nyíljon. Az értelmezési feladatok és műveletek elvégzéséhez nélkülözhetetlen, de sokszor nem kis nehézséget jelentő normalizálás során a logok származási hely és formátum szerint azonos struktúrába kerülnek, így olvasás helyett inkább a számolási képességünkön van a hangsúly.

A logok bányászatához szükséges OLAP (On-Line Analytical Processing – valós idejű adatelemzés) adatbázisok alapjául, a kereskedelmi, pénzügyi elemző rendszereknél megszokotthoz hasonlóan, a produktív rendszerekből kinyert információk szolgálnak. Ezeket különböző szempontok szerint rendezve vizsgáljuk.

5. Logelemző intelligencia

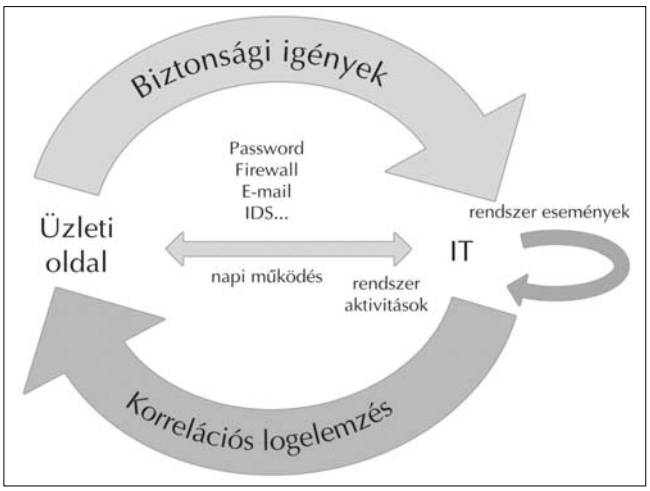
A piacon fellelhető logelemző termékek legfőbb ismérvei, hogy képesek az általánosan elterjedt rendszerek logjainak gyűjtésére, tárolására, archiválására, rendelkeznek néhány törvényi vagy jogszabályi megfelelőségi paraméterrel és ezekre optimalizált előre definiált riportokkal (GLBA, HIPAA, PCI, SOX stb.) Ezeken túl a riportok személyre szabhatóak a felhasználó szájíze szerint, tartalmaznak valamilyen riasztási funkciót és képesek az események közötti egyszerűbb korrelációk megvilágítására.

Ezek a logelemző termékek azonban nem oldják meg teljeskörűen a logelemzés problémáját, a szervezetek menedzsmentje és az informatikát üzemeltetők számára a logelemzésben rejlő széleskörű lehetőségeket és előnyöket csak kismértékben használják ki.

A gyártók fejlesztési tervei az általuk ismert univerzumból indulnak ki, mely azonban sok esetben hiányos. Hatékony terméket létrehozni egy ilyen kaotikus, szabványmentes környezetben nagyon nehéz, majdhogynem lehetetlen feladat. A túl sok logformátum támogatásával a rendszer egésze lassú lesz, a döntési mechanizmusok pedig rendkívül bonyolulttá válnak. Ha viszont kizárólag az elterjedt formátumok támogatására fókuszálnak, akkor a fejlesztések sablonos logmonitoring rendszerek létrehozásába fulladnak, amelyek csak igen korlátozott logelemző funkcionalitással bírnak.

Tapasztalataink alapján jelenleg nem létezik egyetlen olyan kész logelemző termék sem, amely egy szervezet logelemzési igényeit képes lenne maradéktalanul kielégíteni. A különböző területeken alkalmazott részmegoldások és az elemzéshez használt emberi intelligencia,

4. ábra
Üzleti oldal és logelemzés kapcsolata (forrás: KÜRT Zrt.)



illetve döntéshozatali mechanizmusok ötvözésével és segítségével azonban képesek vagyunk hatékony elemző rendszerek kialakítására és üzemeltetésére. Nem szabad azt sem elfelejteni, hogy az elemzői tevékenység a rendszerüzemeltetőkétől távolabbi, holisztikus nézőpontot igényel. Ennek a szemléletnek a hiánya lehet az oka annak is, hogy viszonylag magas számú, félresikerült termékbevezetésre van példa a piacon.

A logelemzés szükségességét egyre több szervezet ismeri fel, a megoldást azonban csak kevesen ismerik. A megoldás egy olyan termékfüggetlen logelemző szolgáltatás, ahol a rendszer felmérését követően optimális, folyamatos szolgáltatás megvalósítása a cél. Az alkalmazott szoftverek körét minden esetben az ügyfél rendszerének ismeretében alakítják ki a szakemberek és annak érdekében, hogy legkönnyebben juthassanak a megfelelő információk birtokába, saját fejlesztésű szoftver-komponensekkel egészítik ki ezt a kört. A gyakorlat eddig számos esetben igazolja, hogy a hatékony logelemző rendszer legfontosabb láncszeme a beégetett algoritmusoktól mentes, szabad döntések meghozatalára és intuícióra képes humán elemző.

A lehetőségeket jól kiaknázó, humán intelligenciával támogatott logelemző szolgáltatás az informatikai rendszer biztonsági szintjének fenntartásában betöltött nélkülözhetetlen szerepe mellett mérhetővé teszi az üzleti oldal számára az informatikai szolgáltatásokat, beruházásokat, fejlesztési igényeket és az informatikai rendszer sokszor átláthatatlannak tűnő működését. Erről lesz szó részletesebben a következő szakaszban.

6. Logelemzésre épülő szolgáltatások

Az informatikai rendszerek hőskorában, különösen a hálózatok kialakulásának kezdetén a logelemzés, mint informatikai „módszer”, önmagában nem létezett. A rendszerfejlesztők, alkalmazásfejlesztők különböző programrészeket „használtak” arra, hogy nyomon követhessék a programokban bekövetkező hibákat, állapotváltozásokat.

Az „áttörést” a hálózatos működéssel együtt megjelenő, többfelhasználós rendszerek megjelenése jelentette, mivel itt már azt is ki kellett mutatni, hogy mikor, ki használt egy-egy terminált, szolgáltatást. Az akkori informatikai rendszerek nem voltak annyira összetettek, mint a mai hálózatok, jellemzően célmegoldásokra használták azokat, a legtöbbször kutatók és programozók. A mai felhasználói réteg akkor még nem alakult ki, a nyomonkövethetőség igénye azonban már a kezdetek kezdetekor is létezett, mivel az első hálózatok és alkalmazások leginkább katonai célokra alakultak ki.

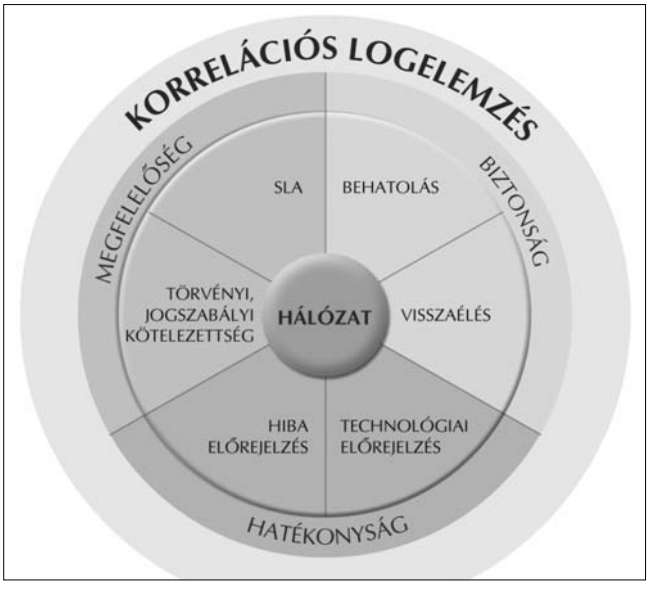
A nyomonkövethetőséget a nagy vállalati hálózatok és az internetes szolgáltatások megjelenése erősítette, de akkor ez kimerült a határvédelmi rendszerek és a szerverek erőforrásainak monitorozásában. A tűzfalak és szerverek eseményeinek monitorozását megoldani képes hálózat-monitoring, erőforrás-monitoring rendszerek elterjedésével a felhasználók valós idejű információkkal rendelkeztek az üzemeltetett hardver és szoftverpark pillanatnyi állapotáról, változásairól. A 90-es évek elejétől terjedő web exponenciálisan növelte meg a rendszerek működéséről kimutatható információéhséget, mivel itt bekapcsolódtak a vállalatok üzleti szintjei is.

A vállalati hálózatok növekedésével a bennük tárolt információ mennyisége elképesztő mértékben növekedett és ez a növekedés a mai napig tart. Az adatbázisokban egyre gyorsabban, egyre több adat tárolódott és megjelentek a vezetői információs igények is. Ennek kézbentartására aztán kialakultak a nagy ERP és HR rendszerek, a védelmi szinteken elindult az IDS-ek (Intrusion Detection Systems – behatolásjelző rendszerek) és a tűzfalmegoldások forradalma is.

A korábbi esemény-monitoring funkciókat rendre kiegészítették az adatokat historikusan kezelő modulok is, a múltbeli események „visszajátszására” képes programrészek. Az alapfelfogás mind a mai napig az, hogy a rendszereseményekből ki kell tudni válogatni a biztonságra, felhasználásra vonatkozókat és azokat „jelezni” kell tudni az üzemeltetők felé. Az üzleti alkalmazhatóság, a pénzügyi rendszerek és az on-line szolgáltatások elterjedése azonban a rendszeresemények „visszajátszhatóságát” is megköveteli. Így már nem elég csupán néhány kiválasztott esemény bekövetkezését jelezni, hanem a rendszerek eseményeit leíró adatokat, logállományokat el is kell tárolni. Kialakultak a loggyűjtést és tárolást megoldó központi szerverek. A hálózatok sebességnövekedése egy időn túl lehetővé tette a rendszer összes eseményének egy központi helyre való továbbítását is.

Az így kialakult megoldások számos lehetőséget biztosítanak a rendszerüzemeltetők, vállalatok számára. Az események statisztikai elemzése leginkább a vezetői információs rendszerekben jelenik meg, az üzemeltetés területén pedig az események mielőbbi jelzése a prioritás. Az on-line marketig térhódítása a rendszerfelhasználás, látogatottság-mérés, a pénzügyi-tranzakciók „videomagnószerű” visszajátszhatóságát, mérését célzó

5. ábra
A korrelációs logelemzés helye a szervezet információbiztonsági rendszerében (forrás: KÜRT Zrt.)



megoldások fejlődését indukálják, míg a megnövekedett biztonsági igények az internetes támadások, vírustámadások jelezhetőségét erősítik. A kialakult helyzetben ez a két fő irány szervesen elválasztásra került, így a pénzügyi, vállalatirányítási rendszerek a naplóállományok elemzésére, míg az üzemeltetői rendszerek az események jelzésére helyezik a hangsúlyt.

Az általunk kidolgozott megoldás e két területet együtt célozza meg, így a logok összegyűjtését követően, azok elemzésével mindkét terület számára képes olyan információkat kinyerni, amelyek korábban nem voltak elérhetők. A tűzfalak, IDS-ek, szerverek eseményeit nem önmagukban, hanem a vállalatok informatikai rendszereinek összes alkotóelemével együtt vizsgálják. Ezzel a megoldással lehetőség nyílik arra, hogy az informatikai vezetők, vállalatvezetők naprakész információkhoz jussanak az informatikai rendszer mindenkori állapotáról, annak viselkedéséről.

A napi logelemzés elsődlegesen az üzemeltetők számára biztosít információkat a rendszerhibák, anomáliák elhárításához. Ennek segítségével az üzemeltetőknek nem kell a logokban keresgélniük a problémák után, hiszen azt az elemzés elvégzi, ráadásul javaslatokat tesz a hibák elhárítására, pénzt és időt megtakarítva ezzel az amúgy is kislétszámú informatikai területeknek.

A szolgáltatás alapvető funkciója továbbá a rendszerek biztonsági szempontú elemzése. A rendszerek biztonságát fenyegető események kiszűrésével és elemzésével elkerülhetőek a tömeges hibás riasztások és rendkívül hatékony incidens-kezelés alakítható ki.

Az összegyűjtött és központilag tárolt naplóállományok segítségével a rendszerösszeomlások, csalások, visszaélések informatikai nyomai is feltárhatóak, így támogatva a forensics, azaz az események okait utólag felderíteni szándékozó, nyomozati jellegű vizsgálatokat.

A logállományok napi feldolgozásával az informatikai rendszerek rendelkezésreállás-mérése is kiválóan megoldható. A napjainkban elterjedt outsource megoldások, valamint a vállalatvezetők stratégiai rendelkezésreállás követelményei elengedhetetlenné teszik a komoly SLA-k (Service Level Agreement-ek) „bevállalását”, a rendelkezésreállás folyamatos biztosítását.

Leginkább a pénzügyi területeken, on-line szolgáltatások esetén van igény az úgynevezett fraud-management megoldásokra, ahol a logelemzés az esetleges visszaélések kivizsgálását képes támogatni.

Az informatikai vezetők folyamatosan harcolnak a megfelelő anyagi erőforrások biztosításáért, alapvetően az üzemeltetők információira támaszkodva. A vállalatok újabb és újabb szolgáltatások bevezetésével szeretnék bevételeiket növelni, amelynek következtében az informatikai rendszerek folyamatosan változnak. Időnként elavulnak, az új rendszerelemek fejlesztése komoly változásokat eredményez, a folyamatos változás pedig megnöveli a biztonsági kockázatokat. A logelemző szolgáltatás napi információkat képes nyújtani az elavult rendszerkomponensekről, a fejlesztés alatt álló alkalmazások, szegmensek hibáiról, valamint a komplex hálózatok pillanatnyi sérülékenységeiről is.

7. Jövőkép

A logelemzés fejlődése a jelenlegi tendenciák alapján a real-time logelemzés és a konvergencia irányába halad.

Folyamatosan változó világunkban a döntéshozók egyre pontosabb és egyre gyorsabb eredményeket követelnek, ezért az adatok elemzése, így a logelemzés is a valós idejű monitoring és elemzés megvalósítására törekszik. Ez egyben a két funkció egymáshoz való közelítését is jelenti, vagyis a monitoring és az elemzés, amelyek ma még elkülönülnek, egyre inkább összeolvadnak majd. Ez persze egyenesen következik abból, hogy a monitoring eleve valósidejű funkció és a tendencia az, hogy az elemzés is ebbe az irányba halad.

A logelemzésnél jelenleg elsősorban technológiai akadályai vannak annak, hogy real-time, valós időben folyhasson az elemzés. Ezek elsősorban a logok, naplófájlok azonnali hozzáférhetőségével, feldolgozhatóságával, értelmezhetővé tételével, normalizálásával vannak kapcsolatban. A technológiák fejlődésének iránya ugyanakkor egyértelműen azt mutatja, hogy a jövőben a real-time logelemzés kap majd egyre nagyobb hangsúlyt.

A konvergenciáról, ugyancsak elmondható, hogy a technológia számos területén varázsszónak számít. A logelemzés vonatkozásában a cél a fizikai és logikai biztonság területéről származó információk és logok közös platformon, együtt történő kezelése. Ezzel a módszerrel lényegesen hatékonyabbá és gyorsabbá válhat az informatika számtalan területéről, s a különböző biztonsági (beléptető, tűzvédelmi, behatolásjelző, zártláncú video stb.) rendszerekből érkező logok és jelzések értékelése. A KÜRT-nél ezzel a témával kapcsolatban konkrét fejlesztések folynak, ilyen értelemben a konvergencia már nem is annyira jövőbeli tendenciája a logelemzésnek.

A szerzőkről

FABIÁNYI GÁBOR 1987-ben végzett a BME Villamosmérnöki Karán. 12 éve dolgozik a KÜRT Zrt-nél, 10 éve marketingmenedzserként. Részt vett a cég információbiztonsági portfoliójának kialakításában, két évig szerkesztette a KÜRT Informatikai Biztonság című szakmai hírlevelét.

FRÉSZ FERENC Budapesten született, 2003-ban diplomázott, tanítói szakon. Újságíróként dolgozott, majd az informatikában indított oktatási, tanácsadói vállalkozást a 90-es évek közepén. Biztonsági szakértőként, majd a Budapest Airport informatikai vezetőjeként szerzett tapasztalatokat a vállalati rendszerek sérülékenységeiről, viselkedéséről. Számos vállalat IT vezetőjeként folytatta pályáját, amelynek keretében több mint 500 biztonsági projektet irányított. Az így szerzett tapasztalatai alapján dolgozta ki a KÜRT logelemzési és legális hackelési módszertanait. Jelenleg a KÜRT Zrt. Biztonsági Intelligencia Központjának vezetője.

SZABÓ LÁSZLÓ a KÜRT Információmenedzsment Megoldások Üzletág Logelemzés csoportjának szakértője. Több hazai vállalat logelemzés projektjében vett és vesz részt. Munkája során loggyűjtő és -elemző, illetve IDS rendszerek finomhangolásával, trendelemzéssel, valamint biztonsági események detektálásával és mintaelemzésével foglalkozik. Tevékenységi területe kiterjed a fizikai biztonsági terület és az informatikai rendszerek eseményeinek vizsgálatára is.

ZSILINSZKY SÁNDOR Budapesten született, itt végezte középiskolai tanulmányait, majd 1984-ben kapott diplomát a Budapesti Műszaki Egyetem Villamosmérnöki karán, Híradástechnika szakon. Az egyetem elvégzése után a hazai informatikai iparban helyezkedett el, mint hardverszakértő. Később a KÜRT-nél számos informatikai biztonsági fejlesztésben vett részt, mint például a cég Informatikai Biztonsági Technológiájának kifejlesztése (IBiT). Jelenleg üzletágvezetőként dolgozik a KÜRT Zrt-ben és aktív részese a logelemzési technológia továbbfejlesztésének, melyről több cikke és konferencia-anyaga is megjelent.

Biztonságos Wi-Fi hálózat tervezése

RÉTI ZOLTÁN, CZUCZ DÁVID

Synergon Informatikai Nyrt.
{reti.zoltan, czucz.david}@synergon.hu

Kulcsszavak: Wi-Fi Site Survey, WLAN, RF tervezés, Wireless Controller, EAP-TLS, biztonságos Wi-Fi hálózat

A megnövekedett mobilszámítógép-felhasználás maga után vonta a vezetéknélküli hálózatok ugrásszerű növekedését is. A szabadon használható WLAN frekvenciák üzleti célú alkalmazásakor elengedhetetlen a megfelelő biztonsági megoldások használata, illetőleg az előzetes rádiófrekvenciás tervezés és mérés. Írásunkban egy konkrét, nagyvállalati környezetben megvalósított rendszeren keresztül mutatjuk be egy WLAN hálózat tervezését, mérését, megvalósítását és felügyeletét.

1. Bevezetés

Napjaink mobil számítógépes világában igen csak megnövekedett a Wi-Fi alkalmazások száma. Az ingyenes frekvenciahasználat és az egyre olcsóbb berendezések megjelenése lehetővé tette a szabadon használható WLAN infrastruktúra széles körű elterjedését mind nagyvállalati, mind otthoni környezetben. Az egyre sűrűbb, egymástól függetlenül kiépülő rádiós infrastruktúrák megjelenése és üzemeltetése a felhasználóik számára azonban rengeteg hibaforrás kiinduló pontját jelentheti.

Amíg lokálisan csak a saját Wi-Fi hozzáférési hálózati rendszerünk működik a környezetünkben, addig könnyen kezelni lehet az esetlegesen felmerülő üzemeltetési problémákat. Azonban ha a közvetlen környezetében kettőnél több, egymástól független rendszer jelenik meg, nem lehet ugyanúgy kézben tartani a rádiós hálózatunk üzemeltetését megfelelő rádiófrekvenciás menedzsment nélkül. A vezetéknélküli rendszerünk berendezései interferenciás zavartatást fognak szenvedni és így a hálózat hozzáférési kapacitása sérülni fog. A kommunikáció bizonytalanná válik, ami legrosszabb esetben akár az összeköttetés megszakadását is eredményezheti.

Ebben a cikkben WLAN-ok rádiófrekvenciás tervezéséről és a biztonságos Wi-Fi-hálózat tervezésének módszereivel foglalkozunk.

2. WLAN-ok RF-tervezése

Egy-egy Wi-Fi hálózat kiépítésekor a felhasználók részben, vagy teljes egészében megfeledkeznek a rádiófrekvenciás (RF-) tervezés szükségszerűségéről. A tervezés első fázisában a kialakítandó rendszer optimális kihasználhatósága érdekében szükséges a környezet rádiófrekvenciás vizsgálata is.

A rádiós rendszerek által kisugárzott jel lefedettségének láthatóvá tétele, megjelenítése nagymértékben megkönnyíti a Wi-Fi rendszerek RF-tervezését, a telepítést követően pedig az üzemeltetését.

Mielőtt WLAN hozzáférési hálózati rendszert kívánunk üzembe helyezni, a tervezés első lépéseként lényeges előzetesen meggyőződni helyszíni felmérés (Site Survey) keretén belül

- az adott helyszín és annak környezetének rádiófrekvenciás telítettségéről, kihasználtságáról,
- a lefedendő terület rádiófrekvenciás interferencia zavartatást kiváltó tulajdonságairól,
- RF-szempontból a térrész jellegéről (zártságáról, nyitottságáról) és azt határoló elemek fizikai tulajdonságáról,
- mindazon egyéb felhasználói követelményekről és jellemzők meglétéről, melyek befolyásolhatják a telepítendő WLAN rendszerünk üzembiztos működését.

A helyszíni felmérést nagymértékben megkönnyíti egy erre alkalmas dokumentáló eszköz, a Site Survey program alkalmazása, mely képes a mérési eredményeket rögzíteni, majd különböző nézetekben hitelesen megjeleníteni és az egész műveletről megfelelő részletezéssel riportot készíteni.

Az aktív helyszíni felmérés során rádiófrekvenciás mérési pontokat kell felvenni egy mérő WLAN klienssel a lefedendő területen belül elhelyezett és ideiglenesen telepített vizsgáló AP (Access Point – elérési pont) közvetlen és távoli környezetében. A helyszíni felmérést megelőzően ismertnek kell lennie, hogy milyen céllal szükséges elvégezni a méréseket. Más és más a mérés lefolytatásának kimenetele és a WLAN hozzáférési hálózat tervezési procedúrája. Minden esetben szükséges megismerni ügyfél igényeit, amelyet a Wi-Fi hálózati rendszerrel szemben támaszt. Ezen igényeket célszerű rendszertechnikai tervben összefoglalni.

Új hálózat kiépítése esetén ismertnek kell lennie, hogy hova kell Wi-Fi lefedettséget biztosítani és az milyen vezetéknélküli LAN alkalmazást fog kiszolgálni. A vizsgálat célja, hogy meghatározásra kerüljön a WLAN hálózat csomópontjainak száma és helye, valamint ismertté váljon a zavaró objektumok és források helyzete.

A lefedettség igényét célszerű méretezett, méretarányos alaprajzon definiálni. A mérési elrendezés kiala-

kításához segítséget ad, ha az alaprajzon feltüntetésre kerülnek a helyiségek berendezései. A mérési pontok számát mindig az határozza meg, hogy a vizsgálandó helyszín mikrohullámú átviteli szempontból milyen telítettséggel rendelkezik. Más és más az elegendő mérési pontok száma nyílt, vagy erősen zárt (berendezett) helyiségek esetében. Nyílt tér esetében, amikor nagy valószínűséggel biztosítható az AP sugárzó elemének optikai láthatósága, csökkenthető a mérési pontok száma. Zárt, zsúfolt tér esetében célszerű minél részletesebb mérést készíteni.

A mérési pontokat a mérő az általa definiált útvonal mentén veszi fel. Ezért az alaprajznak a mérést megelőzően, hosszúságra kalibráltan rendelkezésre kell állnia a mérésadatgyűjtő programban (ESS Professional). Az összes begyűjtött rádiófrekvenciás mérési eredményeket a program a méretarányos alaprajzon grafikusan jeleníti meg. A mérésadatgyűjtő program utólagosan lehetőséget biztosít a mérési eredmények analizálásához, valamint a mért eredmények adminisztrációjához.

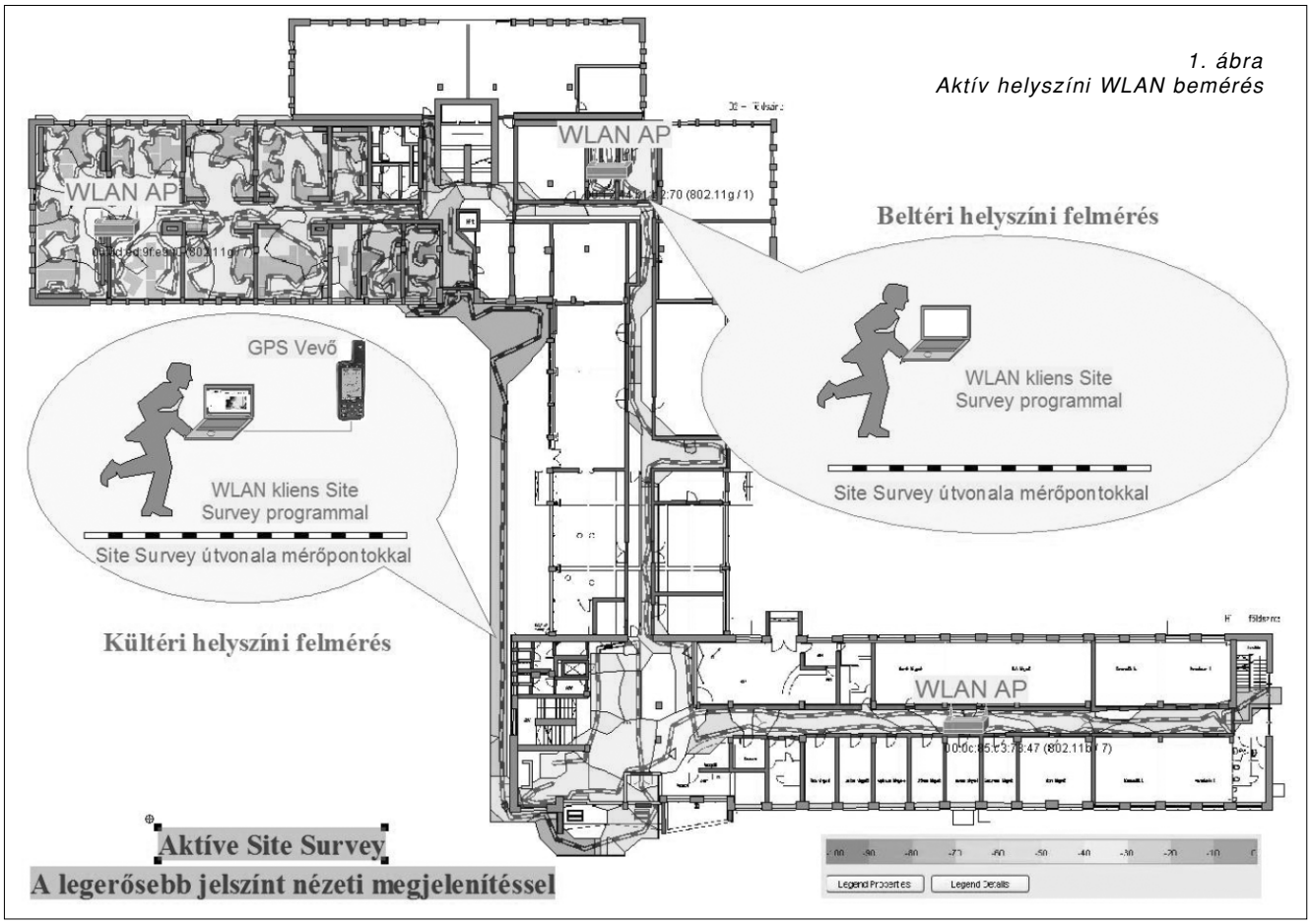
Az *1. ábrán* egy ESS v2.2 Prof programmal támogatott aktív site survey mérés folyamata látszik. Az AP-ok a „WLAN AP” pontba kerültek elhelyezésre. A mérő kliens végponttal a „fehér-fekete” vonallal jelölt útvonalon – valósan berendezett környezetben – megmértük a „WLAN AP” által indukált rádiófrekvenciás jelszint nagyságát.

A mért értékeket az ESSv2.2 Prof. program grafikusan jelenítette meg. A grafikus eredményt felhasználva az ESS program lehetőséget biztosít arra, hogy meghatározzuk a „WLAN AP” rádiófrekvenciás határfelületét. Ezt a vizsgált helyszín térrészére húzott egér kurzor segítségével tehetjük meg, amikor is a program megmutatja a mérővevővel detektált jelszint nagyságát. A kialakítandó hálózat tervezési paraméterének megfelelően (például a demodulációs értéknek megfelelő rádiófrekvenciás jelszint nagyságát figyelembe véve) szükséges elhelyezni és telepíteni a „WLAN AP”-t a következő mérőpontba. Az ideiglenesen telepített „WLAN AP” következő helyzetében ismételten mérési pontokat gyűjtünk, az ESS programmal és azt megjelenítünk. Ezt az iterációs folyamatot mindaddig végezzük, míg a megkívánt lefedett alapterületet bejártuk.

A mérés során a következő két fontos jellemzőt kell vizsgálni:

1) A vevő által mért rádiófrekvenciás jelteljesítmény nagyságát a vizsgált frekvenciasávban. Elsődlegesen az AP által kisugárzott és a vevőben indukált hasznos bejövő jelszint nagyságát mérjük, mely a hely függvényében megfelelően jellemzi az adott térrész rádiófrekvenciás lefedettségének jellemzőjét és a vevő vételi képességét.
2) A vevő által érzékelt rádiófrekvenciás jel-zaj viszony értékét, Signal to Noise Ratio (SNR).

A vizsgáló WLAN kliensen futó Site Survey programnak megfelelően rendszerezve kell begyűjteni a mérési adatokat a későbbi igényes kiértékelhetőség és megjeleníthetőség érdekében.



1. ábra
Aktív helyszíni WLAN bemérés

A szoftvernek képesnek kell lennie:
– a mérési eredmények RF-tervezés szempontjából fontos jellemzői szerinti megjelenítésére;
– tervezési funkciójával egy előre elkészített, modellezett helyszíni környezetben elhelyezett WLAN hálózat lefedettségének szemléltetésére;
– interferenciás zavartatás kialakulása helyének megmutatására;
– idegen WLAN hozzáférési hálózat AP rádiófrekvenciás jelének detektálására, helyzetének becslésére;
– a mért eredményekről részletes riport készítésére.

Az *1. ábra* szól a felmérésről és a korábban meghatározásra került peremfeltételeknek megfelelő (a rendszertechnikai tervben összefoglalt) WLAN AP elhelyezési tervezésről. Más és más WLAN AP szám és elhelyezési sűrűség szükséges egy kis kapacitású WLAN Ethernet átviteléhez, mint egy hangátvitelre szolgáló vagy helyfüggő alkalmazásokat kiszolgáló Wi-Fi tervezéséhez.

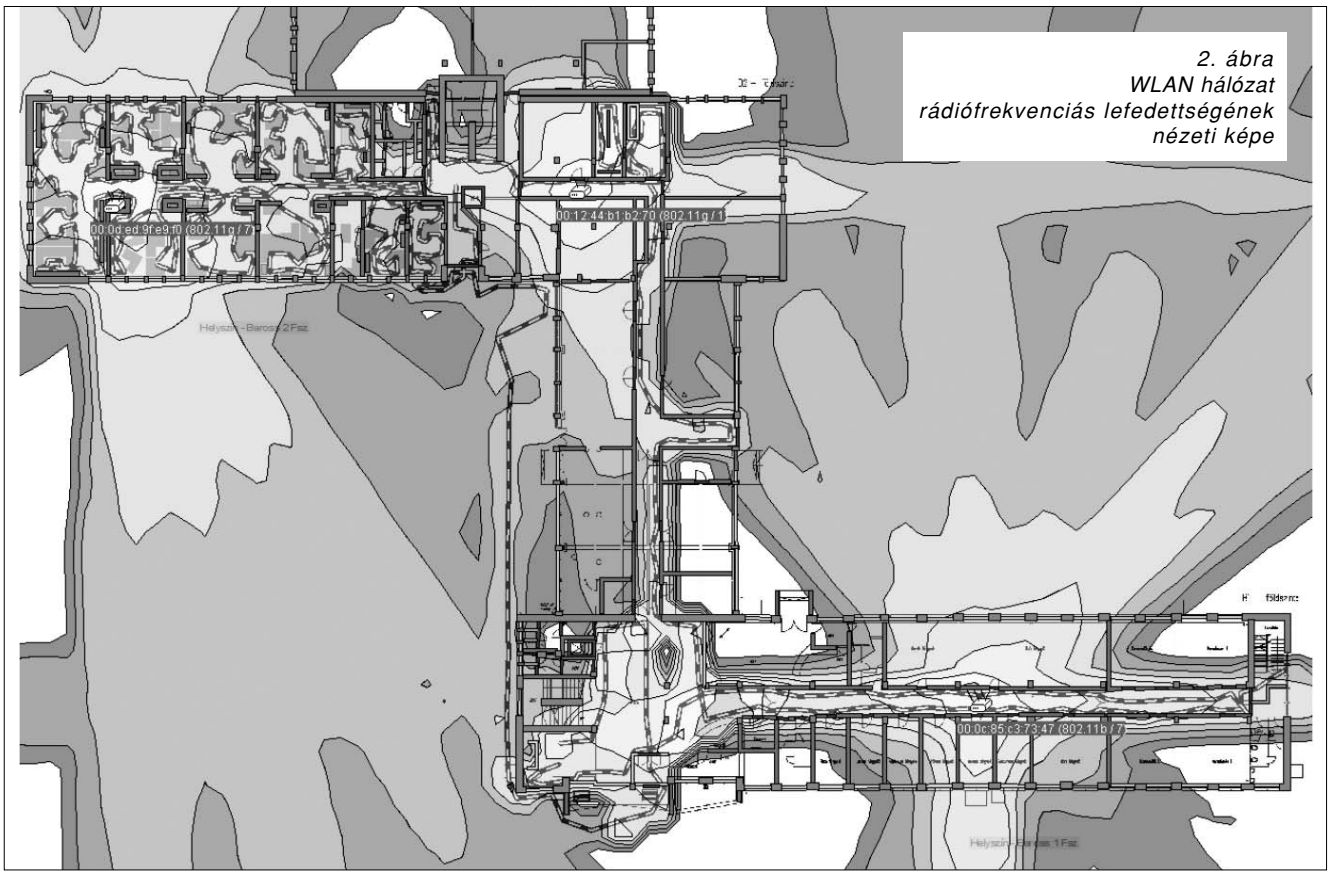
Sok esetben a ráfordítható idő rövidsége miatt, vagy az épület struktúráját figyelembe vevő egyszerűsíthetőség és következtethetőség feltétele miatt nem lehetséges, vagy nem szükséges elvégezni a teljes lefedettség alapterületére az aktív helyszíni felmérést. Ebben az esetben az ESS tervező modulja lehetőséget biztosít passzív Site Survey elvégzésére. Ekkor az ESS program szimulálja az építészeti falak csillapító és szóródó hatását és ennek megfelelően grafikusan jeleníti meg a felvételre került WLAN AP-k rádiófrekvenciás besugárzási jelszintjeit.

A különböző használandó WLAN alkalmazásoknak megfelelő rádiófrekvenciás jelszínt demodulációs értékei és az egy időben jelen lévő WLAN AP-k száma adják meg a tervező részére az alkalmazandó peremfeltételeket a Wi-Fi hozzáférési csomópontok elhelyezéséhez. Az AP-kat manuálisan a tervező helyezi el az alaprajzon, a program csak szimulálva jeleníti meg a várt lefedettség nagyságát grafikus értékét.

A *2. ábra* egy meglévő WLAN hálózat ismételt helyszíni felméréséről (re-site survey) szól. Az AP-k telepítése és üzembe helyezése a korábbi terveknek megfelelően megtörtént. Ezek után egy mérő WLAN kliens segítségével ellenőrizzük a valós környezetbe letelepített Wi-Fi hozzáférési hálózat rádiófrekvenciás lefedettség jelszínt és zajszint értékének nagyságát. Az ESS program grafikusan képes megjeleníteni ezen értékeken túl a tervezésnél felhasznált további származtatott értékeket, mint például a detektált interferenciás zavartatási jelszint, vagy az idegen WLAN hálózatok jelszintjeit, SNR, adatkapacitás értéke.

Az ESS v4.5 Prof. program segítségével lehetőség van többek között egy előre definiált peremfeltétel és követelményrendszer alapján történő grafikus megjelenítésre, ellenőrzésre, megfeleltetésre, mely a tervezést, vagy a mért eredmények kiértékelését megkönnyíti.

A „Live Network Status” elnevezésű táblán az ESS v4.x program megjeleníti a vizsgált helyszínen detektálható valamennyi Wi-Fi hálózat főbb rádiófrekvenciás paramétereit. Ezen a táblán a beállított és kiválasztott rádiófrekvenciás követelmények paraméterei és értékei is visszajelzésre kerülnek.



2. ábra
WLAN hálózat rádiófrekvenciás lefedettségének nézeti képe

A jelenlegi Wi-Fi alkalmazások gombamód-szerű terjedése elkerülhetetlenné teszi a WLAN hálózat RF-s tervezését, majd menedzselését. A professzionális, nagy kapacitású és valós idejű alkalmazások előtérbe kerülése egyenesen megköveteli a szakszerű vezeték nélküli rendszertervezés és dokumentálás tényszerűségét.

3. Biztonságos WiFi hálózat tervezése, megvalósítása és mérése

Egy korszerű, kiemelt biztonságú vezetéknélküli hálózat megvalósítását egy konkrét példán keresztül mutatjuk be. Egy üzleti titkokat is kezelő közintézmény WLAN hálózatának kialakításakor a legmagasabb biztonsági előírásoknak kellett megfelelni, amelyeket csak a legkorszerűbb, mindenre kiterjedő megoldásokkal lehet kielégíteni, ugyanakkor biztosítani kellett az intézményhez érkező kül- és belföldi partnerek, munkacsoportok munkatársai számára a nyilvános hálózat könnyű elérhetőségét.

3.1. A hálózattal szemben támasztott követelmények

A kiépítendő vezetéknélküli hálózat alapvető feladata, hogy megfelelő rádiófrekvenciás lefedettséget biztosítson az intézmény telephelyeinek meghatározott területein (elsősorban tárgyalók) a mobil kliensek számára. A mobil kliensek két csoportba sorolhatók, egyrészről külsős vendégek, másrészről intézményi dolgozók férhetnek a vezetéknélküli hálózathoz. A vezetéknélküli kliensek nem érhetik el az intézmény belső vezetékes hálózatát, a vendég felhasználók számára internet hozzáférést kell biztosítani, az intézményi felhasználók pedig a tűzfal külső lábát érhetik el, ezen keresztül IPSec VPN csatorna felépítésével juthatnak a belső hálózatra.

A kialakítandó vezetéknélküli hálózatnak csak mobil számítógépek adatátviteli forgalmát szükséges továbbítani a vezetékes hálózat felé, nem szükséges valós idejű végpontok forgalmának, mint például hang, vagy videó átvitelét az adat mellett biztosítania.

3.2. Specifikációk

A tervezés során elvárás volt, hogy a kialakítandó WLAN hozzáférési hálózati rendszer szabványos protokollokat és szabadon felhasználható frekvenciasávot, üzemi vivőfrekvenciát alkalmazzon az IP csomagok átviteléhez. A hozzáférési kapacitás és a végponti alkalmazások épületen belüli történő használata megengedett.

További követelmény, hogy a WLAN rendszer legyen alkalmas a jövőben bevezetésre kerülő szabványok támogatására és kezelésére, az elérési pontok (AP) száma szükség esetén, bővíthető legyen.

A kialakítandó WLAN hozzáférési rendszer a következő műszaki tulajdonságokkal rendelkezzen:

– *WLAN rendszer kialakítása:*

Egységesített, kontroller alapú, központi menedzselésű WLAN hozzáférési rendszer Access Point típusú hozzáférési csomópontokkal.

– *Antenna kiválasztása:*

Az AP-k rádiófrekvenciás kimenő pontjára külső antenna csatlakoztatható a megfelelő lefedettség kialakíthatósága érdekében.

– *Átviteli frekvenciatartomány:*

Jelenleg csak a 2,4 GHz az IEEE 802.11bg protokoll használatával.

Az 5 GHz az IEEE 802.11a protokoll használatával a jövőben kialakítható legyen.

– *Frekvenciaműködtetés normája:*

Európai, az NHH szabályozásnak megfelelően.

– *Megfelelőségi szabvány:*

CE tanúsítvány, Wi-Fi, WPA/WPA2, WMM minősítés.

– *Tervezett hozzáférési kapacitás:*

Maximum 54 Mbps kapacitás.

– *LAN interfész kapcsolódás:*

AP-k csatlakoztatáshoz 10/100 BaseT Tx, a központi vezérlő berendezés illesztéséhez pedig 1000BaseT Tx.

– *WLAN AP tápfeszültség ellátása:*

Inline Power Ethernet, vagy szabványos Power over Ethernet (802.3af).

– *WLAN Security:*

802.11i protokollnak megfelelő, Layer2 szintű biztonság, Korszerű idegen WLAN hálózat detektálási rendszer.

– *WLAN menedzselés módja:*

Biztonságos protokollon, egyszerű grafikus megjelenítési felülettel. A CLI egyidejű alkalmazás lehetőségét támogassa az üzemeltetés során.

3.3. WLAN rádiófrekvenciás lefedettség helyének meghatározása

A kialakítandó WLAN hozzáférési hálózat lefedettségének területei, terjedjen ki az intézmény budapesti és több vidéki irodájának tárgyaló és közvetlen környezetére.

3.4. Wi-Fi hálózati topológia

A mobil kliensek számára biztonságos, az intézmény hálózatától szeparált módon biztosít hozzáférést az IT erőforrásokhoz (Internet, intézményi VPN).

A *3. ábra* mutatja be az eszközök intézményi rendszerbe illesztését. A folyamatos vonal a vendég felhasználók hálózatát jelöli, a szaggatott a belső hálózatot. A „belső” forgalom a WPA2/AES biztonság mellett IPSec titkosítást is tartalmaz, a kliensek és a tűzfal között, a „vendég” forgalom WPA/TKIP titkosítással védett a kliensek és a kontroller között, a kontroller utáni forgalom nem titkosított.

3.5. WLAN végponti alkalmazások és szolgáltatások

A vezetéknélküli LAN hozzáférési rendszer végponti kliensei részére két csoportra oszthatók:

- Vendég felhasználók részére nyilvános Wi-Fi internet szolgáltatás, megfelelő biztonsági kontroll alkalmazásával.
- Az intézmény WLAN végponti kliensei részére az intézmény tűzfalán keresztül IPSec VPN csatorna kiépítésével a VPN szabályozásban meghatározott belső erőforrásokhoz való hozzáférés.

3.6. Az intézmény belső mobil számítógépei

Az intézmény belső vezetéknélküli felhasználóinak azonosítását meglévő, központi Steel Belted RADIUS szerver végzi. A Wi-Fi hálózathoz történő IP csatlakozást a kliens használati jogosultságának eldöntése – érvényes, az intézmény által kibocsátott X.509 tanúsítvány ellenőrzése – előzi meg. Amennyiben jogosult a belső WLAN hálózathoz történő csatlakozásra, úgy valós IP címet kap a vezeték nélküli kliens végpont hálózati csatoló kártyája.

A WLAN kliens végpont IP csatlakoztatásakor a következő feltételek biztosítása szükséges:

– Csak akkor induljon el a kapcsolódási folyamat, ha a mobil számítógép vezetékes LAN Ethernet csatlakoztatása megszűnik.
– A WLAN és az IP kapcsolat felépítése csak a mobil végponton előre beállított konfigurációnak megfelelő, valós WLAN hálózaton keresztül valósuljon meg.
– Amennyiben a mobil számítógép ismét a vezetékes LAN hálózathoz kapcsolódik, úgy a WLAN hálózati IP kapcsolata érvényét veszítse és a mobil PC végpont ismét csak a vezetékes IP címével működjön.
– Tegye lehetővé, hogy külső helyszíneken a Wi-Fi felhasználó által előre beállított, más Wi-Fi rendszerekhez is csatlakozhasson (ITU, CEPT stb. ülések).
– A mobil számítógépek forgalmazása csak a központ felé történjen.
– A File and print sharing protocol nem kerül továbbításra.

3.7. Vendég felhasználók mobil számítógépei

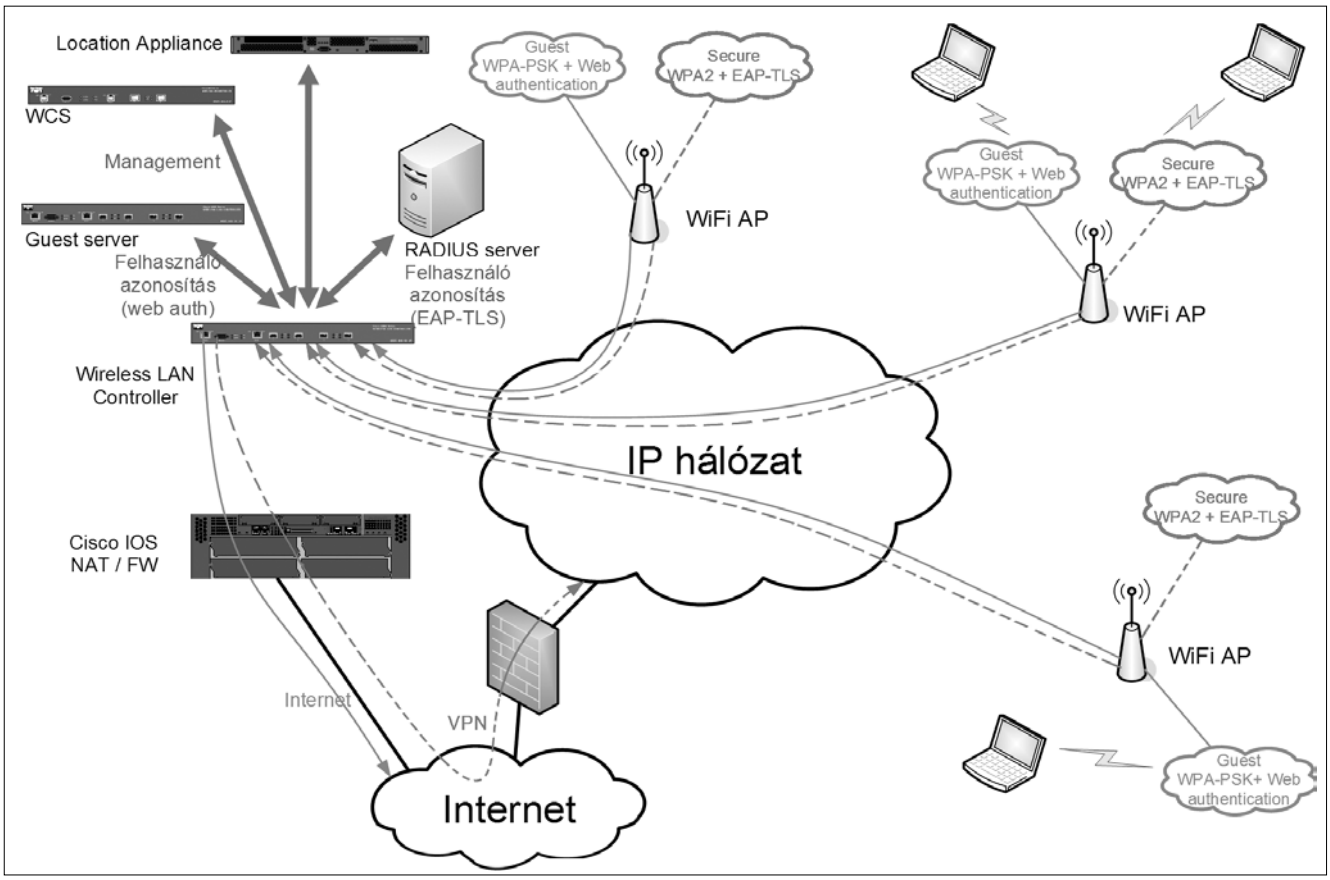
Az intézmény területén csatlakozni kívánó vendég felhasználók WLAN kliens végpontjai részére a következő szempontok valósuljanak meg:

– Megfelelő biztonságú (WPA, vagy WPA2 kulcsmenedzsment és TKIP, illetve AES titkosítás) Layer2 titkosítású adatkapcsolat.
– Kontrollált vezetéknélküli internetszolgáltatás kialakítása valósuljon meg. A vezetéknélküli kapcsolat időtartama és hozzáférési jogosultsága az intézmény részéről könnyen beállítható legyen.
– A vendég felhasználók Wi-Fi forgalma az intézmény belső hálózatától elkülönítve kerüljön átvitelre és a Wi-Fi kliensek hálózathoz történő csatlakoztatásánál szükséges a megbízható azonosítás és az időfelhasználási korlátozás kialakítása!

3.8. Általános biztonsági követelmények

A vezetéknélküli kliensek forgalmát az intézmény hálózatától teljesen elkülönítve kell kezelni, a vezetéknélküli kliensek az intézmény belső IT erőforrásait nem érhetik el (kizárólag a tűzfalon keresztül felépített IPSec VPN csatornán, amelynek használatához csak a belső felhasználók rendelkeznek megfelelő jogosultsággal)

2. ábra WLAN hálózat rádiófrekvenciás lefedettségének nézeti képe



3.9. Általános WLAN Security követelmények

A belső, vezetékes LAN hálózaton szereplő adatok biztonsága érdekében a kialakítandó WLAN hozzáférési hálózat támogassa az IEEE 802.1x port szintű azonosítási protokollt, Layer2 szinten az IEEE802.11i szabványajánlásnak megfelelően.

A vezetéknélküli végponti kliens felhasználók azonosítása szabványos szerver alapú azonosítás alapján valósuljon meg, mely az intézmény belső biztonsági szabályozásával összhangban kerüljön kialakításra.

Az AP-k és a WLAN kontroller közötti kapcsolat kialakítása biztonságos protokoll alkalmazásával valósuljon meg. A WLAN hozzáférési rendszer csomópontjai számára csak azonosított AP csatlakoztatását tegye lehetővé.

Biztosítson idegen WLAN hálózat detektálás megjelenítésének lehetőségét, mind infrastruktúra-alapú, mind ad-hoc hálózati architektúra esetében.

A rádiófrekvenciás média-titkosításához WPA-TKIP vagy WPA2-AES kulcsmenedzsment-titkosítás párosítás használatával biztosítson a végponti kliens tudásának megfelelően lehetőséget a csatlakoztatásra.

4. A WLAN hálózat részletes ismertetése

A vezetéknélküli LAN-ok rendszertechnikája az elmúlt években nagyon sokat változott. A technika népszerűségének növekedése a skálázhatóság növelésének folyamatos igényét tartja életben. A jelenleg legkorszerűbb a Cisco controller-alapú rendszertechnikája, amely a rádiós AP-k vezérlését a vezetékes hálózaton intelligens célberendezésekre, úgynevezett WLAN Controllerekre (WLC) bízza, a WLC-ket pedig a Wireless Control System menedzsment szoftveren keresztül tudjuk kézben tartani. Az intézmény számára ezen az architektúrán alapuló rendszert terveztünk, amelyet kiegészítünk egyéb szolgáltatásokkal is (Location Based Services, Guest Services); ennek részletes eszközeit és rendszertervét ismertetjük a továbbiakban.

4.1. LAP-ok (Ligtweight Access Point)

Olyan mikrohullámú berendezések, amelyek biztosítják a rádiós közeget és annak csatlakozását a vezetékes közeghez. Tápellátásuk az intézménynél power injectorokkal történik, a szabványos PoE (IEEE 802.3af) technikával. A LAP-ok az architektúra triviálisan szükséges elemei. Az LAP-k nem, vagy legalábbis korlátozott funkcionalitással működhetnek (REAP vagy H-REAP üzemmódban) a WLC vezérlése nélkül.

4.2. WLAN controllerek (WLC)

A WLC Controller-ek olyan vezetékes eszközök, melyek az AP-k vezérlését látják el. Az AP-k a Ligtweight Access Point Protocol-lal (LWAPP) kommunikálnak azzal a WLC-vel, amelyhez ugyanezen a protokollon regisztráltak. Az LWAPP egy szabványos, IP alapú tunnel protokoll, amely az AP-k és a WLC között épül ki, az UDP szolgáltatásait használja és a teljes rádiós 802.11 keretet tartalmazza. (Az LWAPP-nek van L2 üzemmódja, amely választható a WLC-kben is, de skálázhatósági korlátai miatt nem javallott.) Az LWAPP két alapvető szolgáltatása az AP vezérlés, és a felhasználói forgalom szállítása.

A vezérlés X.509 certificate alapú, AES algoritmussal titkosított csatornán zajlik, míg a felhasználói forgalom számára az LWAPP a tunnelezésen kívül nem biztosít semmilyen titkosítási szolgáltatást. Ennek oka, hogy a teljes 802.11 keretet becsomagolja, így az alkalmazott rádiós hálózati biztonság (WPA+TKIP, WPA2+AES) a LAP-tól WLC-ig változatlanul érvényesül a vezetékes hálózaton.

4.3. Wireless Control System (WCS)

A Cisco menedzsment szoftvere, amelyen keresztül a WLC-k és AP-k összefogását és kezelését egy vezérlőpultról végezhetjük. Az architektúrának nem alapvető eleme, de kiterjedtebb hálózat (több WLC) és egyéb szolgáltatások igénye (például location-based services) esetén szükséges.

4.4. Location Appliance

Opcionális elem, amely a WCS-sel és az architektúra többi elemével együttműködve elhelyezkedésre vonatkozó szolgáltatásokat nyújt (például meg tudja jeleníteni egy felhasználói gép, Wi-Fi telefon vagy RFID (rádiófrekvenciás azonosító) címkével ellátott tárgy elhelyezkedését az épület térképén). Rack-be szerelhető appliance (szoftver+hardver együtt) kiépítésű, amely a WCS nélkül nem működőképes.

4.5. NAC Guest Server

Opcionális elem, amely a vendég felhasználók adminisztrációját könnyíti meg: a vendég felhasználó felvételét, ideiglenes accountjának nyomtatását, mailben vagy SMS-ben történő elküldését, a használat időkorlátját és a felhasználó azonnali letiltását, valamint vendéglisták készítését teszi lehetővé. Természetesen regisztrálja a felhasználói aktivitást, a be- és kijelentkezés idejét valamint a kliens IP címét. A NAC Guest Server valójában egy speciális AAA szerver, amely RADIUS protokollon szolgálja ki klienseit: a WLC-ket.

4.6. Cisco Secure Services Client (CSSC)

A kliens gépeken futó program, amely csak a kijelölt biztonsági elvek szerint enged csatlakozni a konfigurált vezetékes és vezetéknélküli hálózatokhoz. Az intézménynél érvényben levő szigorú biztonsági szabályozás érvényesítése érdekében a vezetéknélküli szolgáltatást is használni jogosult felhasználók gépére telepíteni kell.

4.7. Az elemek együttműködése

A rendszer központi eleme a kontroller, minden kommunikáció, ellenőrzés és irányítás ezen keresztül történik. A kontroller és a kihelyezett AP-k a WLAN biztonság kialakítási folyamatában fontos (authenticator) helyet foglalnak el. A belső WLAN kliensek azonosítását IEEE 802.1x protokollnak megfelelően meglévő, Steel Belted RADIUS Server-pár biztosítja. A WLC szabványos RA-

DIUS protokollon keresztül kommunikál az azonosítási szerverrel. A vendég Wi-Fi felhasználók azonosítását a NAC Guest server RADIUS szervere biztosítja. A kontrolleren minden WLAN hálózathoz (SSID-hez) külön RADIUS szervereket állítottunk be.

4.8. Eszközkonfiguráció-hozzáférés

A WLAN hozzáférési hálózat konfigurációs állományát a központi kontroller tartalmazza. A berendezés beállításának hozzáféréséhez jelenleg három felhasználónév és jelszó páros került kialakításra.

4.9. Az átvitt forgalom biztonsága

A rádiós forgalom titkosítását a WLC kontroller konfigurációja és a távoli AP-k biztosítják. A hálózatot azonosító SSID-k nincsenek nyilvánosan megosztva a 802.11 Ethernet keretben (No broadcast). Vagyis nem jelennek meg automatikusan a Microsoft Windows operációs rendszerével elérhető hálózatok között egy olyan felhasználó gépén, amelyen az adott SSID-t tartalmazó profile nem ismert. A kapcsolat kialakítása előtt ezen azonosítót mindig szükséges megadni!

A kialakított WLAN hálózatok eltérő biztonságot alkalmaznak a felhasználóik részére:

• A vendég vezetéknélküli LAN felhasználók Internet hozzáférése védett, mind a rádiófrekvenciás média Layer2 titkosítása, mind a forgalom jogosultsága szempontjából. Jelenleg a rádiófrekvenciás forgalmat előre definiált WPA kulccsal és TKIP titkosítással láttuk el. A WLAN kapcsolat kialakítása után az Internet forgalom hozzáféréséhez szükséges egy időkorlátos felhasználó név és jelszó, melyet korábban a NAC Guest szerverrel szükséges generálni a vendég felhasználók részére.

• A belső Wi-Fi felhasználók WPA2 kulcs menedzsment és AES titkosítás kódolási algoritmussal és meglévő digitális tanúsítvány hitelesítése után csatlakozhatnak a hálózathoz. A belső vezetéknélküli LAN kliensek hitelesítéséhez 802.1x szerver alapú, EAP-TLS módozatú megoldás használatos, meglévő PKI infrastruktúrával. A kliens oldalon CSSC felhasználói program v5.1 verziójának előre kialakított konfigurációja alapján gondoskodik az intézmény belső Wi-Fi végpontok kapcsolatának további biztonságáról, mind a vezetékes LAN, mind a WLAN kapcsolódásakor. Amennyiben az intézmény belső mobil kliens végponti PC-je a vezetékes LAN hálózathoz kapcsolódik, úgy a CSSC program gondoskodik a WLAN kapcsolat (IP és rádiófrekvenciás) megszüntetéséről. Ha a mobil végpont megszakítja a vezetékes Ethernet kapcsolatát, úgy a CSSC program átvált a Wi-Fi rádiófrekvenciás IP kapcsolatra. A biztonsági funkció kiszolgálásához minden egyes belső WLAN mobil számítógépre szükséges telepíteni a CSSC felhasználói programot.

4.10. WLAN felhasználói csoportok biztonsági beállítása

Az intézmény WLAN hozzáférési hálózati rendszerében a csatlakozni kívánó Wi-Fi felhasználók elkülönítetten, megfelelő azonosítás után kapcsolódhatnak. A megfelelő IP csatlakoztatással rendelkező kliens végpontok hálózati környezetüktől függően a következő jogosultsággal és szolgáltatási igénnyel rendelkezhetnek:

– A belső WLAN felhasználók teljes jogosultsággal rendelkeznek és érhetik el a vezetékes LAN hálózat erőforrásait.
– A vendég Wi-Fi felhasználók az intézmény belső hálózatát nem érhetik el. Csak nyilvános internet hozzáféréssel és szolgáltatással rendelkezhetnek.

4.11. WLAN Menedzsment

Az intézmény WLAN hozzáférési hálózat eszközeinek felügyelet-menedzselése a következőképpen valósul meg:

• A LWAP és a WLC4404 kontroller ugyanazon hálózatba (VLAN=2), a valós forgalomtól történő elkülönítéssel menedzselhető.

• A WLC4404 kontrollert egy erre a célra adott IP címen akár grafikusan, akár CLI felületen menedzseljük.

• A LWAP menedzselését a WLC4404 kontroller megadott IP címtől kezdődően, az „ap-manager” nevű interfész felületén keresztül biztosítja.

• A menedzsment funkciók grafikus megjelenítése és ellátása érdekében WCS (v5.0.148) hálózat felügyeleti szerver szoftver került telepítésre az erre a célra adott IP címen. A WLC-től érkező információkat a WCS SNMP-n keresztül kérdezi le.

• Biztonságos, tanúsítvány alapú https (SSH) protokoll került kialakításra.

• A kontroller CLI konfigurációja közvetlenül a soros portjáról is ellenőrizhető és módosítható (9600Bps Baud Rate, 8bits, Flow Control tiltva, Stop Bits:1, Paritás nélkül).

• WLAN-n keresztül a menedzselés tiltva van.

5. Összefoglalás

A fentiek alapján elmondhatjuk, hogy egy közintézmény megfelelően védett, ugyanakkor széles kör számára szolgáltatásokat nyújtó Wi-Fi hálózatában szinte minden ma elérhető technikai és biztonsági megoldásra szükség volt. A vezetékes hálózattól elválasztott, központi kapcsolású adatforgalom, WPA és WPA2 titkosítás, tanúsítvány alapú felhasználó azonosítás, ideiglenes felhasználók kezelése és ellenőrzése, terület alapú szolgáltatások, idegen kliensek és hálózatok felderítése, központi grafikus adminisztráció... A végeredmény egy minden igényt kielégítő, biztonságos, jól adminisztrálható és ellenőrizhető Wi-Fi rendszer.

A szerzőkről

RÉTI ZOLTÁN 1968-ban született Mohácson. 1992-ben diplomázott a BME Villamosmérnöki Karán. 1992-től számítógépes hálózatok tervezésével és megvalósításával (LAN, WAN) valamint hálózatmenedzsmenttel, IP telefóniával és VPN hálózatokkal foglalkozik. Több országos rendszer tervezésében és megvalósításában vett részt. Jelenleg technikai tanácsadóként dolgozik a Synergon Informatika Nyrt. Infrastruktúra divízió Hálózati kommunikációs üzletágában.

CZUCZ DÁVID 1962-ben született Budapesten. 1985-ben diplomázott a Kandó Kálmán Villamos Ipari Műszaki Főiskolán, majd 1993-ban szerzett szaküzemmérnöki másoddiplomát Mikrohullámú PCM hírközlés szakon. Jelenleg technikai tanácsadóként dolgozik a Synergon Infrastruktúra divízió Hálózati kommunikációs üzletágában. Fő területe a vezetéknélküli hozzáférési hálózati rendszerek. 2006 óta CAWLANFS minősítésű vizsgával rendelkezik.

Mérésinformatikai fejlesztés az NHH-ban

GÁSPÁR ERNŐ
NHH Mérésügyi Igazgatóság
gaspar.erno@nhh.hu

ZIMMER ANDRÁS
Kryonet Magyarország Kft.
andras.zimmer@kryonet.hu

Kulcsszavak: mérésügy, NHH, mérésinformatika

A szerzők bemutatják a Nemzeti Hírközlési Hatóság mérésügyi feladataival kapcsolatos kihívásokat, kontextusba helyezve azokat a komplex informatikai rendszereket, amelyek a terület eredményes és hatékony munkáját támogatják. Áttekintő képet adnak a jelenlegi helyzetről, a most futó és tervezett fejlesztésekről és arról, hogy a várható eredmények hogyan tudják alátámasztani a beruházást.

1. Bevezetés

A korszerű szabályozó és piacfelügyeleti munkát végző hírközlési hatóságok számára a valóságadatok ismerete elengedhetetlen. Műszaki területen ez egyrészt a spektrumhasználatra vonatkozik, másrészt a szolgáltatók által használt és a kereskedelemi forgalomba kerülő elektronikus berendezések műszaki paramétereinek ismeretét igényli.

A szükséges adatok biztosításának egyik, általánosan alkalmazott módja a szolgáltatók, gyártók, termékek tanúsítása. Ez azonban önmagában nem képes kielégíteni a felmerülő igényeket.

Egyrészt azért nem, mert a spektrumhasználat ellenőrzésével, frekvenciagazdálkodással, új szolgáltatások bevezetésével kapcsolatos mérések végrehajtása nemzetközi egyezményekben és törvényekben rögzített állami feladat, melyekre a világon mindenhol hatósági jogosítványokkal bíró mérőszolgálatot tartanak fent. Általában a szükséges adatok máshonnan, mint egy ilyen mérőszolgálattól be sem szerezhetők, hiszen országonként egynél több azonos profilú spektrumellenőrző szolgálat üzemeltetése gazdaságtalan lenne.

A szolgáltatások és berendezések vonatkozásában a méréssel történő ellenőrzések fontosságára utal, hogy bár a hatósághoz benyújtott gyártói és szolgáltatói tanúsítványok túlnyomó többsége értelemszerűen a termék vagy szolgáltatás megfelelőségéről nyilatkozik, ez nem a valóság pontos képe. Európai statisztikai összegzések szerint a kereskedelmi forgalomba kerülő hírközlési berendezéseken végzett piacfelügyeleti ellenőrző mérések igen magas, a tanúsítványok ellenére közel 50%-os nem megfelelőséget mutattak bizonyos kategóriákban. A helyzet hazánkban is ehhez az átlaghoz közelít.

A Nemzeti Hírközlési Hatóság (NHH) Mérésügyi Igazgatóságának mérési feladatai is a fenti két nagy témakörbe csoportosulnak.

A jelenleg használt mérésinformatika folyamatosan fejlődött és fejlődik, a mérőszolgálattal szembeni követelmények, a mérőeszközök fejlődése és az elérhető informatikai lehetőségek által meghatározott keretek között. Ha ez az organikus fejlődés megfelelően történt az elmúlt években, miért szükséges áttekinteni és átalakítani a terület informatikai eszközeit? Miért fogalmazódik meg az „egységes” mérésinformatika gondolata és igénye? És miért pont most?

A mérőszolgálat működését meghatározó külső-belső igények, a működés jellemző sajátosságai, a külső informatikai környezet fejlődése és még számos tényező mind egy irányba mutat, az önmagukban jól működő mérésinformatikai rendszereknek olyan rendszerré kell összeállni, ahol a rendszer működése képes új „minőséget” produkálni. Az egységbe szervezett rendszer által szolgáltatott plusz persze nem független az alkotó elemektől, de az új minőséget az integrációs mechanizmusok nyújtják. Ezt az új minőséget pedig csak az összehangolt működés tudja produkálni.

A mérésügyi területtel kapcsolatos elvárások nagyobb hatékonyságot, eredményességet, aktivitást, cselekvőképességet és gyorsabb reagálást követelnek, míg a rendszereket üzemeltetők egyre több információt kérnek, látni szeretnék munkájuk értelmét, hasznát és eredményességét. A jelenleginél nagyobb hatékonyság igénye azonban már csak korlátozottan elégíthető ki a rendszerek önmagukban történő fejlesztésével. Nagyobb és látványosabb eredményt biztosít az egységes rendszer kialakítása.

2. Az ellátott mérési feladatok típusai

Az NHH Mérésügyi Igazgatósága meglehetősen sok különféle mérési feladatot végez el az igények függvényében kisebb-nagyobb rendszerességgel. A feladatokat sok szempontból lehet csoportosítani, például célok, igénylők, eszközök, erőforrásigény, rendszeresség stb. szerint.

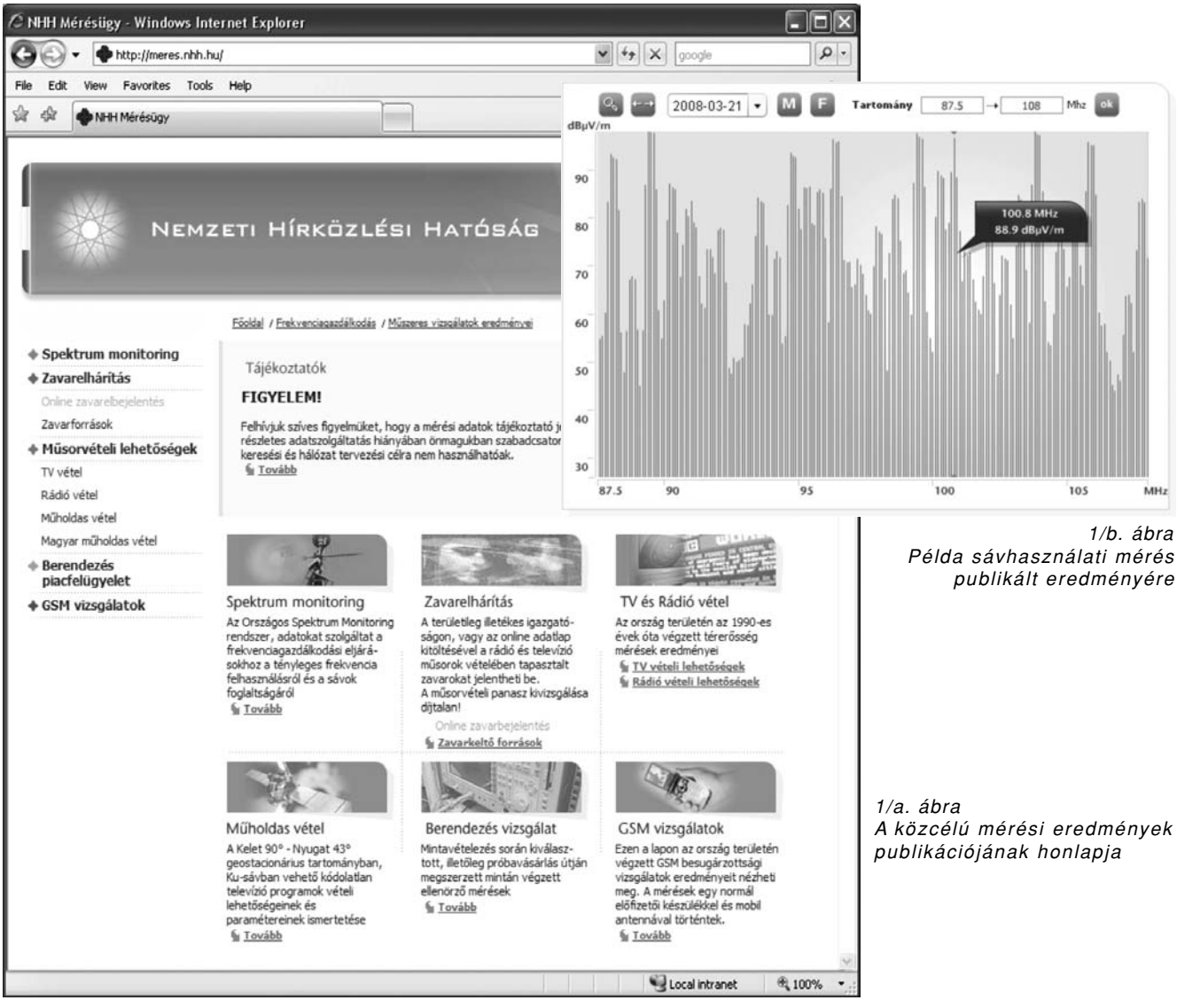
A célok szerinti például az alábbi fő csoportokba lehet sorolni a méréseket:

1. *Berendezésmérések*
   a. piacfelügyeleti mérések
   b. kalibrációk
2. *Spektrumhasználati mérések*
   a. általános spektrumhasználati mérések (engedélyköteles és nem egyedi engedélyköteles sávokban egyaránt)
   b. rádióengedélynek való megfelelőség ellenőrzése
   c. engedély nélkül üzemelő adóberendezések felderítése
   d. elektromágneses sugárterhelés („elektroszmog") mérések
3. *Műsorvételi lehetőségek*
   a. Televíziós adások vételi lehetőségei (analóg és digitális)
   b. Rádióadások vételi lehetőségei (analóg és digitális)
   c. Műholdas sugárzás vételi lehetőségei
4. *GSM mérések*
   a. ellátottságmérések
   b. szolgáltatásminőségi paraméterek mérései
5. *Zavarvizsgálatok*

A mérési feladatok egyik célja és eredménye a közcélú publikáció. Ezeket a Mérésügyi Igazgatóság az NHH közcélú mérési eredményeit bemutató WEB oldalán teszi közzé (*http://meres.nhh.hu/*, ami elérhető az NHH központi honlapjáról – *http://www.nhh.hu* – is). Az oldalak tartalma folyamatosan bővül; nem kis részben az új informatikai fejlesztések révén rövidesen kiterjesztésre kerül a megjelenített információk mennyisége és tematikája is (például életvédelmi sugárzási határértékek teljesülése).

3. Mérőeszközeink és -rendszereink

A mérőszolgálat kiterjedt feladatainak ellátására használ egyedi mérőberendezéseket is, de a mérések legnagyobb részét már hosszabb ideje a mérőrendszerekkel történő mérések adják. Az általunk használt mérőeszközök részben fixen telepített mérőállomásokból, részben pedig mobil egységekből állnak. A mobil egységek feladattól függően, önállóan vagy a fixen telepített rendszerekkel szoros együttműködésben végzik feladataikat.



1/b. ábra
Példa sávhasználati mérés publikált eredményére

1/a. ábra
A közcélú mérési eredmények publikációjának honlapja

A korszerű műszerek – felhasználási területtől függetlenül – összetett feldolgozó algoritmusokat tartalmazó informatikai eszközök. A műszerek manuális kezelése interaktív program futtatásával valósul meg. A hírközlésben ellenőrzésre használt eszközöknek sokfajta szolgáltatás és berendezés vizsgálatára kell alkalmasnak lenniük, ezek ritkán egyedi műszerek, majdnem mindig komplett távvezérelt mérőrendszerek. A hatékony ellenőrzés minden felhasználási területen megkövetel egy minimális, a reprezentativitáshoz szükséges mintaszámot, amelyet hatékonyan csak automatizálással lehet biztosítani. A viszonyokat a *2. ábra* szemlélteti.

Az előállítható és feldolgozható adatmennyiség az egyes kategóriákban több nagyságrendet nőhet, cserébe a rendszer növekvő összetettségével kell számolni. Azt hogy a növekvő összetettség mit jelent, a *3. ábra* illusztrálja.

3.1. A meglévő méréstechnikai informatikai rendszerek struktúrája

A 3. ábrán összefoglalóan látszik, hogy a mérőszolgálat kb. 30 mérőállomása, illetve a kapcsolódó egyéb rendszerek milyen sokszintű rendszerbe szerveződnek – és itt még el is tekintettünk az egyes rétegelemek belső bonyolultságától (nem ábrázoltuk a mérőállomások belső szerkezetét, sem az amúgy önmagukban is nagyon összetett egységes kezelést lehetővé tevő szintek informatikai rendszereinek részleteit).

Az ábra alsó rétege a mérőállomások rendszere, melyeket az adott állomáson domináns műszergyártónak megfelelő helyi mérésvezérlő program vezérel. Az azonos típusba tartozó állomások képesek egyetlen egységként illetve állomásonként is feladatot fogadni. Az állomások részhalmazainak önálló működését központi mérésvezérlők irányítják. A rendszerbe kapcsolódó mobil állomások offline és online üzemmódban, a fix állomások online üzemmódban működnek. Az egyes állomások ütemezett automatikus, riasztásra történő automatikus, operátori manuális, távoli felhasználó által kezdeményezett méréseket párhuzamosan végeznek.

A mérő és feldolgozó képesség, valamint informatikai infrastruktúra és architektúra tekintetében inhomogén rendszereket egy absztrakciós réteg „fedi el”. Ez lehetővé teszi, hogy az üzleti logika mérésvezérlési parancsai és a visszaérkező mérési eredmények a központi feldolgozásban egységes formát mutassanak. Így az üzleti logika (és így a feladatkiadás-feldolgozás) szempontjából közömbös a mérést végrehajtó rendszer felépítése, konkrét műszertartalma. Minden, az adott feladat végrehajtására képes rendszer számára azonos formátumú utasítás szükséges és azonos formátumú a visszaküldött válasz. Ha az állomások felépítése változik, más gyártó műszerei kerülnek bevezetésre, frissítésre kerül az állomások mérésvezérlő programja, csak az absztrakciós réteg ehhez tartozó elemét kell változtatni a működés megőrzéséhez.

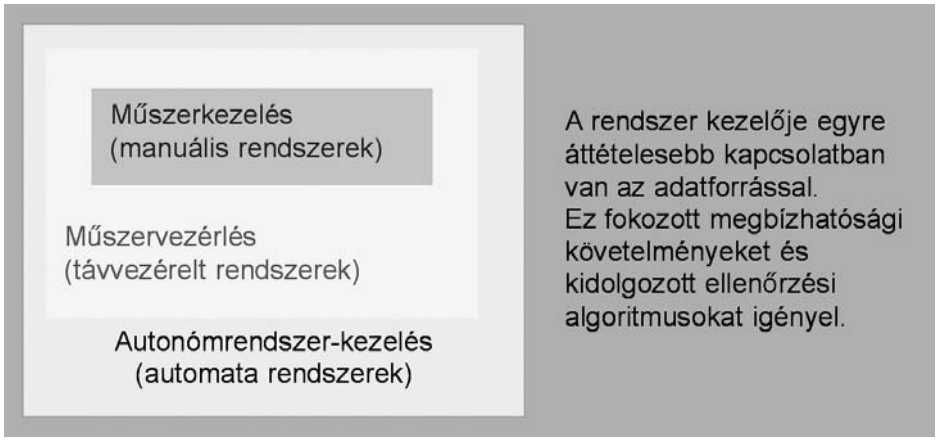
Az absztrakciós réteg fölé a közel azonos mérési képességeket összefogó funkciócsoport került. Ez az, amin keresztül az operátorok (és más rendszerek) elérik és kezelik a mérőrendszereket és ami egységesen tárolja a mérési feladatokat és eredményeket. Ez a rendszer felügyeli a mérési feladatok ütközésének elkerülését, illetve a megfelelő időrések lefoglalását-felszabadítását, a prioritásos feladatrangsor kezelését, ez a feladatok átütemezését szolgáló egység tehát a logikai erőforrás gazdálkodó. Ugyancsak ez a rendszer biztosítja a külső kapcsolódási pontokat (külső adatokhoz hozzáférés, külsős szereplők hozzáférése a rendszerhez).

Azonban részben gyakorlati, részben műszaki okokból nem minden mérőrendszer kezelhető ilyen módon. (Vannak például olyan mérőrendszerek, amelyekkel csak off-line adatcsere oldható meg.)

Az ilyen rendszerek esetében

– vagy központi adatkezelést és -tárolást valósítunk meg (vagyis a rendszert vezérelni ugyan nem, vagy legalábbis nem közvetlenül tudjuk, de központilag és egységesen tároljuk a mérési eredményeket és lehetőség szerint az őket létrehozó feladat fontos paramétereit is);
– vagy funkcionálisan csatoljuk őket (bár adott esetben veszünk át és adunk át adatokat, sokkal inkább „szolgáltatásként” tekintünk rájuk, mint „adat-generátorként”). Ez az eset jobban hasonlít a közel azonos mérési képességek összefogására, azzal a különbséggel, hogy itt egyetlen rendszert „fogunk össze”.

2. ábra A manuális kezeléstől az automata rendszerekig



4. Fejlesztések

4.1. A jelenlegi helyzet kialakulása

Természetes, hogy egy ekkora rendszert nem lehet (és a gyakorlatban nem is célszerű) egyetlen lépésben létrehozni; ehhez a szükséges anyagi, emberi és szakmai erőforrások nem állnak rendelkezésre. Ezt is szem előtt tartva az elmúlt években a mérőszolgálat folyamatosan

fejlesztette rendszereit. Általános elvként követtük, hogy a fenti sémának megfelelően alulról felfelé építkezünk. Ezzel párhuzamosan természetesen horizontálisan is folyamatosan bővítjük eszközkészletünket, egyrészt a megjelenő újabb és újabb feladattípusoknak megfelelően, másrészt pedig a minél jobb területi és szakmai lefedettség és a gyorsabb reakcióképesség érdekében.

A rendszerfejlesztés vertikális elveit azonban nem lehetett steril, tankönyvi módon alkalmazni; minden lépésben a gyakorlathoz és egyéb külső elvárásokhoz is igazodni kellett (és kell ma is). A gyakorlatban ez azt jelentette, hogy egyfelől bizonyos fejlesztési lépcsőket nem lehetett horizontálisan teljes szélességében egyszerre kiépíteni, másfelől egyes esetekben ki kellett építeni olyan átmeneti vertikális funkciókat, amiket a későbbi fejlesztések kiváltottak.

Az utóbbira példa a közcélú publikáció megvalósítása, ami már jóval a jelenleg kialakítás alatt lévő Egységes Mérőszolgálati Információs Rendszer elkészülte előtt (sőt, részben az egységes adatkezelési réteg teljes kiépítése előtt) elkezdett éles üzemben működni. Ilyen esetekben mindig egyensúlyt kellett találni az igények, a megvalósított funkciók „gazdagsága”, az átmeneti üzemeltetés többlet erőforrás ráfordítása, a (később „kidobandó”) fejlesztés költségei, a várhatóan szerezhető tapasztalatok és egyéb tényezők között.

4.2. Jelenlegi fejlesztések és a közeljövő tervei

Most jutottunk el arra a pontra, amikor a meglévő informatikai rendszerek integrációját több kényszerítő körülmény is sürgeti. A hatóság teljes informatikai rendszeréhez illeszkedés (ügyvitel, WEB-es publikációk, más szakmai rendszerek), az adatfelhasználók növekvő igényeinek teljesítése (hatóságon belüli, tárhatósági, társigazgatási), a nagymértékben automatizált több rendszert is érintő folyamatok nyomon követhetősége egyaránt az egységesítés irányába mutat. A mérőrendszerek belső organikus fejlődése is elérte azt a szintet, ahol az egységesítés hiányában a rendszerek nem menedzselhetőek (törzsadatbázisok menedzsmentje, folyamatintegráció, dokumentumkezelés-tárolás stb.).

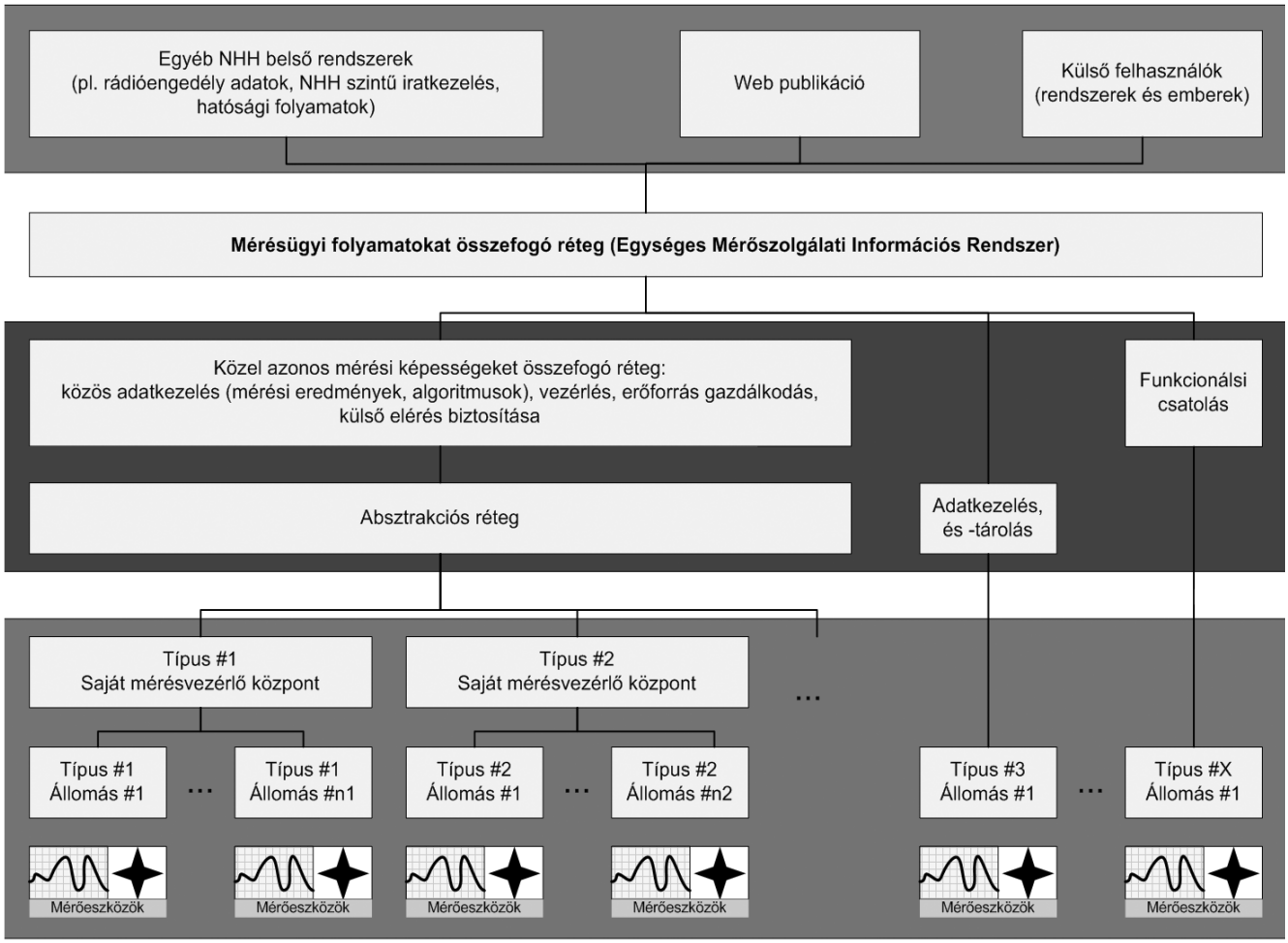
Ezért jelenleg a fejlesztés fő csapásiránya a mérésügyi folyamatokat és a hozzájuk tartozó információkat összefogó, úgynevezett EMIR réteg kialakítása.

A 2008 januárjában indult projekt első félévében végzett elemző-tervező munka eredményeként a projekt megvalósítása három ütemre bomlott.

Az első ütemben a kialakítandó EMIR réteg legfontosabb szerkezeti elemei valósulnak meg:

• Elkészül az EMIR logikai-funkcionális váza, a törzsadatbázisok nagyobbik hányada, a dokumentumtár és a legfontosabb mérőrendszerek felé csatlakozó interfészek.

3. ábra A mérőszolgálat rendszertechnikai felépítése



• Megindul a mérési eredmények webes publikációinak átalakítása: az eddigi „átmeneti” rendszert és mechanizmusok felváltja az NHH belső szabványos publikációs rendnek megfelel megoldás, bővítésre kerül az adatbázisokból történő automatikus publikáció rendszere és megjelennek új témák is.

• Ugyancsak az első ütemben elkészül a berendezés piacfelügyeleti méréseket és ügyviteli folyamatait támogató rendszer és ennek egyszerűsített iratkezelési integrációja. Szintén megvalósul az adóengedélyek engedélyezési adatbázisból történő átvétele.

• Emellett a mérésvezérlő rendszerek szintjén is kell fejlesztéseket végezni, elsősorban az azonos absztrakciós és funkcionális szintre hozás területén. Továbbá – a szélessávú mobilkommunikáció lehetőségének kihasználásával – megindul a mobil mérőrendszerek hatékonyabb integrációja. Integráljuk a „spektrum szmog” monitoring rendszer informatikai hátterét a teljes mérőszolgálati rendszerbe.

Az első ütem fejlesztéseit 2009 első negyedévében, fokozatosan állítjuk éles üzembe.

Az ezt követő második ütem legfontosabb feladata a folyamatkezelés és a strukturált dokumentumok használatának bevezetése. Eredményeként a rendszer biztosítja az automatikus mérési tevékenységet kiszolgáló automatikus feldolgozási és folyamatkezelési funkciókat:

– megvalósul a személyi és vezetői feladatkövetés;
– bevezetésre kerül a rendszer által kezelt munkakosár a tervek, heti jelentések, beszámolók, feladatok, és mérési eredmények automatikus kölcsönös egymáshoz rendelése;
– kialakul a teljes ügyviteli integráció és az elektronikus ügykezelés;
– megvalósul a külsős munkavégzések elektronikus feladatkiadás-teljesítményigazolás teljes rendszere;
– integrálódik a gépkocsi nyomkövető rendszer és az elektronikus menetlevél-vezetés alkalmazásba vétele;
– a folyamatkezelés és a strukturált dokumentumok használatba vételének lehetőségeit kihasználva továbbfejlesztésre kerülnek az első ütem moduljainak szolgáltatásai (mérési eredmények újrahasznosítása, mérési riasztást kezelő rendszer kialakítása.)

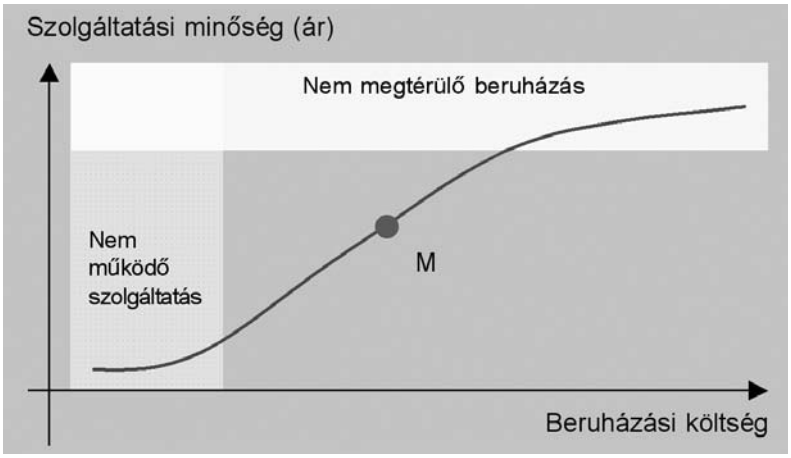
Ezen túlmenően befejeződik a webes publikáció teljes átalakítása.

A második ütem várhatóan 2009 végére lesz lezárható, jelenleg az előkészítése zajlik.

A harmadik ütembe azok a feladatok kerültek, melyek jelentős belső előkészítő munkát igényelnek: részben az NHH egyéb rendszereinek képességeit, részben a teljes szervezet folyamatait, részben pedig a mérésügy belső munkáját (például módszertanok) és rendszereit (például mérőrendszerek) érintik olyan mértékben, hogy kialakításuk leghamarabb középtávon 2-5 éves időtávon elképzelhető. Ebben a csoportban tervezzük elkészíteni a következőket:

– funkcionális rendszerintegráció a mérőrendszerekkel (nem csak adatexport-import, hanem valódi szolgáltatások biztosítása egymás számára),
– SAP integráció (eszközgazdálkodás, teljesítésigazolás stb.),
– funkcionális integráció a frekvenciagazdálkodási rendszerrel (nem csak adatcsere, hanem a két rendszer képes legyen egymás funkcionalitását szükség szerint közvetlenül használni),
– teljeskörű integráció egyéb NHH rendszerekkel (külső szereplők részére biztosítható mérési képesség elérés, közös partnertörzs, teljes integráció a hatósági folyamatrendszerbe stb.)
– adatelérési szolgáltatások biztosítása külső-belső adatfelhasználók részére (megfelelően biztonságos internet elérésen keresztül), valamint
– a nagytömegű, nagy mennyiségű mérési eredmény feldolgozására szolgáló adatbányászati technológiák beépítése.

Ezek mellett természetesen tervezzük az első két ütemben megvalósított rendszer tapasztalatok alapján történő továbbfejlesztését is.



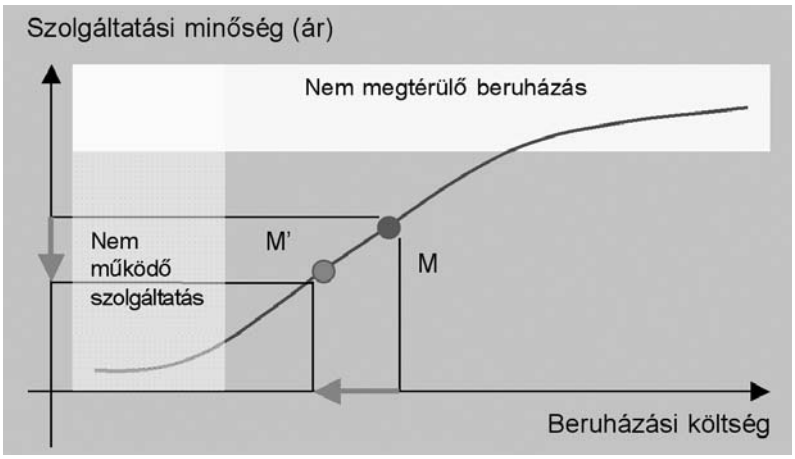
4. ábra

4.3. A fejlesztések révén remélt eredmény

A mérésügyi terület valóságadatainak fontosságát a bevezetőben már említettük. A folyamatban lévő fejlesztéstől azt várjuk, hogy a hatósági, társhatósági adatszolgáltatás gyorsabbá és részletesebbé válása révén a piacszabályozási és ellenőrzési tevékenység pontosabbá és gyorsabbá, így hatékonyabbá válik.

Ezen az áttételes eredményen túlmenően közvetlen pozitív következményei is lehetnek a mérési hatékonyság fokozásának.

Ennek illusztrálására nézzük a *4. ábra* kvalitatív példáját. Egy szolgáltatás megvalósításakor az ábra diagramjának M pontját méretezik a beruházók. Ha a beruházási költség alacsony, nem működő szolgáltatást kapunk, ha a szolgáltatás minőséget túl magasra méretezzük, akkor a beruházási költségek válnak nem megtérülő nagyságúvá.



5. ábra

Ha a megvalósított rendszert zavar éri, vagy a rendszerben használt berendezések nem megfelelő minőségűek, akkor a szolgáltatási minőség romlik. Ahogyan az *5. ábrán* látható, a szolgáltatási minőség romlása olyan viszonyokat teremt, amelyet a beruházási-üzemeltetési költségek alacsonyabb szintjén is biztosítani lehetett volna. Minél gyorsabban és minél pontosabban történik az okok megszüntetése, annál kisebb ideig tart és annál csekélyebb a jelentkező veszteség.

Tehát nem számolva az esetleges kieső szolgáltatások igénybevevőinél jelentkező másodlagos veszteségek nagyságrendjét, csak a szolgáltató közvetlen beruházási veszteségeit, a gyors és pontos mérőszolgálati beavatkozás közvetlenül csökkenti a veszteségeket. Mivel a diagram vízszintes tengelyén a hazai távközlési szolgáltató szektor beruházási költségei szerepelnek, ez a pozitív gazdasági hatás még kis zavartatás esetén is jelentős nyereséget jelent.

5. Összefoglalás

Összefoglalóan azt várhatjuk, hogy a sikeres informatikai fejlesztés hatására nő a hatósági mérőszolgálati munka hatékonysága és eredményessége, amely közvetve és közvetlenül is a hírközlési piac egésze számára gazdasági előnyöket fog jelenteni.

A szerzőkről

GÁSPÁR ERNŐ a BME Villamosmérnöki karán diplomázott 1981-ben, illetve ugyanitt szerzett számítástehnikai szakmérnöki oklevelet. Jelenlegi munkaköre a Nemzeti Hírközlési Hatóság Rádiómonitoring osztályának vezetése. Ennek keretében feladata a mérőszolgálati fejlesztések előkészítése és menedzselése.

ZIMMER ANDRÁS a BME-n végzett mérnök-informatikusként, valamint a Weatherhead School of Management-en szerzett MBA fokozatot. Informatikai és vezetői tanácsadó, legszívesebben az informatikai eszközök és a szervezeti működés közös határterületeivel foglalkozik. Cégével elsősorban egyedi rendszerek kialakításában és rendszerintegrációs feladatokban vesz részt. A Nemzeti Hírközlési Hatóság mérésügyi informatikáját hat éve támogatja külső szakértőként.

Hírek

A HP ProCurve Networking a Trainer C Oktató központtal együttműködve regionális képzési központot hoz létre az üzletág eszközeinek és megoldásainak magas színvonalú oktatása érdekében.

A központ 2009. januárjától fog működni és számos új témában biztosít majd képzési lehetőséget a régió viszonteladó partnereinek. A kibővült oktatási kínálatból a kereskedők Sales Professional és Sales Consultant tanfolyamokon vehetnek részt, míg a technikai jellegű oktatások közül is számos elérhető lesz Budapesten: Bevezetés a ProCurve hálózatok világába, Hálózatmenedzsment, Hálózatbiztonság, Nagy megbízhatóságú hálózatok. Továbbá a jövőben lehetőség lesz a már tapasztalt hálózati mérnököknek egy gyorsított jellegű tanfolyam elvégzésére, amely után rögtön ASE minősítést szerezhet a hallgató.

Az üzletág több, mint 40 ezer Euró értékben szerelte fel a központot ProCurve eszközökkel, így a képzésben résztvevők 2 darab 7102dl routeren, 2 darab 2610-24 switchen, 3 darab 3500yl és 2 darab 5400zl intelligens perem switchen, valamint két 530-as access point-on sajátíthatják el a gyártó megoldásait.

A kapcsolat a ProCurve és az oktatóközpont között nem újkeletű: a Trainer C 2005 óta rendez HP Procurve minősítő tanfolyamokat. Az oktatásokon a magyar HP partnerek közül évente mintegy 30-40 hallgató vesz részt. A tanfolyamok résztvevői eddig összesen 55 technikai, 45 kereskedői minősítést szereztek meg.

A Sun Microsystems bemutatta a JavaFX 1.0 verzióját, a Java(TM) platform fejlődéstörténetének legújabb és legjelentősebb állomását. Ezzel olyan új platform jött létre, amely a forma és a funkcionalitás tökéletes együttesét kínálja a web-böngészőkre és a felhasználói számítógépekre készített magával ragadó, élethű médiaélményt kínáló gazdag internetes alkalmazások (RIA) létrehozásához. A Sun JavaFX 1.0 platform óriási piaci lehetőségeket nyit meg a szoftver- és tartalomfejlesztők előtt, akik a szolgáltatásokat és funkciókat az ügyfelek valamennyi eszközére el kívánják juttatni. Néhány látványos demóalkalmazás a http://www.javafx.com/samples/ címen tekinthető meg.

A nemzetközi felmérések szerint a Java technológia jelenleg az asztali és noteszgépek több mint 90 százalékán, valamint a mobil eszközök 85 százalékán jelen van, és a fejlesztések éllovasaként jelenik meg az újgenerációs televíziókban, Blue-ray lejátszókban és televíziós set-top boxokban is.

NGN szolgáltatások sávszélesség-menedzsmentje LAN/MAN környezetben

GÁL ZOLTÁN

Debreceni Egyetem Tudományegyetemi Karok, Információtechnológiai Központ
zgal@unideb.hu

Lektorált

Kulcsszavak: NGN, TCP, UDP, kodek, QoS, DiffServ, önhasonlóság, wavelet, fraktál, entrópia

Az NGN (Next Generation Network), konvergens infokommunikációs hálózatokkal szemben támasztott elvárások a jelfolyamok továbbítása közben szolgáltatásminőségi (QoS) garanciák betartását igénylik. LAN/MAN környezetben a valós idejű és a hagyományos adatforgalmak protokoll adatelemeinek osztályozásához a QoS mechanizmusok közül leggyakrabban a DiffServ-et alkalmazzák. Kézenfekvő kérdésként vetődik fel a késleltetésre és késleltetésváltozásra leginkább érzékeny IP telefonok VoIP forgalmának viselkedése különböző hangkódoló/dekódoló megoldások alkalmazása esetén. Az analóg hang-jelfolyam digitalizálását és szűrését végző kódolók közül a G.711, a G.723, a G.728, a GSM, és a Wideband (G.722) szabványok által generált Ethernet adatforgalmak vizsgálatára került sor. Másfél évtizede ismeretes, hogy LAN környezetben a TCP-re épülő hagyományos szolgáltatások (http, ftp, telnet stb.) önhasonló, fraktál és multifraktál tulajdonságúak. A cikkben elemezzük az UDP-re épülő, az utóbbi időben egyre inkább elterjedő telefon-hangátviteli mechanizmusok Ethernet forgalom önhasonlóságára gyakorolt hatását. Ehhez megvizsgáljuk az IP telefonok UDP forgalmát torlódásos, illetve torlódásmentes környezetekben a wavelet analízis és az entrópia módszereivel. A saját elemzési módszert VoIP forgalmak jellemzéséhez használjuk fel.

1. Bevezetés

A jelenlegi és az ITU-T NGN (Next Generation Network) kommunikációs hálózatainak egyik legfontosabb időkritikus szolgáltatása a hangátvitel. A hang csomagkapcsolt hálózat feletti továbbításához a VoIP (Voice over IP) technológiát fejlesztették ki, amely az utóbbi években radikálisan megváltoztatja a telefontársaságok szolgáltatásainak árkalkulációját és a felhasználók hívásszokásait is. Mivel a VoIP hatékonyan veszi igénybe az Internet-alapú hálózati infrastruktúrát, így képes megközelíteni a hagyományos áramkörkapcsolt PSTN telefonrendszerek szolgáltatási minőségét.

Mivel az IP hálózatok „best-effort" továbbítási mechanizmusa nem képes a késleltetésre érzékeny hangtovábbításhoz megfelelő garanciákat biztosítani, a VoIP sikeres működtetéséhez a végfelhasználói berendezések között QoS (Quality of Service) technikák alkalmazására van szükség. A különböző QoS mechanizmusok optimális kiválasztásához LAN környezetben meg kell vizsgálni a hang- és egyéb adatok aggregált forgalmának modellezéséhez szükséges jellemzőket. A hangforrásból származó hálózati forgalom szignifikánsan függ az alkalmazott hangkódoló-dekódoló (kodek) típusától. A szakirodalom a hangkodekeket két csoportba sorolja. Az egyik csoportba a konstans bitsebességű továbbítási mechanizmusok (pl. G.711), míg a másik csoportba a csend elnyelésére, valamint aktív (ON) és inaktív (OFF) szakaszok periodikus ismétlődésére alapozó mechanizmusok (pl. G.728, GSMFR, G.722) tartoznak [4].

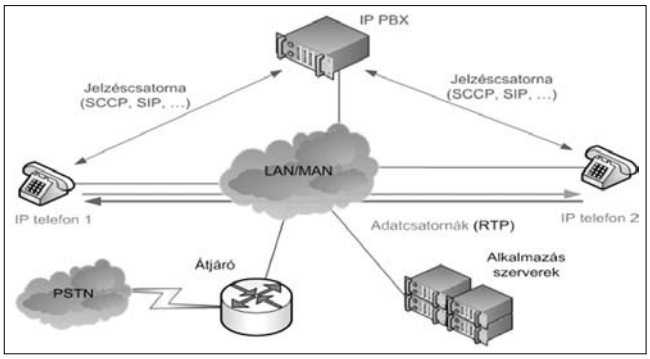
A csomagkapcsolt adatátvitel modellezésére általában jellemző, hogy csak a keretek beérkezési időpillanatainak idősorát, mint sztochasztikus folyamatot vizsgálják [5]. Jóval kevesebb azon vizsgálatok száma, melyek során figyelik a keret bájtban mért hosszát is, és e két folyamat együttes elemzésével magyarázzák a PDU-k továbbítását [6].

Jelen cikk célkitűzése, hogy a csomagkapcsolt hálózati mechanizmusok valós idejű szolgáltatásai számára szükséges QoS megoldások viselkedésének bemutatásához a beérkezési időközök és a keretméretek együttes elemzését elvégezze. Mivel a csatorna sávszélessége két szomszédos hálózati eszköz között technológiafüggő és rögzített, ezáltal a bájtszámban kifejezett keretméret egy lineáris leképezéssel könnyen az idődimenzióba konvertálható. ON/(ON+OFF) transzformáció segítségével csatornaterhelés- és intenzitás-idősorunk keletkezik, ami együttesen előnyösen elemezhető.

2. Hangkodekek VoIP és IP telefónia környezetben

A korszerű, csomagkapcsolt telefonrendszer nemcsak az IP forgalomra képes telefonvégpontokat foglalja magába, hanem a jelzésrendszerért, a kapcsolatok felépítéséért és a forgalom elszámolásáért felelős alkalmazás szervereket is. A végpont foglaltságára, illetve annak mértékére vonatkozó jellemzők nyilvántartása a hívásmenedzsmentért felelős szerverben történik *(1. ábra)*.

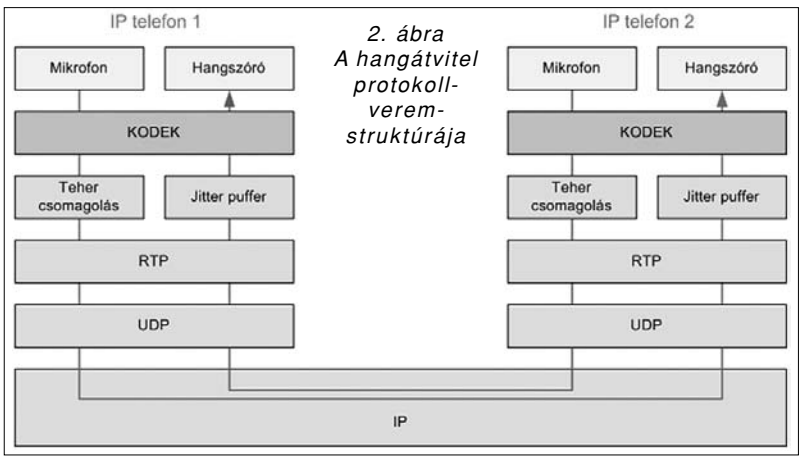
Különböző típusú jelzésrendszerek (SSCP, SIP stb.) léteznek, amelyek intelligensebbek, mint a hagyományos telefonhálózaton alkalmazottak (pl. QSIG). A hangtartalom átvitele RTP (Real Time Protocol) protokoll segítségével történik, amely a szerverek tevékenysége nélkül az adathálózaton közvetlenül a végpontok között zajlik. A jelzéseket TCP, a digitalizált hangot pedig UDP protokoll szállítja.



1. ábra IP telefon és VoIP

A régi PSTN telefonhálózatok irányába átjárók biztosítják a kapcsolatot, amelyek úgy a jelzésrendszer konverzióját, mint a csomagkapcsolt és az áramkör kapcsolt hálózatok közötti hangtranszformációt képesek elvégezni. Az IP telefon végpontok üzenetekbe helyezik el a mintavételezett hangot és különféle optimalizációs eljárások alapján szegmenseket alakítanak ki *(2. ábra)*. Az RTP protokoll a hangszegmens-sorozatot UDP-n továbbítja, amelyet vételi oldalon jitter puffer segítségével simít ki. A vevőkészülék dekódolója a szegmenseket és üzenetként adja át a telefon-alkalmazási szoftvernek.

A kodekek egy csoportja viszonylag kis, maximum 64 kbit/sec sávszélességet igényel. Ide tartoznak a G.711, G.723, G.728, GSM, amelyeket keskenysávú kodekeknek neveznek [4]. A jóminőségű hang továbbítása céljából kialakítottak szélessávú kodekeket is, mint a BrandVoice32, G.722 stb. Az IP hangkodekek jellemző paraméterei a hang bitsebessége, a hangkeret időtartama, a hangkeret mérete, a hang IP csomagban történő továbbításának sebessége, valamint a hang késleltetésének ideje. A paraméterek a kodektől függnek, így a hangkeret időtartama 0,125 és 20 msec között, mérete 80 és 520 bájt között, az IP csomag bitsebessége 24 és 272 kbit/sec között, míg a hangkésleltetés 0,25 és 40 msec között van. A késleltetést nyolc mechanizmus befolyásolja: mintavételezés-pufferelés, kódolás, csomagolás, küldés, LAN feletti szállítás, fogadás-pufferelés, dekódolás és lejátszás. Az interaktivitás biztosításához a nyolc mechanizmus késleltetésének összege nem haladhatja meg a 200 msec (magas hangminőség), illetve a 400 msec (elfogadható minőség) időtartamot.



2. ábra
A hangátvitel protokoll-verem-struktúrája

3. LAN/MAN QoS mechanizmusok

A különböző alkalmazások egymástól eltérő követelményeket támasztanak az adatforgalmat továbbító LAN hálózat felé. A generált forgalom erőforrás-igénye időben változó és általában szükséges, hogy a hálózat megfeleljen ennek az igénynek. Bizonyos alkalmazások többé vagy kevésbé toleránsak a forgalom késleltetésére, valamint a késleltetés változására. Továbbá néhány alkalmazás képes elviselni korláton belül adatvesztést, míg mások nem.

Ezek a követelmények a következő négy QoS-jellegű paraméter segítségével kerülnek kifejezésre: *sávszélesség* – az alkalmazás forgalmának továbbítási sebessége; *lappangási idő* – az a késleltetés, amit egy alkalmazás a csomag kézbesítésénél képes elviselni; *jitter* – a lappangási idő szórása; *adatvesztés* – az elveszített adatok százalékos aránya [7]. Mivel a hálózati erőforrások korlátosak, időtől függően a rendszer bizonyos részein a kerettovábbítási igények nem teljesíthetők. A QoS mechanizmusok az alkalmazások szolgáltatásigényének függvényében a hálózati erőforrások használatát szabályozzák. Ilyenek a dedikált sávszélesség allokálása, az előírt csomagvesztési jellemzők monitorozása, a torlódáskezelés és megelőzés, a forgalom formázása, valamint a forgalom priorizálása.

Többfajta QoS mechanizmus létezik, mindegyik speciális környezetben képes optimálisan kifejteni hatását. A QoS nélküli FCFS (First Come First Served) mechanizmust *„best effort"*-nak nevezzük. Az *Intserv* forgalomkezelő mechanizmus két modulból álló szolgáltatáshalmaz, ezek a garantált, illetve az ellenőrzött terhelés szolgáltatások (Guarranteed Service, Controlled Load Service).

A garantált szolgáltatás a forgalom számára kvantálható mértéket és korlátos lappangási időt biztosít. Az ellenőrzött terhelés szolgáltatás megadott mértékű forgalom számára terheletlen hálózati környezetet emulál. Az Intserv szolgáltatások többsége az IETF RSVP-re (Resource ReserVation Protocol), egy előre lefoglalásos típusú jelzésrendszerre épül. Mindegyik Intserv szolgáltatás vezérlési algoritmusokat definiál, amelyek az adott eszköznél befogadott forgalom mennyiséget határozzák meg anélkül, hogy romolna a szolgálat minősége. Az Intserv szolgáltatások nem használnak várakozásisor-algoritmusokat.

A *Diffserv* forgalomkezelő mechanizmus a hálózati rétegben fejti ki hatását. Az L3 protokoll adatelem fejrészében DSCP (Diffserv CodePoint) nevű mezőt helyez el. A végfelhasználói csomópontok és a routerek a diffserv hálózatba küldött forgalom minden egyes csomagját a megfelelő DSCP értékkel látják el. A diffserv hálózatban lévő routerek minden csomagra a DSCP érték alapján történő osztályozás szerint specifikus PHB (Per-Hop Behavior) várakozásisor-kezelő algoritmust vagy ütemezőt alkalmaznak. A QoS tartomány bemeneti oldalán a hálózati interfésznek a következő műveleteket kell elvégeznie: osztályozás, szabá-

lyozás, jelölés (marking), valamint várakozási sorba helyezés (queueing). A kimeneti oldalon szükséges tevékenységek: a várakozási sorba helyezés és ütemezés, valamint a belső DSCP alapján kimeneti queue választása. A kimeneti interfészeken alkalmazott queue algoritmusok leggyakrabban: FIFO, FQ, WFQ, WRED, „taildrop" és az LLQ. Fontos megjegyeznünk, hogy a QoS minőségi modellek fejlődése során a hangátvitelt a videóátvitelnél is kritikusabb alkalmazásnak tartják, ezért a nyolc közül a legmagasabb QoS osztályba sorolják.

4. IP hálózatok teljesítménye, Corvil sávszélesség

A modern IP hálózatok alkalmazásainak teljesítményét három tényező befolyásolja: *sávszélesség, statisztikai multiplexelés* és a *QoS mechanizmusok* [3]. A sávszélesség megmérése egyszerű, mivel a gerinchálózati eszközök (router, switch) SNMP (Simple Network Management Protocol) MIB (Management Information Base) objektumokban képesek letárolni az öt perces átlagértéket.

Az így rendelkezésre álló adatok a hálózaton átfolyó forgalom mértékét képesek megadni, de nem mérik meg az alkalmazások előírt működéséhez szükséges sávszélességet. A csomagvesztés és a jitter lényegesen függ a forgalom ms szintű viselkedésétől. Nincs elegendő rálátás a forgalomra, ezért az alkalmazások teljesítménye nem látható előre. Közepes méretű hálózatban a VoIP alkalmazásnál a lappangás és a jitter csak n*10 ms nagyságrendű lehet. Adott forgalmakkal kapcsolatos gyakorlati tapasztalatok empirikus szabályok kidolgozásához vezettek. Ilyen szabály az is, amely szerint a „best effort" IP szolgáltatásoknál a 95%-os öt percenkénti terhelés az erőforrások használatának csak 60%-ában ajánlatos. Ha a forgalom ezt a küszöbértéket meghaladja, akkor az infrastruktúra bővítése szükséges. A fenti százalékok „érzés" szerintiek, de nem általánosíthatók tetszőleges hálózati szolgáltatások esetén. Tapasztalat alapján VoIP számára 60% helyett 40% javasolt.

A hálózati szolgáltatók hatékony eszköze a *statisztikai multiplexelés* nyeresége, amely a csomagkapcsolt hálózatokban az erőforrások véletlenszerű megosztását jelenti. Például, ha tíz videócsatornát áramkörkapcsolt hálózaton kellene továbbítani, akkor pontosan egyetlen csatorna sávszélességének tízszeresére lenne szükség. Ugyanez csomagkapcsolt hálózatban a tízszeresnél jóval kevesebb sávszélességet igényel. Ennek magyarázata, hogy az egyik csatorna rövid időskálájú börsztje nagy valószínűséggel más csatornaforgalom hiányával esik egybe, így az aggregált forgalom simítottabb, mint bármelyik egyedi folyam. A folyamonkénti sávszélességek összege és az aggregált sávszélesség különbségét a statisztikai multiplexelés nyereségének nevezzük, ami egyben az IP hálózatok hatékonyságát is jellemzi.

A forgalomsimítás, a policing és a különbözeti várakozási sorkezelés a leghatékonyabb *QoS mechanizmusok*. A robusztus statisztikai megbízhatósághoz szükséges sávszélesség méretezése, az előírt statisztikai multiplexelési nyereség nyújtása, valamint a QoS mechanizmusok konfigurálása két, nehezen eldönthető választási mód egyikével lehetséges: kihozható a legnagyobb nyereség az elérhető minőség biztosítása árán, vagy megcélozható az előre látható teljesítmény nyújtása a hálózat erőforrásainak túldimenzionálásával. Az első választási mód esetén speciális szolgáltatások nem nyújthatók, míg a második választási módnál költséges hálózati rendszer szükséges.

A hálózati forgalom bizonytalanságának megnyilvánulási jellemzője a három alapvető összetevő közötti összefüggés nem-determinisztikus viszonya [3]. A hálózat sávszélessége, a forgalom terhelése és a QoS célok lényegében összefüggnek. Egyik módosítása befolyásolja a másik kettő közötti kapcsolatot. Így például adott késleltetés garantálásához szükséges sávszélesség nemcsak a hálózat terhelésétől, de a forgalom típusától (VoIP, adat) is függ. Az alábbi összefüggés választ ad arra a kérdésre, hogy a hálózat milyen minőséget nyújt a rajta folyó forgalom számára:

$$\text{Minőség} = \mathrm{F_Q}(\text{Hálózat}, \text{Forgalom}) \qquad (4.1)$$

Ez az alapvető összefüggés kiemeli azt a tényt, hogy a minőség nem csak a hálózat konfigurációjától, hanem a forgalom mennyiségétől és jellegétől is függ. A 4.1. összefüggés két másik kérdést is implikál.

Először: milyen hálózati erőforrások szükségesek a forgalmak előírt minőségéhez? Ha a kérdéses erőforrás a sávszélesség, az alapvető összefüggés az alábbi lesz:

$$\text{Sávszélesség} = \mathrm{f_B}(\text{Hálózat}, \text{Minőség}) \qquad (4.2)$$

Másodszor: adott hálózati erőforrás készlet esetén mennyi forgalom továbbítható anélkül, hogy a minőség lényegesen romolna? Erre a választ az alábbi alapvető összefüggés adja:

$$\text{Forgalom} = \mathrm{f_T}(\text{Hálózat}, \text{Minőség}) \qquad (4.3)$$

A fenti viszonyokat figyelembe kell venni ahhoz, hogy a minőségi szint megtartása mellett a hálózat kihasználtságának minél magasabbra emeléséhez áteresztő-vezérlő mechanizmusokat lehessen kidolgozni. A Corvil sávszélesség technológia a fenti három egyenlet adott környezetben történő megoldására ad nem-nyilvános módszert. Ehhez az adott forgalmak mérésére van szükség, amiből erőforrás-méretezési ajánlások származtathatók.

A sávszélesség a legegyszerűbb, legjobban érthető és legkönnyebben méretezhető a fenti három komponens közül. A minőség viszonylag egyszerűen definiált és mért jellemző. A mai legtöbb SLA (Service Level Agreement) rögzíti a csomagvesztési, illetve a késleltetésparamétereket, amelyeket heti vagy havi időskálán mérnek. Ezek túlságosan durva értékek az értelmes alkalmazások teljesítményének garantálásához.

A csomagforgalmak mérése nem elég részletes manapság, ami korlátozza a legjobb gyakorlatok kialakításának lehetőségét. A hálózati forgalom minősége erőteljesebben függ az eseményektől, mint amit az SNMP-vel (Simple Network Management Network) egyszerű átlagolással mérnek. A mennyiségi részletek gyakran börszt-

ként jelennek meg. Ismeretes, hogy minél börsztösebb egy forgalom, annál több sávszélesség szükséges a hullámzás szabályozásához, ugyanakkor analitikusan nem számszerűsíthető a sávszélesség, a forgalom és a minőség közötti pontos viszony.

A *Corvil sávszélesség* (CB, Corvil Bandwidth) technológia a nagy kilengések statisztikai elméletre épül, amely a megfigyelt rendszer kulcsfontosságú statisztikai jellemzőit, entrópiáját vizsgálja. A sorbanállás elméletben egy csomagfolyam entrópiája azt írja le, hogy miként jönnek létre várakozási sorok a hálózati eszközökben, illetve hogyan történik a várakozási sorokban és az ütemezőkben a multiplexelés más csomagfolyamokkal.

$$\mathrm{CB} = \mathrm{f_Q}(\text{Corvil entrópia}, \mathrm{QoS}) \tag{4.4}$$

Interfészek vagy forgalomosztályok CB méretezéséhez az alábbi irányelvek léteznek: várakozási sor késleltetésének (0,001...1 s) és méretének (1...2000 csomag) küszöbértéke; védett csomagok százalékos aránya (1...100%, 0,0001%-os lépésekben); védelmi irányelv alkalmazásának periódusa (5 perc; 1, 2, 4 óra; 1 nap; 1 hét). Ha öt perces periódussal készül a CB mérése, akkor ez összehasonlítható a szabványos hálózatmonitorozó eszközök által SNMP-vel mért sávszélességgel. Az alapvető különbség az, hogy a CB öt percenkénti mérése figyelembe veszi az ezredmásodperc szintű tulajdonságokat is, így a valós sávszélességigény a csomagtovábbítás késleltetése és a csomagvesztés mértéke függvényében határozható meg.

5. Önhasonló folyamatok wavelet analízise

A valós értékű $\{Y(t), t \in \mathbf{R}\}$ folyamat $H>0$, Hurst paraméterű önhasonló (H-ss), ha $\forall a>0$ esetén $Y(at) \overset{\text{def}}{=} a^H Y(t)$. A valós értékű $\{Y(t), t \in \mathbf{R}\}$ folyamat H-sssi, ha H paraméterű önhasonló és stacionárius növekményű. Ha $\{Y(t)\}$ H-sssi véges szórású, akkor $0<H\leq 1$. Diszkrét időben képezett növekménysorozat előállítható az $X_k = Y(k) - Y(k-1)$, $k = 1,2,...$ módon.

Legyen $X^{(m)}$, illetve $r^{(m)}(\cdot)$ az X m-agregált idősora, illetve annak autókorrelációs függvénye, ahol

$$X_k^{(m)} = \frac{1}{m}\sum_{i=(k-1)m+1}^{km} X_i.$$

A $0<H<0,5$ esetén a folyamat rövid memóriájú (SRD), $0,5<H<1$ esetén pedig hosszú memóriájú (LRD). Ha a folyamat LRD, akkor a növekményfolyamat autókorrelációs függvényének alakja a következő:

$$r(k) = \frac{1}{2}[(k+1)^{2H} - 2k^{2H} + (k-1)^{2H}].$$

Pontosan önhasonló folyamat esetén az aggregált növekményfolyamat szórása

$$var\left(X^{(m)}\right) = m^{2H-2} var(X), \text{ és } r^{(m)}(k) = r(k).$$

Megfigyelhető, hogy LRD esetén $var(X^{(m)}) > m^{-1} var(X)$, míg SRD esetén $var(X^{(m)}) < m^{-1} var(X)$.

Az X folyamat aszimptotikusan önhasonló, ha elég nagy k esetén $\lim_{m\to\infty} r^{(m)}(k) = r(k)$.

A diszkrét wavelet-transzformáció (DWT) egy idő-frekvencia felbontás, amely az n hosszúságú X idősorhoz kétváltozós együtthatókat rendel a következő módon [1]:

$$d_{j,k} = \int X(s)\psi_{j,k}(s)ds, j \in \mathbf{Z}, k \in \mathbf{Z} \tag{5.1}$$

ahol a wavelet-ek alakja a következő:

$$\psi_{j,k}(s) = 2^{-j/2}\psi(2^{-j}t - k) \tag{5.2}$$

Több fajta elemi hullámfüggvény létezik és mindegyikre igaz az alábbi:

$$\int t^k \psi(t)dt \equiv 0, \ \forall k = 1,2,\ldots,N-1 \tag{5.3}$$

A wavelet-felbontás a speciális elemi hullámfüggvények és a $d_{j,k}$ együtthatók lineáris kombinációja az alábbi módon:

$$X(t) = \sum_{j\in\mathbf{Z}}\sum_{k\in\mathbf{Z}} d_{j,k}\psi_{j,k}(t) \tag{5.4}$$

A wavelet-együtthatók felhasználhatók az LRD folyamat skála-, illetve frekvenciafüggő tulajdonságának tanulmányozására.

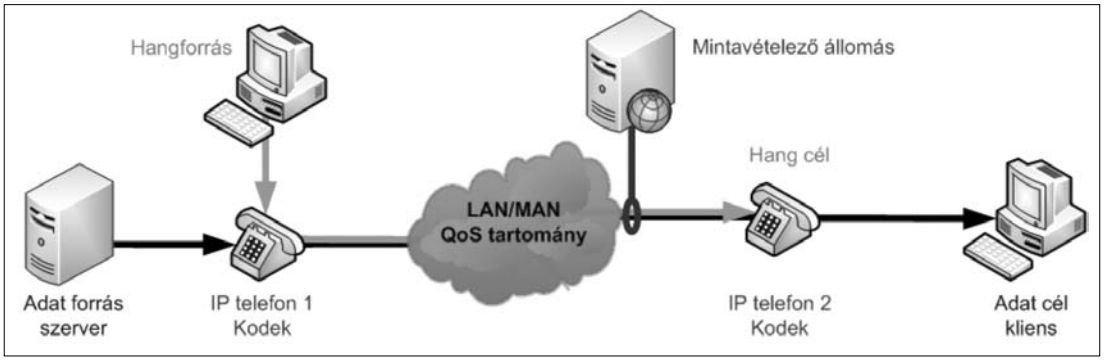
A másodrendű Log-skála diagram (2-LD) a becsült második momentum j-oktáv függvényében készített Log-lineáris grafikonja: (5.5)

$$\mu_j = \frac{1}{n_j}\sum_{k=1}^{n_j}|d_{j,k}|^2 \approx 2^{j(2H-1)}, \text{ahol } n_j = 2^{-j}n$$

A wavelet együtthatók k szerinti négyzetösszegének átlagát az idősor μ_j energiafüggvényének nevezik. Ennek logaritmusa a (4.5) alapján a j-oktáv lineáris függvénye lesz.

$$y_j = log_2(\mu_j) \approx (2H-1)j + c \tag{5.6}$$

A Hurst paraméter becsléséhez a 2-LD lineáris szakaszát vagy szakaszait lehet felhasználni. Ha több lineáris szakasz különíthető el, akkor a folyamat multifraktál, egyébként monofraktál.



3. ábra
VoIP kapcsolatok mérési környezete

A súlyozott legkisebb négyzetek módszerével (WLS) becsülhető a $[j_1,j_2]$ lineáris oktáv szakaszhoz tartozó Hurst paraméter az alábbi módon [1]:

$$\widehat{H}(j_1,j_2)=\frac{1}{2}\left|\frac{\sum_{j=j_1}^{j_2}s_j j\, y_j-\sum_{j=j_1}^{j_2}s_j j\sum_{j=j_1}^{j_2}s_j y_j}{\sum_{j=j_1}^{j_2}s_j\sum_{j=j_1}^{j_2}s_j j^2-\left(\sum_{j=j_1}^{j_2}s_j j\right)^2}+1\right|,$$

$$ahol\ S_j=\frac{n\ ln^2 2}{2^{j+1}}\ súly. \qquad (5.7)$$

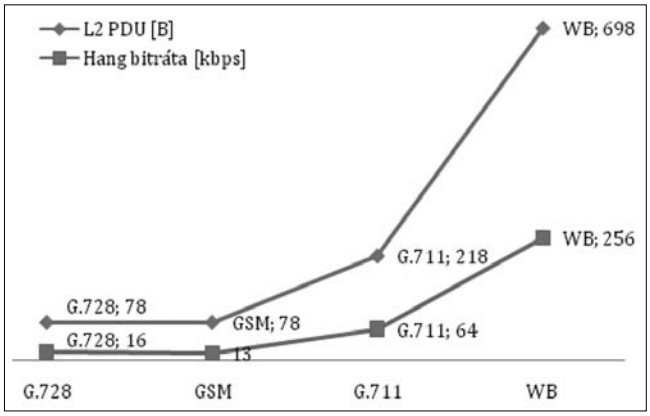
6. Mérési környezet és a mért folyamatok elemzése

a.) *VoIP kapcsolatok forgalomelemzését torlódásos környezetben* végeztük. Az adatforrás és adatcél gépek között mesterségesen (T) TCP, illetve (U) UDP adatforgalmat generáltunk, amellyel a 10 Mbit/sec Ethernet csatorna rendelkezésre álló kapacitását teljesen kitöltöttük. Az IP telefonok LAN kapcsolatán a hangforgalom és az adatforgalom egyaránt továbbítódott *(3. ábra)*.

Egyenként egy perces (H) hard rock (Limp Bizkit – Eat You Alive), illetve (P) zongora (W. A. Mozart – Concert for horn and orchestra KV KV 285d C major Adagio non troppo) zeneszámokat játszottunk le a hangforráson, amit az 1-es IP telefonról a 2-es IP telefonra küldtük át. Különböző hangkodekeket (G.728, GSM, G.711, WideBand-G.722) alkalmaztunk, miközben a LAN QoS tartományon belül csak a hangforgalom QoS paramétereit szabályoztuk DSCP=(0x00-"best-effort", 0x02-alacsony ár, 0x04-megbízható, 0x08-teljesítmény, 0x10-kis késleltetés) szempontok alapján. A nyolcvan darab idősort a szállítási réteg protokolljának típusa, a hangműsor dinamikája, a kodek típusa és a hangforgalom DSCP változtatásával állítottuk elő és Wireshark program segítségével 1 μsec pontossággal mintavételeztük: [(T,U) x (H,P) x (G.728, GSM,G.711,WB) x (0,2,4,8,16)] =2x2x4x5=80.

b.) *VoIP gerinc torlódásmentes környezetben* mért forgalmát elemeztük. Ehhez mintavételeztük egyetemi környezetben munkanapon, délelőtti időszakban 1500 darab IP telefon populáció IP/PBX gateway felé haladó hang VLAN aggregált forgalmát. A hang-gerinchálózat számára rendelkezésre álló 100 Mbps-os Ethernet kapcsolaton a mintavételezés egy órán át tartott és 1 μsec pontossággal készült.

4. ábra Kodek jellemzők



Mindkét mérési környezetben a mintavételezés során az Ethernet-keretek beérkezési időközét, valamint bájtban kifejezett méretét használtuk fel. A hangforgalom esetén az IP csomagok sohasem fragmentálódtak, mivel az Ethernet *MTU*=1500 bájt. A keretméretet egyszerű lineáris transzformációval az idő dimenzióba konvertáltuk át, ami lehetővé tette az L_i, átlagos kerettovábbítási időtartam (ON), illetve a tan(φ_i), csatornaterhelés idősorok kiszámolását. A mintavételezés periódusa, $T=T_{ON}+T_{OFF}$ rögzített időtartam és az összes mérés esetén T=100 ms. M_i jelöli T időközönként beérkezett keretek számát (számosság, intenzitás).

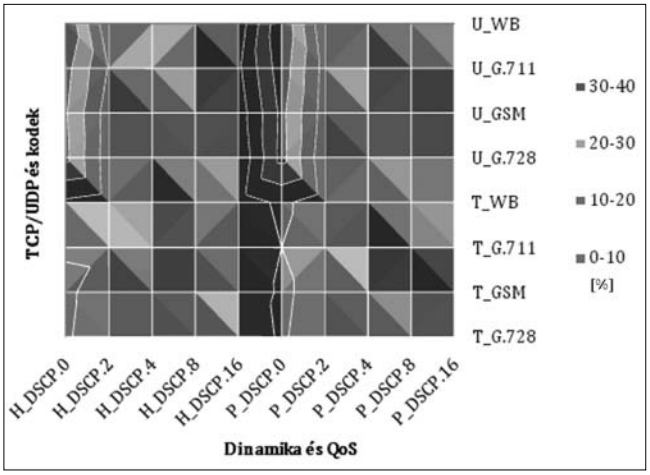
Ezáltal egyszerűen kiszámolhatóvá válik a hangforgalom pillanatnyi csatornaterhelése, illetve fázisa az alábbi módon

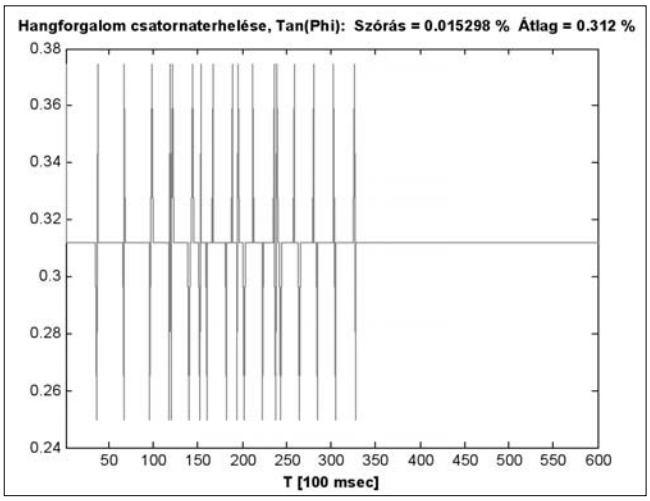
$$\left.\begin{array}{l} M_i,\ Számosság, intenzitás \\ L_i,\ Keret\ továbbítási\ idő \\ D_i=\sqrt{L_i^2+T^2},\ Négyzetes\ átlagidő \\ \tan(\varphi_i)\,[\%]=\frac{L_i}{T}*100,\ Terhelés \\ \varphi_i[Rad]=\tan^{-1}\frac{L_i}{T},\ Fázis \end{array}\right\} \qquad (6.1)$$

VoIP torlódásos környezet számára a négy fajta kodek jellemzőit a *4. ábra*, a nyolcvan darab számosságidősor relatív szórását pedig az *5. ábra* szemlélteti. A hang csatornaterhelésének relatív szórása gyakorlatilag megegyezik a számosság relatív szórásával. Az 5. ábrán a sötétebb színek a kisebb értékeket, a világos színek a nagyobb értékeket jelzik.

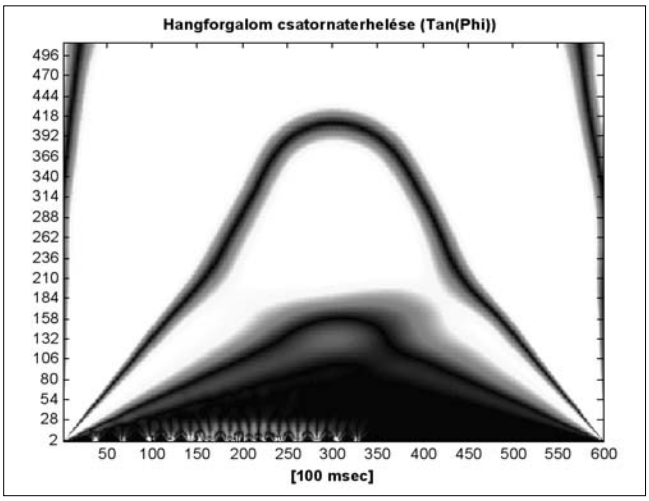
Megfigyelhető, hogy DSCP=0 („best effort") és TCP adatforgalom esetén a G.711 kodekkel meghajtott hangforgalom intenzitásának relatív átlagos szórása alacsony, míg a többi kódolónál ez jelentősebb és elérheti akár a 20%-ot is (GSM). Ugyanakkor QoS-biztosítás esetén, azaz a hangforgalom prioritással való kezelésénél a relatív szórás mindegyik kodeknél alacsony marad. Az UDP adatforgalom esetén nagyobbak a terhelés relatív szórásai, míg TCP adatforgalom esetén ezek kisebb értéket mutatnak. Ezt a TCP folyamszabályozó mechanizmusa okozza, amely torlódott csatornán a TCP adatforgalmat az UDP hangforgalom javára kisebbre és egyenletesebbre simítja. Az UDP adatforgalom esetén nincs adat-

5. ábra Számosság, intenzitás (M)

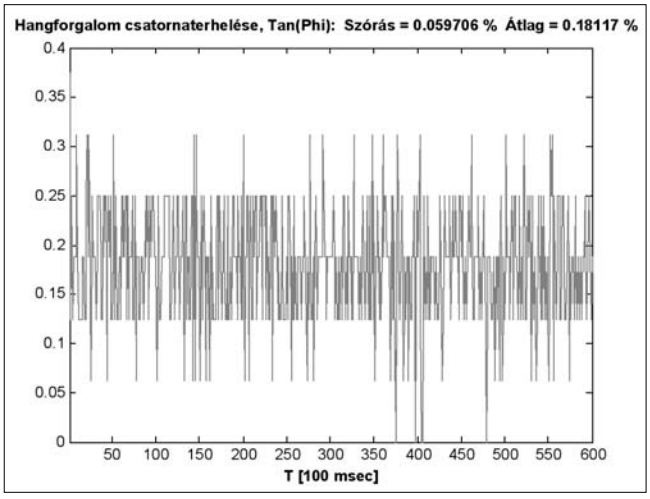




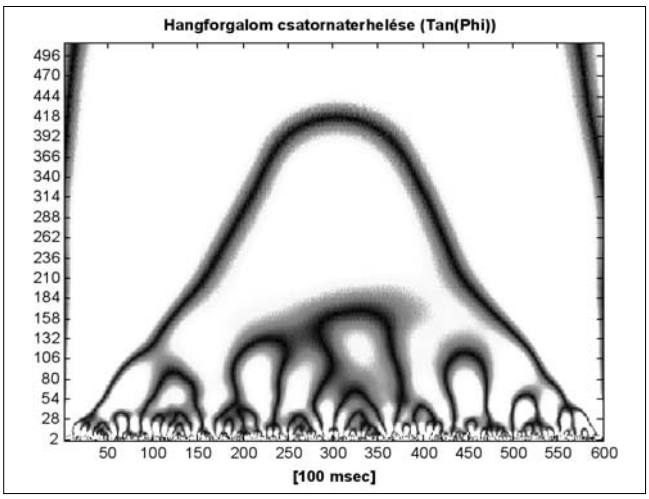
6. ábra Csatornaterhelés, Tan(Phi) (UDP, G.728, QoS nincs, Hard Rock)



7. ábra Wavelet transzformált, Tan(Phi) (UDP, G.728, QoS nincs, Hard Rock)



8. ábra Csatornaterhelés, Tan(Phi) (UDP, G.728, DSCP=8, Piano)



9. ábra Wavelet transzformált, Tan(Phi) (UDP, G.728, DSCP=8, Piano)

folyam szabályozás, így a QoS nélküli hangforgalom számára nagyobb szórások tapasztalhatók. A hangforrás dinamikája csak az alacsony bitsebességű kodekeknél okoz észrevehető terheléskülönbséget.

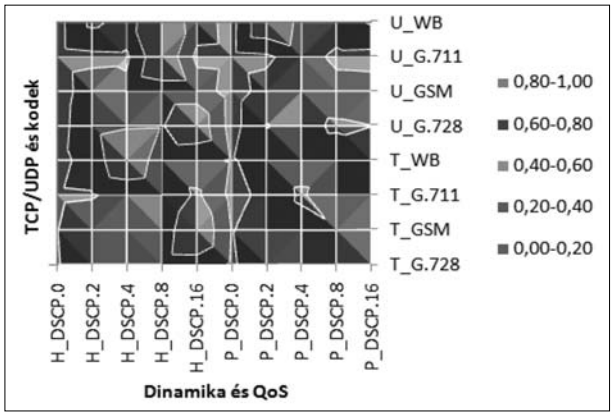
1. táblázat Becsült H paraméter Tan(Phi) esetén

	T G.728	T GSM	T G.711	T WB	U G.728	U GSM	U G.711	U WB
H_DSCP.0	0,86	0,87	0,79	0,59	0,92	0,91	0,73	0,57
H_DSCP.2	B	B	0,73	0,76	B	B	0,75	0,93
H_DSCP.4	B	B	0,83	B	B	B	0,80	0,81
H_DSCP.8	B	B	0,74	0,76	B	B	B	B
H_DSCP.16	B	B	B	0,74	B	B	0,77	0,79
P_DSCP.0	0,87	0,85	0,78	0,57	0,91	0,89	0,72	0,56
P_DSCP.2	B	B	0,83	0,77	B	B	0,80	B
P_DSCP.4	B	B	B	0,79	B	B	0,96	0,82
P_DSCP.8	B	B	0,75	0,77	B	B	0,78	0,81
P_DSCP.16	B	B	0,74	0,81	B	B	0,76	0,90

A *6–9. ábrák* a csatornaterhelés idősorokat, valamint ezek wavelet-transzformáltját mutatják UDP adatforgalom, G.728 kodek, „best-effort”/QoS és hard rock/piano zene feltételek mellett. Annak ellenére, hogy a két idősor jellege hasonlít egymásra, a lényeges különbséget a wavelet transzformált érzékelteti szemléletesen.

Az *1. táblázat,* illetve a *10. ábra* a nyolcvan különböző esetben vizsgált csatornaterhelés, illetve intenzi-

10. ábra Becsült H paraméter M esetén



tás wavelet-módszerrel becsült Hurst-paraméterét mutatja. Úgy TCP, mint UDP adatforgalmak esetén a QoS mechanizmussal szabályozott hangforgalom csatornaterhelése G.728 és GSM kódolóknál nem mutat önhasonlóságot, ami miatt a becsült H paraméter egynél nagyobb. Ezzel ellentétben a G.711 és a G.722 (WB) az esetek többségében önhasonló és hosszú memóriájú (LRD).

A hangforrás dinamikájától és a torlódást okozó adatforgalom szállítási réteg protokolljától (UDP/TCP) függetlenül a QoS nélküli („best effort") esetekben a hangforgalom csatornaterhelése önhasonló (H-SSSI) és hosszú memóriájú (LRD), a becsült Hurst paraméter $\hat{H} \in [0.56, 0.91]$. Megfigyelhető, hogy a kodek sávszélességével ellentétes irányban változik a torlódott hangforgalom csatornaterhelésének becsült Hurst paramétere (lásd 4. ábra és 1. táblázat). A mérések során a fogadó oldalon tapasztalt hang minősége a nagyobb sávszélességű kodekek esetén jobb volt, ugyanakkor a QoS mechanizmusok alkalmazása, azaz *DSCP*≠0 esetén a hang torlódása kevésbé volt érzékelhető.

Az intenzitás idősorok is LRD típusúak és minden esetben $\hat{H} \in [0.52, 1]$. Megfigyelhető, hogy az adatforgalom szállítási réteg protokolljától függetlenül, QoS nélküli esetekben, a hangforgalom intenzitásának becsült Hurst-paramétere, a 0.5 értéket csak kis mértékben lépi túl: $\hat{H} \in [0.51, 0.6]$ (lásd 10. ábra). G.711 kodek esetén csak a dinamikus hang és *DSCP*=8, teljesítmény-optimalizálási QoS mechanizmus ad az intenzitás $\hat{H}$ paramétere számára magas értéket. A dinamikus hangforgalom intenzitásának $\hat{H}$ értéke nagyobb, mint a dinamika nélküli hang esetén (lásd 10. ábra.)

VoIP torlódásmentes környezet számára a *11-12. ábrák* aggregált IP hangforgalmak által generált csatornaterhelését, illetve intenzitását, míg a *13-14. ábrák* ezeknek az (5.7) szerinti 2-LD grafikonját mutatja be. Habár a csúszó átlagok korrelációt mutatnak, az intenzitás idősor helyi maximumai miatt a két idősor jellege lényegesen különbözik egymástól.

A csatornaterhelés 1 másodperces csúszó átlagai nagyon jól mutatják az egyidejű beszélgetések darabszámát, ami a grafikonok lépcsőzetességéből származtatható. A csatornaterhelés relatív szórása 53%, az intenzitásé pedig annál kisebb, csupán 44%. A kisebb értéket az intenzitás helyi maximumai okozzák. A VoIP gerinchálózati hangforgalom is torlódásmentes állapotban multifraktál tulajdonságot mutat.

Addig, amíg a csatornaterhelésnél a wavelet-módszerrel becsült Hurst-paraméter, $\hat{H}$=0.88 és kevésbé skálafüggő, addig az intenzitásnál ez, $\hat{H}$=0.61 és nagyobb oktávoknál szignifikánsan változik (13-14. ábrák).

Mivel ebben az esetben torlódásmentes az Ethernet csatorna, ezért az aggregált hangkapcsolatok forgalma önhasonló és hosszúmemóriájú (LRD).

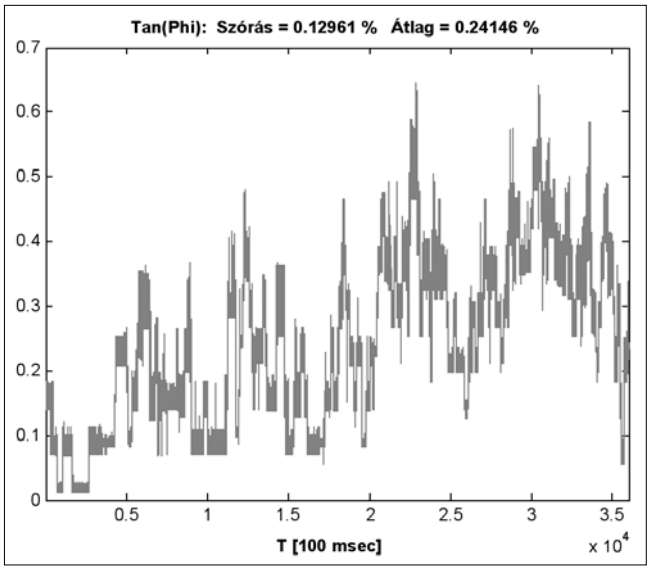
7. Összefoglalás és következtetések

A hangátvitel IP felett az egyik legkritikusabb valósidejű hálózati alkalmazás, üzemeltetése komplex feladat. A hangkodek típusa meghatározza a hangcsatorna minőségét. A VoIP hangcsatorna UDP-n működik, így nincs a szállítási rétegben visszacsatolás, nincs folyamszabályozás és nincs hangkeretméret-változtatás sem. A kodek hangminősége függ a hangcsatorna bitsebességétől, valamint a csomagkapcsolt protokoll adatelemeinek méretétől is.

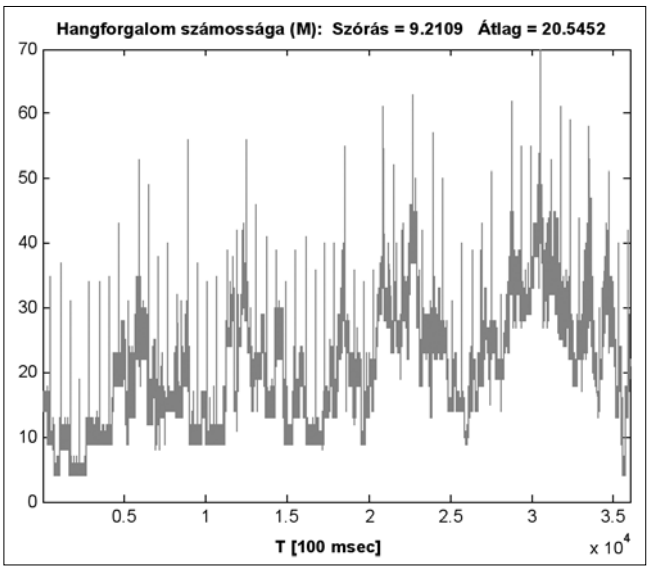
A vizsgált esetekben a hangkodekek növekvő minőségi sorrendje az alábbi: G.728, GSM, G.711, WB (G.722). Megállapítottuk, hogy LAN/MAN környezetben az L2/L3 hangforgalmak fraktálosodása torlódás esetén a hang minősége számára komoly romlást okoz. A csomagkapcsolt adat- és hangforgalom fraktál és skálafüggő tulajdonságának elemzéséhez kényelmes statisztikai eszközt biztosít a wavelet-analízis.

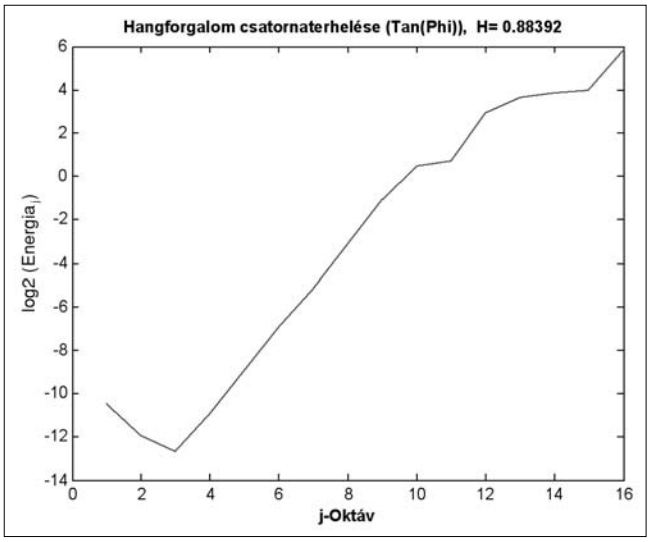
A QoS egy másik síkban, szolgáltatásként jelenik meg az OSI rétegprotokollok számára és erőteljesen megváltoztatja a csomagkapcsolt protokollelemek további-

11. ábra VoIP gerincforgalom csatornaterhelése

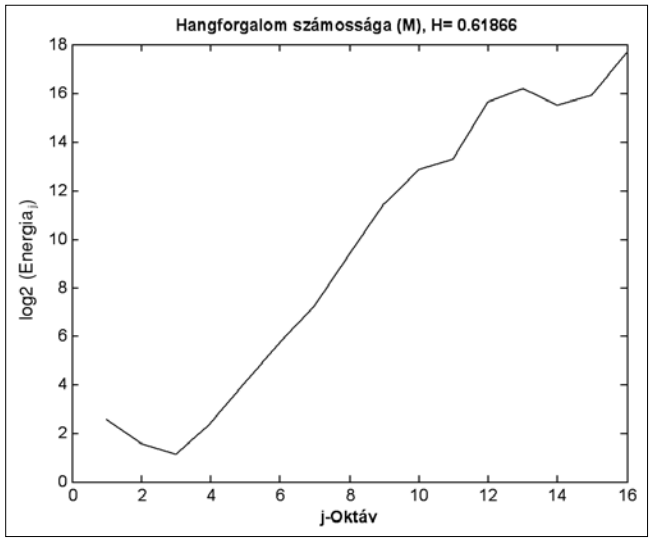


12. ábra VoIP gerincforgalom intenzitása





13. ábra VoIP gerincforgalom csatornaterhelés Hurst paraméterének wavelet becslése ($\hat{H}$)



14. ábra VoIP gerincforgalom intenzitása Hurst paraméterének wavelet becslése ($\hat{H}$)

tásának hagyományos értelemben vett önhasonló tulajdonságát. QoS segítségével mesterségesen szabályozott hangforgalmak továbbításánál az önhasonló, illetve LRD tulajdonságok érzékenyen befolyásolhatók. Ez új irányokat nyit meg a QoS-sel történő forgalomszabályozás területén.

További elemzések szükségesek a csomagkapcsolt protokoll adatelemeinek csatornaterhelési, illetve intenzitás-jellemzőinek együttes alkalmazására vonatkozóan annak érdekében, hogy a gerinchálózati eszközökben a rendelkezésre álló véges hálózati erőforrások használatához a legoptimálisabb QoS konfigurációs beállításokat meg lehessen határozni. Ehhez a 10...100 µs-os tartományban lezajló folyamatok statisztikai elemzésére van szükség, ahonnan kinyert entrópia jellemzőinek és makro-hatásának meghatározó fontossága van.

A szerzőről

GÁL ZOLTÁN Gyergyószentmiklóson született 1966-ban. Temesváron diplomázott informatika-villamosmérnökként. 1991-től a Kossuth Lajos Tudományegyetem Informatikai Szolgáltató Központ munkatársa, 1994-től a Hálózatok Osztály vezetője, 2001-2005 között a Debreceni Egyetem Informatikai Szolgáltató Központjának, majd 2006-tól ugyanott a Tudományegyetemi Karok Információtechnológiai Központjának igazgatója. Jelenleg az egyetem Informatikai Tudományok Doktori Iskolájának doktorjelöltje. Kiemelkedő szerepe volt a debreceni városi felsőoktatási hálózat (FDDI, ATM, 10GE) kiépítésében és fejlesztésében, a telekonferencia, valamint a VoIP/IP telefon szolgáltatások intézmény szintű bevezetésében. Érdeklődési területe a csomagkapcsolt infokommunikációs hálózatok minőségének elemzése. 1997-től tagja az IEEE Communications Society-nek, 2001-től az NIIFI Műszaki Tanácsának, 2003-tól pedig a Hungarnet Egyesület Elnökségének.

Irodalom

[1] Patrice Abry, Lois D'échelle,
Multirésolutions et Ondelettes,
Habilitation Travaux de Recherche,
Université Claude Bernard Lyon, Mars 2001.
[2] Corvil Ltd, Whitepaper:
An Introduction to Corvil Bandwidth Technology, 2004.
[3] Corvil Ltd, Whitepaper:
Managing Performance in
Financial Trading Networks, 2008.
[4] T.D. Dang, B. Sonkoly, S. Molnár,
Fractal Analysis and Modelling of VoIP Traffic,
Proc. of NETWORKS 2004,
Vienna, Austria, June 13-16, 2004.
[5] Leland, W.E., Taqqu, M.S., Willinger, W., Wilson, D.V.,
On the self-similar nature of Ethernet traffic (ext.vers.),
IEEE/ACM Transactions on Networking (TON),
Vol. 2, Issue 1, February 1994,
ISSN:1063-6692.
[6] Z. Gál, Gy. Terdik, E. Igloi,
Multifractal Study of Internet Traffic,
2000 WSES International Conference on
Applied and Theoretical Mathematics,
Vravrona, Greece, December 1-3, 2000.
http:/www.worldses.org
[7] Gál Zoltán, Balla Tamás,
A QoS infokommunikációs alkalmazásokra
kifejtett hatása,
Híradástechnika, 2007/4, pp.7–16.

Polifonikus zenei felvételek hangjegy-alapú szétválasztása

ACZÉL KRISTÓF, VAJK ISTVÁN

BME Automatizálási és Alkalmazott Informatikai Tanszék
{aczelkri, vajk}@aut.bme.hu

Lektorált

Kulcsszavak: polifonikus zene, szeparáció, hanglenyomat, energiaelosztás

Egy polifonikus zenei felvétel szétválasztása külön szólamokra igen nagy kihívást jelent. A több külön sávból kevert jelből tökéletesen visszaadni az eredeti jeleket a mai technikákkal lehetetlennek tűnő feladat. A cikk egy új módszert mutat be egycsatornás (mono) felvételek szeparációjára. Egy rendszerarchitektúrát javaslunk, amely a hiányzó információt valódi hangszermintákkal pótolja, így lehetővé téve egyes megismételhetetlen felvételek szeparációját és javítását.

1. Bevezetés

Ha képesek lennénk már létező, felvett polifonikus felvételek zenei szerkezetét változtatni, javítani, az új ajtókat nyitna a hangfeldolgozás területén. Egy felvétel szólamokra bontásával képesek lehetnénk kijavítani hibás hangokat, vagy egyszerűen megváltoztatni egy dallamot egy többszólamú műben. Az alapprobléma abban rejlik, hogy bár egy zeneművet lehetséges több mikrofonnal felvenni, ez azonban csak néhány területen (főként könnyűzene) bevett gyakorlat. Általánosságban pedig a többsávos hanganyagot is sztereo csatornába keverik, amely gyakorlatilag lehetetlenné teszi az utólagos módosítást. E lépés után a zene egyes hangjai különkülön nem módosíthatóak, csupán a felvétel egésze változtatható különböző szűrők segítségével. Kutatásunk hibás zenei felvételek szólamainak javítását tűzte ki hosszú távú célként, jelentse ez hangok frekvencia- vagy időbeli változtatását.

Kutatásunk során egy olyan rendszert fejlesztettünk ki, mely tetszőleges zenei hang elkülönítését teszi lehetővé a felvétel többi részétől. A zenei hangokat a felhasználó választhatja ki, a felvétel többi szólamának egymástól való elkülönítése nem célunk. Ez a megközelítés különösen alkalmas a már említett javítások támogatására.

A minél magasabb hangminőség elérése érdekében gyengébb automatizáltságot is megengedünk. Mivel megbízható automatikus kottázó algoritmusok ma még nem léteznek, munkánkban jelentős mértékű segítséget várunk el a felhasználótól, amely főképp a kotta bevitelénél jelentkezik. Nem teszünk továbbá túlzottan erős megkötéseket a rendszer futási idejét illetően sem.

A szeparációnál nagy szükség van kiegészítő információkra a puszta felvétel hanghullámán kívül. A problémát az okozza ugyanis, hogy az információ, amelyet szeretnénk kinyerni a felvételből, egyszerűen nincs benne a jelben. A problémával rengeteg kutatás foglalkozott. Az egyik ígéretes területet a modellalapú rendszerek képviselik. Itt a bemeneti jelek parametrikus modelljét állítják fel, amely a kimeneti jelre kényszerként szolgál.

A modell paramétereit a mixtúrából nyerik. A terület két fő ága a szabályalapú algoritmusok [1], amelyek implicit előzetes információ alapján építik fel a modellt és a Bayes-becslésen alapuló rendszerek [2], ahol az előzetes információt valószínűségeloszlás-függvényekkel explicit megadják. Zenei alkalmazásokban legelterjedtebb megközelítés a szinuszos modellezés, amely harmonikus hangszerek, valamint beszéd szeparációjához igen jól alkalmazható [3].

A felügyelet nélküli tanuláson alapuló módszerek [4-6] általában egyszerű, nem paraméteres modellt használnak és kevésbé függenek az eredeti hangforrásokról rendelkezésre álló információktól. A mixtúrából közvetlenül próbálnak meg információt kinyerni olyan információelméleti alapelvek alapján, mint például a források statisztikai függetlensége. A legismertebb módszerek a független komponens analízis (ICA), nemnegatív mátrix faktorizáció (NMF) és a sparse coding. Ezen algoritmusok a hang spektrogramját (vagy egyéb hasonló reprezentációját) faktorizálják elemi komponensekre, amelyek a klaszerizáció követ, felépítvén a kimeneti jeleket az elemi komponensekből.

Ezen cikkben modellalapú rendszert javaslunk a problémára. Ennek globális architektúráját megadjuk, majd ennek részeit külön bemutatjuk. Ismertetjük a felállított modellt, a *hanglenyomatot* (Instrument Print), valamint az Egyszerűsített Energia Elosztás (Simplified Energy Split, SES) módszerét, amely a felvétel energiáját szétosztja a kimeneti csatornák között. A rendszer lehetővé teszi azonos alapfrekvencián szóló hangok elkülönítését is, míg erre a legtöbb módszer nem képes.

2. A szeparáció folyamata

A szeparációs rendszer frekvenciatartományban működik, ezért transzformációra van szükség a be- és kimeneteken. A szokásos STFT mellett a Brown-féle frekvenciabecslő módszert is alkalmazunk [7], amely a szokványos STFT alapú spektrogramnál jóval pontosabb képet biztosít. A módszert bővebben a [8] tárgyalja.

A rendszer két módban képes működni. Az első mód a *hanglenyomat vételezés*. Itt valódi hangszerek hangmintáját olyan reprezentációban tároljuk el, amely később a szeparációnál hasznos lesz. A hangszermintára javasolt modellünk a *hanglenyomat*, amely a hangminták bandogram alapú leírásán alapszik [8]. A bandogram hasonló egy spektrogramhoz, annak frekvenciasávok szerint vett összegzésével kapható. A szétválasztáshoz a felvételben szereplő hangszerek bandogramjára lesz szükségünk.

Az *1. ábra* a hanglenyomat vételezés folyamatát mutatja be, míg a jelöléseket az *1. táblázat* foglalja össze. Mindezt bővebben a 3. szakaszban tárgyaljuk.

A második működési mód a *szeparációs* mód, amelyet a *2. ábra* vázol. A három bemeneti jel, az eredeti felvétel, a kotta és a hanglenyomatok alapján ez végzi el az egyes hangok külön sávokba való elválasztását. A rendszer két nagy blokkját különböztetjük meg: az Egyszerűsített Energia Elosztót (SES) és a lebegés helyreállítást. A SES tekinthető a legfontosabb modulnak, melynek feladata a felvétel energiájának szétosztása a kimeneti csatornák között. A SES által létrehozott kimeneteket gyakran lebegés terheli. Ez a lebegés ugyan már az eredeti felvételben is jelen volt, de a különválasztott hangokat meghallgatva sokkal észrevehetőbb és zavaró lehet. A jelenség csökkentését célozza meg a lebegés helyreállítás. Ezekről részletesebben az 5. szakaszban szólunk.

W	*Egyszerű hullámforma*
F	*Frekvenciabecsült spektrogram:* Az STFT $c_{k,t}$ amplitúdói és $\varphi_{k,t}$ fázisai mellett az $f_{k,t}^{true}$ valódi frekvenciát is tartalmazza a mintavételi pontokhoz.
B	*Bandogram:* Alsávokon összegzett spektrogram. A mintavételi pontok energiáját és fázisát külön nem, csak amplitúdóik összegét tartalmazza az egyes sávokban.

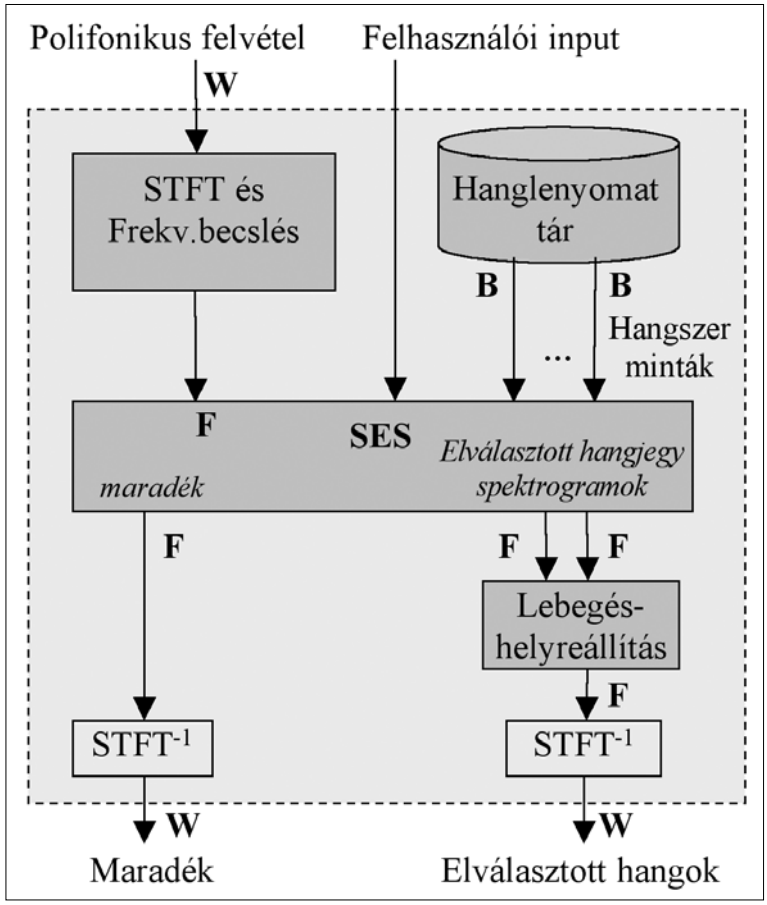
1. táblázat
Jelölések a szeparációs rendszer blokkdiagramjához

3. Hanglenyomatok

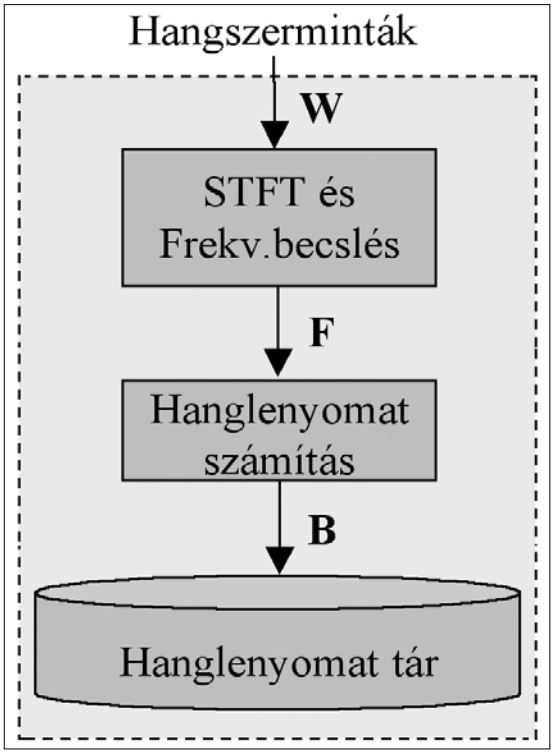
Mind a mai napig nem ismerjük teljes mértékben az emberi hallás folyamatát. Számtalan kutatás során arra a következtetésre jutottunk, hogy agyunk valószínűleg a hangszerek valamiféle emlékét őrzi [9]. Ez a pluszinformáció segít minket a dallamok felismerésében. Jelen esetben a szeparáció során plusz információra lesz szükségünk. Ezért megpróbáljunk a természetet lemásolni és utánozni az agy feltételezett működését. Hanglenyomatainkat ennek szem előtt tartásával készítjük el.

Az itt javasolt hangszermodell, a *hanglenyomat* egy hangszer különböző frekvenciákkal és intonációkkal (fuvola fújásának erőssége, zongoraleütés ereje, hang melegsége stb.) előadott mintáinak összessége. Egy lenyomat több ortogonális intonáció-dimenziót is tartalmazhat egyszerre, attól függően, mennyire „szabadon” játszha-

2. ábra
A szeparációs fázis blokkdiagramja



1. ábra
A hanglenyomat vételezés blokk diagramja



tó az illető hangszer. Elképzelhető például egy hangerő- és egy melegség- dimenzió is szaxofon esetén, amelyek értékei 1-10-es skálán mozoghatnak. A dimenziók általában nem írhatók le matematikai kifejezésekkel, inkább csak szubjektív szavakkal. Röviden tehát egy lenyomat egy mintakollekció különböző f_0 alapfrekvenciákon és $\underline{\mathbf{M}} = [m_1, m_2, \ldots m_p]$ intonációkkal. Ez a következő függvénnyel szemléltethető:

$$\underline{\mathbf{A}}(\underline{\mathbf{M}}, f, f_0, t) \tag{1}$$

ahol $t, m_x, f_0 \in \mathrm{R}^+$,
$0 < m_x < m_{x,max}$,
$0 \le t < \infty$,
$0 < f, f_0 \le 20000 Hz$.

A függvény azt mutatja, hogyan változik egy f_0 alapfrekvenciájú $\underline{\mathbf{M}}$ intonációjú hang energiája az idő múlásával különböző f frekvenciákon.

A valóságban megelégszünk azzal, hogy frekvenciasávokra tároljuk az ott megjelenő energia összegét. Ezt nevezzük *bandogram*-nak. A frekvenciasávok szélessége logaritmikusan nő magasabb frekvenciák felé. A bandogramot egy hang spektrogramjából az 1. táblázat jelöléseit használva így számolhatjuk:

$$A_{\mathbf{M},f_0,b,t} = \sum_{\rho(f_{k,t}^{true}, f_0, b)} c_{k,t}\ , \tag{2}$$

ahol $c_{k,t}$ és $f_{k,t}^{true}$ a k-ik komponens amplitúdója és becsült valódi frekvenciája, $\rho(f, f_0, b)$ kifejezés igaz, ha f és f_0 pontosan b sávnyi távolságra vannak, és b jelöli a frekvenciasávot:

$$b = \left\lfloor \log_{\sqrt[R]{2}} \frac{f_0}{f_{k,t}^{true}} \right\rfloor . \tag{3}$$

R a frekvenciasávok szélességét meghatározó kísérleti érték, a sávok száma oktávonként, t pedig idő. Kísérleteink alapján R=12 megfelelő felbontást nyújt, miközben egyszerűen elképzelhető, mivel egy zenei oktáv 12 félhangból áll. A valóságban természetesen nem tárolhatjuk az összes lehetséges mintát. A hiányzó minták interpolálással nyerhetők.

4. A szeparációs probléma

Mivel a szeparációs probléma megoldása igen nehéz, egyszerűsítést javaslunk, amely a némi minőségromlás árán egyszerűbb megoldást kínál a problémára. Jelölje $\underline{\mathbf{c}}_{r\tau} = \left\{ c_{r\tau,k} \cdot e^{\gamma_{r\tau,k}} \right\}$ a felvétel spektrumát $r\tau$ időben ($r \in \mathbf{N}$), $\underline{\mathbf{s}}_{i,r\tau}^{orig} = \left\{ s_{i,r\tau,k}^{orig} \cdot e^{\sigma_{i,r\tau,k}} \right\}$ és $\underline{\mathbf{d}}_{r\tau} = \left\{ d_{r\tau,k} \cdot e^{\delta_{r\tau,k}} \right\}$ pedig az eredeti i-ik hang spektrumát, valamint a zajkomponenst.

A szeparációs egyenlet a következő:

$$\underline{\mathbf{c}}_{r\tau} = \sum_{\forall i} \underline{\mathbf{s}}_{i,r\tau}^{orig} + \underline{\mathbf{d}}_{r\tau}\ , \tag{4}$$

ahol $c_{r\tau,k}, s_{i,r\tau,k}^{orig}, \sigma_{i,r\tau,k}, \gamma_{r\tau,k} \in \mathrm{R}^+$.

Mivel (4) egyenletrendszer további megkötések nélkül nem oldható meg, egyszerűsíteni próbáljuk olyan módon, hogy az ezáltal okozott minőségromlás minél kevésbé legyen érzékelhető. Korábbi kutatások [10-12] azt mutatták, hogy az emberi fül rendkívül érzéketlen a hangok fázisinformációjára, feltéve, hogy a fázisfolytonosság fennáll az egymást követő keretek között. Ez alapján (4) oly módon módosítható, hogy kiküszöböljük az ismeretlen $\sigma_{i,r\tau,k}$ és $\delta_{r\tau,k}$ fázisokat:

$$\gamma_{r\tau,k} = \sigma_{i,r\tau,k} = \delta_{r\tau,k}\ . \tag{5}$$

Ezáltal (4) a következőképp alakul:

$$\left| c_{r\tau,k} \right| = \sum_{\forall i} \left| s_{i,r\tau,k} \right| + \left| d_{r\tau,k} \right|, \tag{6}$$

ahol keressük $|s_{i,r\tau,k}|$ és $|d_{r\tau,k}|$ értékeket minden $i,r\tau,k$-ra, ha $|c_{r\tau,k}|$ és $\gamma_{r\tau,k}$ ismert.

Az egyszerűsítés hátránya némi minőségromlásként jelentkezik. A közeli frekvencián megszólaló hangok által okozott lebegést a módszer nem kezeli direkt módon. Ezért ezzel később külön kell foglalkoznunk.

5. Az Egyszerűsített Energia Elosztás módszere

Ez a fejezet a szeparáció fő algoritmusával, a SES-sel foglalkozik. Ennek feladata a felvétel energiájának elosztása a kimeneti hangok között. A SES a megfelelő hanglenyomatokat használja az energia elosztására, amely a felhasználó által megadott kotta, hangerő és hangszertípus információk alapján kerül kiválasztásra.

A szétválasztásra a következő iteratív algoritmust javasoljuk. Kiindulunk az eredeti felvétel $\underline{\mathbf{c}}$ spektrogramjából, tartozik továbbá minden kimeneti hanghoz egy $\underline{\mathbf{s}}_i$ spektrogram, energiájuk kezdetben nulla. Minden lépésben a felvétel spektrogramjából valamekkora energiát áthelyezünk az egyes kimeneti spektrogramokba a megfelelő frekvenciasávokban. Ezen energia nagysága a minták által indokolt energia egy előre meghatározott δ töredéke. Ha a felvétel már nem tartalmaz elegendő energiát, akkor a teljes maradék energiát áthelyezzük.

δ számítása:

$$\delta = \frac{A_{i,\mathbf{M}_i,f_{0,i},b}(r\tau - T_{onset,i})}{\sum_{\rho(f_{k,r\tau}^{true}, f_0, b)} c_{[j,i],r\tau,k}} \cdot \frac{1}{J}\ . \tag{7}$$

Egy lépés állépésekből áll, pontosan annyiból, ahány kimeneti hangunk van. Egy állépésben csak egyetlen kimenethez helyezünk át energiát. A d-ik lépés i-ik állépésében a felvétel energiája

$$c_{[j,i+1],r\tau,k} = \begin{cases} \rho(f_{k,r\tau}^{true}, f_0, b): & \max\left(0, (1-\delta) \cdot c_{[j,i],r\tau,k}\right) \\ \text{egyébként:} & c_{[j,i],r\tau,k} \end{cases} \tag{8}$$

Az i-ik hang aktuális energiája pedig:

$$\underline{\mathbf{s}}_{i,[j+1],r\tau} = \underline{\mathbf{s}}_{i,[j],r\tau} + (\underline{\mathbf{c}}_{[j,i-1],r\tau} - \underline{\mathbf{c}}_{[j,i],r\tau})\ . \tag{9}$$

A módszert azért kell több lépésben végrehajtani, mert előfordulhatna, hogy miután egy erősebben megszólaló hangszer kimeneti spektrogramjába energiát helyeztünk át, az eredeti felvétel energiája nullára csökken, más hangszereket „kiéheztetve". Ha minden lépésben csak a hanglenyomatok által indokolt energia töredékét helyezzük át, ez a jelenség kiküszöbölhető. Az algoritmus így az energia igazságos szétosztását biztosítja a kimeneti hangok között. Pontos működéséről bővebben korábbi publikációink számolnak be [8].

A felvételben fellépő lebegések a szétválasztás után sokkal jobban kihallhatók. A jelenség utófeldolgozással azonban javarészt kiküszöbölhető. A hanglenyomatokat az elkülönített hangokkal összevetve ugyanis a kioltási helyek megtalálhatók és visszaerősíthetők.

6. Teszteredmények

A rendszer minőségét szintetikus tesztekkel ellenőriztük. Tesztrendszerünket a *3. ábra* szemlélteti. A mérésekhez az Iowai Egyetem hangszer adatbázisából [13] származó 3841 db hangszermintát (vonós, fúvós, pengetős és billentyűs) használtuk.

A teszt során véletlenszerűen választottunk néhány hangot. Ezekből hanglenyomatot készítettünk. Ezután a hangokat egy felvételbe kevertük és a szeparációs rendszerrel újból szétválasztottuk. 2-10 polifóniafokú mixtúrákkal teszteltünk, egy szinten 50 tesztet végezve. A kimeneti hangokat az eredetihez hasonlítottuk, melyhez kétféle mértéket alkalmaztunk.

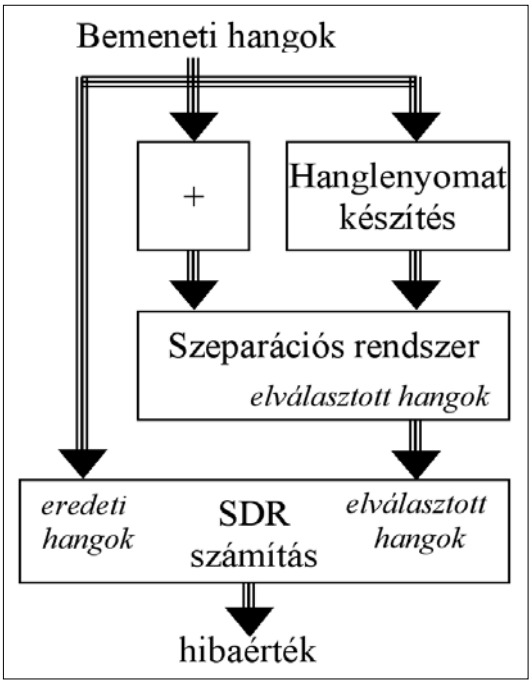
Az első mérték az úgynevezett Signal-To-Distortion Ratio. Az eredeti jeleket a kimeneti jelekből időtartományban kivonjuk és az így kapott hullámok energiáját hasonlítjuk az eredetikhez:

$$SDR_i = 10\log_{10}\frac{\sum_n \tilde{s}_i^{orig}(n)^2}{\sum_n\left[\tilde{s}_i(n)-\tilde{s}_i^{orig}(n)\right]^2}, \qquad (10)$$

ahol $\tilde{s}_i^{orig}$ az eredeti, $\tilde{s}_i$ pedig az elkülönített *i*-ik hang hulláma. A másik mérték hasonló elv alapján frekvenciatartományban mér:

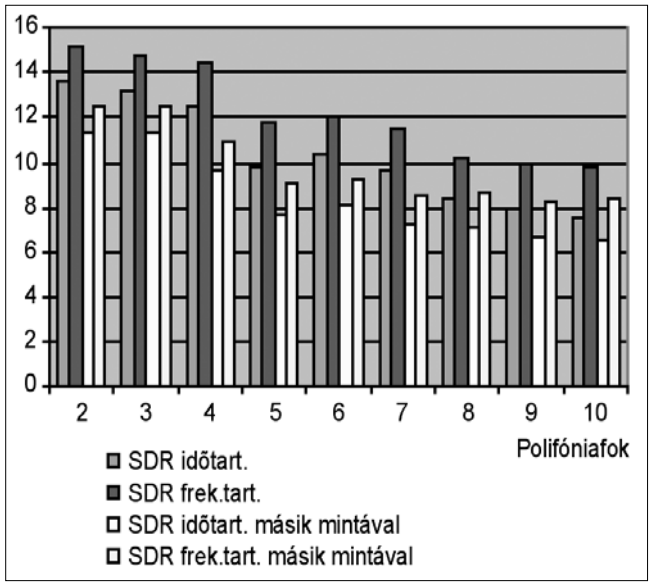
$$SDR_i^F = 10\log_{10}\frac{\sum_{\forall r\tau}\sum_{k=0}^{K} s_{i,k}^{orig}(r\tau)^2}{\sum_{\forall r\tau}\sum_{k=0}^{K}\left[s_{i,k}(r\tau)-s_{i,k}^{orig}(r\tau)\right]^2} \qquad (11)$$

Az eredményeket a *4. ábra* szemlélteti. Két konkurens hang esetén 15 dB a rendszer teljesítménye, amely lassan csökken a polifóniafok növekedésével.



3. ábra A tesztrendszer

A polifóniafok mellett a másik minőséget befolyásoló fő tényező a lenyomatok minősége. Kísérleteinket úgy is elvégeztük, hogy a felvételeket azonos típusú, de nem ugyanazon hangszer lenyomatai segítségével választottuk szét (például más gyártmányú zongora mintáit használva). Ebben az esetben a szétválasztás minősége átlagosan 2 dB-lel alacsonyabb volt.



4. ábra Teszteredmények

7. Összefoglalás

Kifejlesztettünk egy módszert, mely képes zenei hangok elkülönítésére polifonikus felvételben hanglenyomatok segítségével. Bemutattuk a rendszer architektúráját, majd a részleteit is kifejtettük. Egyszerű modellt ajánlottunk hanglenyomatok tárolására és az SES módszert javasoltuk a felvétel energiájának elosztására.

A rendszer minőségét teszteredményekkel szemléltettük. 2 polifóniafokú felvételek esetén a rendszer 15 dB felett teljesít, mely érték folyamatosan csökken, ahogyan a polifóniafok nő. Ez hasonló rendszerekkel összevetve igen magas érték.

A szintetikus teszteredmények, valamint néhány valós felvétel szétválasztott szólamai meghallgathatók és letölthetők a következő helyről:

http://avalon.aut.bme.hu/~aczelkri/separation.

A szerzőkről

ACZÉL KRISTÓF a Budapesti Műszaki és Gazdaságtudományi Egyetem Műszaki Informatika szakán szerezte diplomáját 2004-ben. Jelenleg az egyetem Automatizálási és Alkalmazott Informatikai Tanszékén folytat PhD kutatást polifonikus zenei felvételek elemzése és manipulálása témakörében. Mindeközben a Nokia Research Center-ben, majd később a Nokia Siemens Networks-nél szoftver kutató mérnökként dolgozik, ahol főként kép- és dokumentummegosztó rendszerek tervezésében és fejlesztésében vesz részt.

VAJK ISTVÁN 1975-ben kapott villamosmérnöki oklevelet a Budapesti Műszaki Egyetem Villamosmérnöki Karán. 1977-ben egyetemi doktori, 1989-ben kandidátusi, 2007-ban pedig MTA doktora fokozatot szerzett. 1976-tól dolgozik a BME Automatizálási és Alkalmazott Informatikai Tanszékén. 1994-től a tanszék vezetője. Jelenlegi munkaköre egyetemi tanár. Fő kutatási területe: rendszeridentifikáció, irányításelmélet és alkalmazott informatika.

Irodalom

[1] Every, M.R., Szymanski, J.E., „Separation of synchronous pitched notes by spectral filtering of harmonics”. IEEE Trans. on Audio, Speech and Language Proc., Vol. 14, No.5, pp.1845–1856., 2006.

[2] Cemgil, A. T., „Bayesian Music Transcription”, PhD thesis, Radboud University Nijmegen, 2004.

[3] Virtanen, T., „Sound Source Separation in Monoaural Music Signals” PhD thesis, University of Kuopio, 2006.

[4] Mitianoudis, N., Davies, M.E., „Using Beamforming in the audio source separation problem”, 7th Int. Symp. on Signal Proc. and its Applications, pp.89–92., 2003.

[5] Smaragdis, P., Brown, J.C., „Non-Negative Matrix Factorization for polyphonic music transcription”, IEEE Workshop on Applications of Signal Processing to Audio and Acoustics, pp.177–180., 2003.

[6] Plumbley, M., Abdallah, S., Blumensath, T., Davies, M., „Sparse representations of polyphonic music”, EURASIP Signal Processing Journal, Vol. 86, No.3, pp.417–431., 2006

[7] Brown, J.C., Puckett, M.S., „A high resolution fundamental frequency determination based on phase changes of the Fourier Transform”, J. Acoust. Soc. Am., Vol. 94, No.2, pp.662–667, 1993.

[8] Aczél, K., Vajk, I., „Note separation of polyphonic music by energy split”, WSEAS International Conf. on Signal Processing, Robotics and Automation, pp.208–214., 2008.

[9] McAdams, S., „Recognition of Auditory Sound Sources and Events. Thinking in Sound: The Cognitive Psychology of Human Audition”, Oxford University Press, 1993.

[10] Zwicker, E., Flottorp, G., Stevens, S.S., „Critical band width in loudness summation”, J. Acoust. Soc. Am., Vol. 29, pp.548–557., 1957.

[11] Smith, S.W., The Scientist and Engineer’s Guide to Digital Signal Processing, California Technical Publishing, 1997.

[12] Edler, B., Purnhagen, H., „Parametric Audio Coding”, IEEE Int. Conf. on Communication Technology, Vol. 1, pp.614–617., 2000.

[13] The University of Iowa Musical Instrument Samples Database (2008.07.07), http://theremin.music.uiowa.edu

Hírek

Regionális Cisco Hálózati Akadémiát avattak a Pannon Egyetem Műszaki Informatikai Karán

Veszprémben 2001 áprilisában indult el a Cisco Hálózati Akadémia Program, amely az Egyetem hallgatóinak a magas színvonalú tudásátadás mellett órarendi keretek között biztosít lehetőséget a nemzetközi szinten elismert CCNA (Cisco Certified Network Administrator, azaz hálózati szakértő) képzés elvégzésére és az ezzel járó tanúsítvány megszerzésére.

A Műszaki Informatikai Kar fejlesztési stratégiájával összhangban, tudatos építkezéssel sikerült elérni, hogy az intézmény – közel fél év előkészítő munka után és négy új partnerintézmény bekapcsolódását követően – elnyerte a „Regionális Akadémia” státuszt. Az Akadémia így a korábbi feladatain túlmenően a csatlakozó partnerintézmények felé folyamatos szakmai támogatást és oktatói képzést is biztosít.

A Cisco Hálózati Akadémia keretében szerzett ismeretek széles körben alkalmazhatók, mivel a számítógép-hálózatok az élet minden területén egyre fontosabb szerepet töltenek be, így a megbízható szakemberek a legtöbb vállalatnál nélkülözhetetlenek. A képzés anyagát a számítógép-hálózatok tervezése, építése, menedzselése, valamint a hálózati szakértők által leggyakrabban használt eszközök használata képezi.

A hallgatók számára a megszerzett tudáson felül a képzés által nyújtott nemzetközi és OKJ-s tanúsítvány közvetlen versenyelőnyt jelent.

A Hálózati Akadémia kurzusai az elmúlt években magyar illetve angol nyelven egyaránt megjelentek a nappali és levelező tagozatos képzések választható tárgyai között, az érdeklődő hallgatók létszáma pedig évről évre folyamatosan nő. A fejlesztői munka eredményességét jól mutatja, hogy 2007-ben már a Műszaki Informatikai Kar bocsátotta ki a legtöbb CCNA tanúsítvánnyal rendelkező hallgatót Magyarországon. A 2007-ben oklevelet szerzett hallgatók száma 143 volt, az idei tanévben pedig újabb 138 hallgató iratkozott be a CCNA kurzusokra.

Egykapus mérési módszer
szemcsés és folyékony anyagok komplex anyagparamétereinek meghatározására

KÁROLYI GERGELY, JAKAB LÁSZLÓ, LÉNÁRT FERENC

BME Szélessávú Hírközlés és Elméleti Villamosságtan Tanszék
{karolyigergo, jaklac}@gmail.com, lenart@mht.bme.hu

Lektorált

Kulcsszavak: komplex permeabilitás, komplex permittivitás, CMPS, skaláris mérés, egykapus mérés, nanoferrit

A cikkben ismertetjük anyagok elektromos és mágneses anyagparamétereinek rádiófrekvenciás vizsgálatára kifejlesztett új mérési módszerünket (Complex Material Properties from Scalar data, CMPS). Részletesen bemutatjuk az egykapus eljárás alapelveit, majd mérési eredmények bemutatásával alátámasztjuk a módszer helyességét. A vizsgált anyagok komplex permittivitását és permeabilitását egyidejűleg lehet megkapni egy hálózatanalizátor és egy vezérlő, adatfeldolgozó szoftver segítségével. A méréshez tervezett koaxiális mintatartó kitűnően alkalmas folyékony és finom szemcsés anyagok vizsgálatára. A bemutatott eljárás egyik különleges előnye, hogy a komplex mennyiségeket skalár adatokból lehet származtatni, ami lehetővé teszi az algoritmus egyszerű, gazdaságos megvalósítását különböző célalkalmazások esetén. Emellett a vizsgált minta hosszának, vagyis mennyiségének az előzetes ismerete sem szükséges, ami tovább növeli a módszer alkalmazhatósági területeit.

1. Bevezetés

Az anyagok elektromágneses tulajdonságainak jellemzése mindig kulcsfontosságú területnek számított a mikrohullámú technikában. Állandó jelentőségét a technológia fejlődése adja; új anyagok fejlesztése folyamatosan zajlik és azok jellemzése elengedhetetlen az elektromágneses tulajdonságok tervezése szempontjából.

Az elmúlt évtizedekben számos kutatási eredmény látott napvilágot ezen a területen, különböző elméleti alapokra támaszkodva. Az elektromágneses paraméterek nagy pontosságú meghatározásához általában rezonáns mérési módszereket alkalmazhatunk, amelyekkel diszkrét frekvenciákon kaphatjuk meg a kívánt jellemzőket. Amennyiben a mérési pontossággal szemben alacsonyabbak az elvárásaink, úgy szélessávú mérési technikákat érdemes alkalmazni, hogy az anyagparamétereket egy folytonos spektrumon ismerhessük meg. Ezeket a szélessávú módszereket négy nagy csoportba sorolhatjuk aszerint, hogy a frekvencia, vagy az időtartományban vizsgálódunk, illetve hogy egy-, vagy kétkapus mérést valósítunk meg. Egykapus mérési módszerekre az [1] és [2] irodalmakban találunk példákat, míg kétkapus eljárásokat a [3-5] mutatnak be.

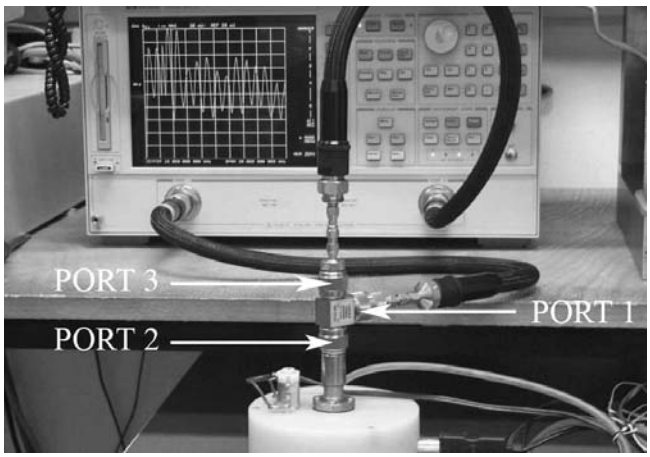
Általánosan elmondható, hogy az egykapus mérésekkel csak egy elektromágneses anyagparamétert – tipikusan a permittivitást vagy a permeabilitást – tudjuk egyidejűleg meghatározni. Ezzel szemben kétkapus elrendezéssel lehetőség nyílik a két paraméter szimultán kinyerésére. A hetvenes évek elején hozta nyilvánosságra Nicolson és Ross mérési módszerüket [6], amelyet Weiss kiegészítése nyomán NRW algoritmusnak nevezünk és mára ez vált a leggyakrabban használt eljárássá anyagok szélessávú elektromágneses paramétereinek a meghatározására.

Az algoritmus az egy-, vagy kétkapu szórási mátrix elemeinek (S-paraméterek) a meghatározásán alapul, és az anyagjellemzőket ezekből származtatja. Később az eljárásnak számos változata jelent meg, mégis vannak olyan esetek, amikor ezt a módszert csak nehézkesen, vagy egyáltalán nem tudjuk alkalmazni. Ilyen eset például, amikor alacsony veszteségű és/vagy nem szilárd anyagokat szeretnénk vizsgálni.

Cikkünkben egy egykapus mérési eljárást mutatunk be, amellyel lehetséges a vizsgált anyagminták komplex permittivitásának és permeabilitásának az egyidejű meghatározása. A mérési módszer neve *„Complex Material Properties from Scalar data”* (CMPS), amely kifejlesztéséhez a széleskörűen használt, úgynevezett *„Distance-To-Fault”* (DTF) eljárás – amely kábelhibák lokalizációjára szolgál – adta az alapötletet. Mérési módszerünk a minta végein létrejövő impedancia-diszkontinuitásokon ébredő reflexiók detektálásán alapszik. Az eljárást 7/3 mm-es koaxiális tápvonal használatával, TEM típusú terjedésre fejlesztettük ki, de különösebb elvi nehézségek nélkül átültethető bármilyen más tápvonaltípusra. Mivel a mintatartó tápvonaldarab rövidzárban végződik, így az kitűnően alkalmas folyékony, vagy porszerű anyagok vizsgálatára.

Egy HP8722D típusú hálózatanalizátort használtunk a frekvenciában sweepelt jel előállítására, valamint a később bemutatásra kerülő mérési összeállítás átvitele abszolútértékének ($|S_{21}|$) mérésére a 2-17 GHz tartományban. A műszer vezérlése, a mérési eredmények rögzítése, valamint azok feldolgozása egy HP VEE környezetben fejlesztett programmal történt. Az algoritmus elkülöníti a levegő-minta és a minta-rövidzár határfelületekről érkező reflexiókat, majd a komplex anyagparamétereket ezekből származtatja.

Az új algoritmus helyes működését egy elektromágneses szempontból ismert referenciaanyag (parafinolaj), valamint egy kísérleti ferrit por mérési eredményeivel támasztjuk alá. A bemutatott mérési elrendezéssel, és a hozzátartozó vezérlő és jelfeldolgozó programmal



1. ábra
Mérési összeállítás:
HP8722D hálózatanalizátor, mérőkábelek, teljesítményosztó és mintatartó

lehetővé válik anyagok elektromágneses paramétereinek gyors és szélessávú mérése.

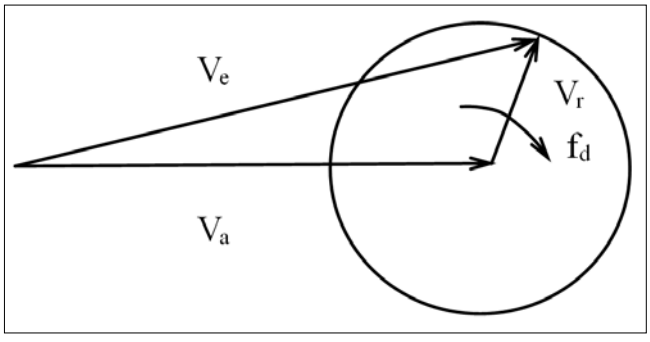
A következő részben bemutatjuk az eljárás elméleti hátterét, ezt követi a mérési eredmények ismertetése, valamint azok értékelése.

2. Elméleti összefoglaló

A mérési összeállítás az *1. ábrán* látható. A mintatartó egy 3 dB-es osztón keresztül csatlakozik a hálózatanalizátorhoz. A generátor a teljesítményosztót egy lineárisan sweepelt jellel gerjeszti az első kapun keresztül. A beeső teljesítmény – melyet az f_a pillanatnyi frekvencia jellemez – egyik fele a 2. kapun át a mintára jut, másik fele pedig a 3. kapun keresztül a detektorra kerül. A mintáról reflektálódott jel – melyet az f_r pillanatnyi frekvencia jellemez – egyik fele ugyancsak a detektorra jut, a másik fele pedig disszipálódik a generátoron. A detektorra került jelek összeadódnak, ami jól szemléltethető az f_a és f_r pillanatnyi frekvenciájú jelekhez rendelt komplex V_a és V_r vektorok segítségével.

A *2. ábra* mutatja a két vektort, illetve vektoriális eredőjüket, V_e-t, mely f_d különbségi frekvenciával forog V_a körül, akárcsak V_r.

2. ábra
Vektorábra az adott (V_a), a reflektált (V_r) és az összeg (V_e) vektorokkal.
V_e és V_r a különbségi frekvenciával (f_d) forognak V_a körül.



[7] alapján a különbségi frekvencia a következőképp adható meg:

$$f_d = f_a - f_r = \frac{B}{T} \cdot \tau \qquad (1)$$

ahol B a sweepelésnél alkalmazott sávszélesség, T a sweepelés időtartama, τ a reflektált hullám időbeli késése az adott jelhez képest. A hálózatanalizátor V_e abszolútértékét méri időtartományban. A komplex elektromágneses anyagjellemzők ebből az adatsorból származtathatók.

A jelfeldolgozás folyamata a következő: először meghatározzuk egy hitelesített rövidzárral lezárt tápvonal esetére a $V_{r1}(t)$ függvényt. Az *FMCW (Frequency Modulated Continuous Wave)* gerjesztőjel használata következtében a frekvencia és az időtartomány között kölcsönösen egyértelmű megfeleltetés áll fenn, így megkapjuk $V_{r1}(f)$-et. A következő lépésben a vizsgált mintát mérve kapjuk $V_{r2}(f)$-et, majd a két függvény segítségével már számolhatóvá válik a reflexiós együttható, $\Gamma(f)$.

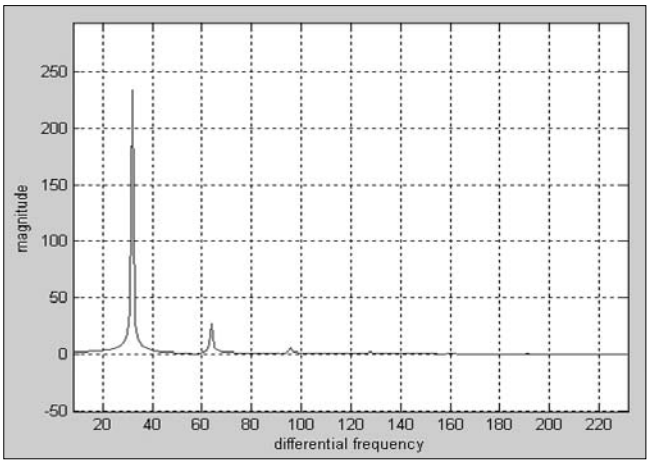
Mivel reflexiót jellemzően a minta elejéről és végéről várunk, ezért két reflexiós együttható-görbét kapunk, melyek segítségével a komplex anyagjellemzők már egyszerűen számíthatóak. Így tehát a feladat a $V_r(t)$ függvények kinyerése a mért adatokból. Fontos itt megjegyezni, hogy bár t az időváltozót jelöli, a $V_r(t)$ egy komplex értékű függvény, hiszen egy vektor mozgását képezi le, a komplex burkoló elnevezéssel fogunk rá hivatkozni. V_r-rel a vektor egy adott időpillanatban felvett értékét jelöljük.

Tekintsük most a háromszöget, melyet a vektorok alkotnak a *2. ábrán!* A következő kifejezés adható $|V_e(t)|$ értékére a koszinusztétel segítségével:

$$|V_e(t)| = \sqrt{|V_a(t)|^2 + |V_r(t)|^2 - 2 \cdot \cos(2\pi f_d)|V_a(t)||V_r(t)|} \qquad (2)$$

Az egyszerűbb analízis kedvéért tételezzük fel, hogy $|V_a(t)|$ és $|V_r(t)|$ is állandó. Ekkor (2) amplitúdó-spektruma a *3. ábrán* látható módon alakul, elhanyagolva az egyenkomponenst.

3. ábra
A (2) kifejezés amplitúdóspektruma a DC komponens nélkül. Az ábra MatLab segítségével készült,
V_a=1, V_r=0.5 feltételezéssel.



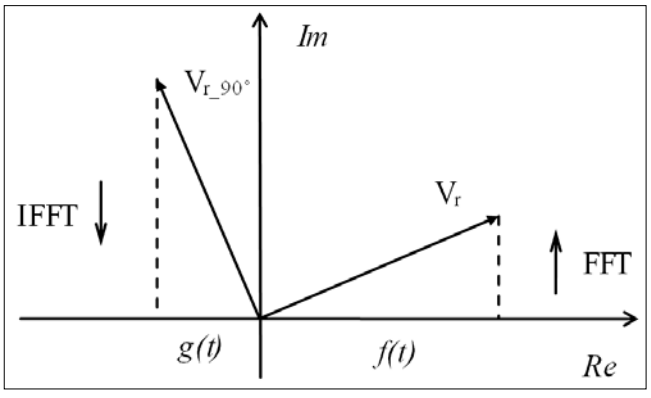
Kitűnik, hogy az alapharmónikus – mely természetesen megegyezik a különbségi frekvenciával – hordozza a jel energiájának döntő többségét (továbbra is elhanyagolva a DC-t). Így tehát az alapharmónikus, mint forgó vektor jó közelítéssel megegyezik V_r-rel. Másképp megfogalmazva eltekinthetünk a felharmónikusoktól. A 3. ábra megerősíti azt az állítást, mely szerint egy periódikus, m-szer deriválható függvény amplitúdóspektruma legalább $1/f^m$ mértékben tűnik el, f»1 esetén [8]. Jelen esetben m»1, miután $|V_e(t)|$ kvázi-szinuszos függvény. Az ábrán látható spektrumot különbségi-frekvenciás spektrumnak nevezzük.

Miután a V_a $|V_e(t)|$ kialakításában mint egyenkomponens vesz részt, kiszűrhető belőle. Ekkor egy olyan kvázi-szinuszos periódikus függvényt kapunk, melynek amplitúdója $|V_r|$, jelöljük a függvényt $f(t)$-vel (ennek spektruma látható a 3. ábrán). Ez azt jelenti, hogy a V_r hozzárendelhető $f(t)$-hez úgy, hogy a komplex síkon forgó vektor valós síkra eső vetülete előállítsa a függvényt. Fontos itt megjegyezni, hogy ekkor V_r forgása már nem egy állandó körfrekvenciájú forgás (bár csak kis mértékben tér el attól), illetve az egyenkomponens kifejezés szigorúan csak a különbségi frekvenciatartományra vonatkozik és nem a sweepelt (abszolút) frekvenciatartományra. Az előző bekezdésben elmondottakból következik viszont, hogy a kvázi-szinuszos jel alapharmónikusával jól közelíthetjük a V_r vektort. Így arra jutunk, hogy $V_r(t)$ közvetlenül megkapható $f(t)$ Fourier-transzformáltjából, csak az alapharmónikust figyelembe véve. Mindehhez a $|V_r(t)|$ = állandó feltételezéssel jutottunk. Továbbiakban azt az esetet tekintjük, amikor $|V_r(t)|$ nem állandó.

A fentiekből kiindulva a következőképpen lehet továbblépni: ha $|V_r(t)|$ időben változik, akkor az a spektrumban is változást okoz. Tekintsünk például egy exponenciális csillapodást, amelynek spektruma $1/f^2$ szerint csökkenő. Az exponenciális függvény (vagy tetszőleges egyéb) függvény és a periódikus függvény szorzata a különbségi frekvenciatartományban konvolúciót jelent, mely hatására az $1/f^2$-es spektrum (vagy a tetszőleges egyéb időfüggvény spektruma) megjelenik a felharmónikusok körül.

Figyelembe véve a kvázi-szinuszos függvény spektrumáról elmondottakat, állíthatjuk, hogy csak az alapharmónikus és annak spektrális környezete fogja döntően meghatározni $V_r(t)$-t. Így $f(t)$ FFT-vel előállított spektrumából kiemelve ezt a részt, a spektrumkomponensek vektori összege a $|V_r(t)|$ = állandó esethez hasonlóan jó közelítéssel a forgó V_r vektort fogja közelíteni. Látszik viszont, hogy most nem elég pusztán FFT-t alkalmazni, mert a spektrumból nem tudjuk közvetlen meghatározni a komplex burkolót.

4. ábra
A komplex vektorok és az időfüggvények kapcsolata. A nyilak mutatják a transzformációs irányokat.



Ezért vizsgáljuk meg a *4. ábrát*, mely a következőt mutatja: az FFT-vel előállított spektrum számunkra érdekes részét toljuk el 90 fokkal (vagyis V_r-t forgassuk el) és ezen a fázisban eltolt spektrumon alkalmazzunk egy IFFT-t. Ekkor megkapjuk $g(t)$-t (amely tehát V_r képzetes tengelyre eső vetülete) , majd $f(t)$ és $g(t)$ segítségével, vagyis két skalár (idő)függvénnyel meg tudjuk adni a komplex burkolót, $V_r(t)$-t.

Mint azt már említettük, két reflexiót használunk fel az anyagparaméterek meghatározásához: egyet a minta elejéről, egyet pedig a végéről. Itt felmerülhet a többszörös reflexiók kérdése: a minta – a generátorhoz viszonyított – távolabbi végén ideálisnak tekintett rövidzár található. Az erről visszaverődött jelnek egy része a minta-levegő impedancia diszkontinuitáson ismét reflektálódik, vagyis a minta két vége között a vizsgáló jel egy része úgymond „pattog". Amennyiben ezeket a többszörös reflexiókat nem tudnánk különválasztani, az nagyban meghamisítaná a mérési eredményeinket. A legtöbb ismert mérési módszernél – amelyek frekvenciatartománybeli méréseken (S-paraméterek) alapulnak – ez hibát is okoz. Ennek a hibának a mértéke a minta hosszától, valamint annak csillapítási tényezőjétől függ.

A bemutatott mérési módszernél két alapvető szempontot kell figyelembe venni: a minta maximális hossza olyan legyen, hogy a rövidzárról reflektálódó jelet tisztán detektálni lehessen (nagyobb csillapítású anyagoknál rövidebb minta), valamint a minimális mintahosszt úgy állítsuk be, hogy a minta elejéről és végéről érkező reflektált jelek szétválaszthatók legyenek.

Itt mutatkozik meg a CMPS eljárás egyik nagy előnye: az FMCW mérőjel használatával lehetőség nyílik a reflektált jelek idő-, vagy távolságtartományban történő szétválasztására. Ezt meg is teszi a kifejlesztett jelfeldolgozó program, amellyel ezután a minta elején és végén ébredő reflexiók abszolútértékéből meghatározzuk a komplex anyagjellemzőket.

A minta elején fellépő reflexióból a minta karakterisztikus impedanciája határozható meg (Z_0=*50 Ω, a tápvonal karakterisztikus impedanciája*) [9]:

$$Z = Z_0 \frac{1+\Gamma_{in}(f)}{1-\Gamma_{in}(f)} \tag{3}$$

A minta végén ébredő reflexió segítségével pedig a komplex terjedési együttható határozható meg: (4)

$$\gamma = j\omega\sqrt{(\varepsilon' - j\varepsilon'')(\mu' - j\mu'')} = j\omega/c\sqrt{\varepsilon_{rk}\mu_{rk}}$$

Végül a keresett komplex anyagjellemzők:

$$\mu_{rk} = \frac{Z(-jc\,\gamma/\omega)}{50} \qquad \varepsilon_{rk} = \frac{50(-jc\,\gamma/\omega)}{Z} \tag{5}$$

3. Mérési eredmények

A bemutatott mérési módszer alkalmazhatóságát az alábbiakban mérési eredményekkel igazoljuk. Ismertetjük a bevezetőben említett anyagok (parafinolaj és ferrit por) komplex anyagjellemzőit, név szerint a komplex permittivitást és permeabilitást. Az anyagokat a 2-17 GHz-es frekvenciatartományban jellemezzük. A felső frekvenciahatárt a mérési összeállítás alkotóelemei; a tápvonaldarabok, valamint a teljesítményosztó határozza meg.

A második részben ismertetett algoritmust, a mérésvezérlést, valamint az adatok gyűjtését egy HP VEE környezetben fejlesztett programmal valósítottuk meg. Az algoritmusban felhasznált referenciamérést a mintabefogó helyére illesztett rövidzárral végeztük, a műszert is erre a síkra hitelesítettük.

A *5. ábrán* bemutatott komplex permittivitást és permeabilitást a következő formában ábrázoljuk:

$$\varepsilon(\omega) = \varepsilon'(\omega) - j\varepsilon''(\omega) \quad (6)$$

$$\mu(\omega) = \mu'(\omega) - j\mu''(\omega) \quad (7)$$

ahol ε' és μ' a permittivitás és a permeabilitás valós, míg ε'' és μ'' a képzetes részei.

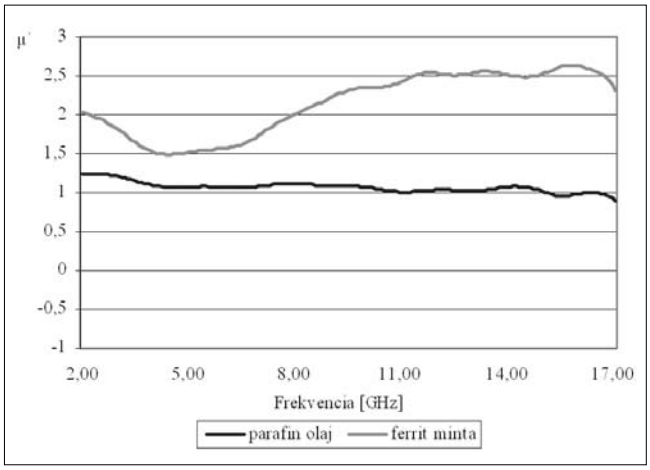
A referenciaként használt parafinolajról tudjuk, hogy dielektromos állandójának valós része 10 GHz-en 2 és 2,2 között van, mágneses szempontból pedig gyakorlatilag átlátszó, tehát, μ_r=1.

A *7. ábra* a permittivitás valós részét mutatja be. Látható, hogy a mérési eredmény jól megfelel a fent említett értéknek; a dielektromos állandó az egész frekvenciatartományon 2 közelében marad. A mágneses átlátszóságot mutatja az 5. ábra, ahol a permeabilitás valós része végig 1 körüli értéket vesz föl. Mivel a parafinolaj elektromágneses vesztesége igen csekély, a *6. és 8. ábrákon* látható permeabilitás és permittivitás képzetes részei valóságszerűnek tekinthetők.

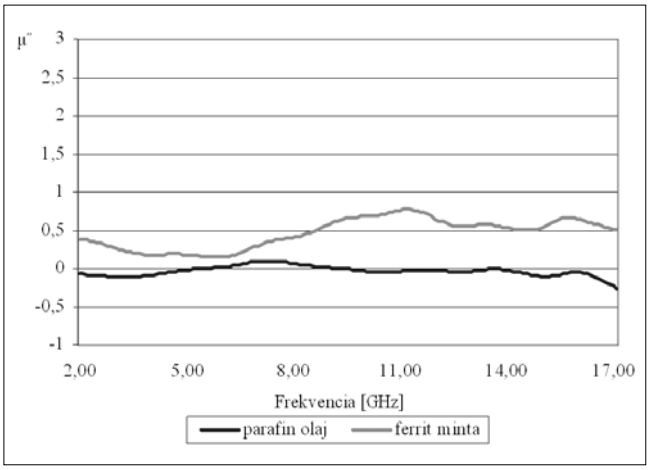
A mérési eljárás egyik fő előnye, hogy kitűnően alkalmazható porszerű, illetve folyékony anyagok vizsgálatára, így második tesztanyagnak az olaj mellé egy porszerű ferritmintát választottunk. Ez egy kísérleti anyag, így előzetes adatok – azon kívül, hogy az átlagos szemcseátmérő a mikronos tartományban található – nem álltak rendelkezésünkre.

A mért elektromágneses anyagparaméterek valós részei az *5. és 7. ábrákon* láthatók. A ferritminta mágneses permeabilitásának valós része a tekintett frekvenciatartományon 1,5 és 2,7 közötti értékeket vesz föl, a per-

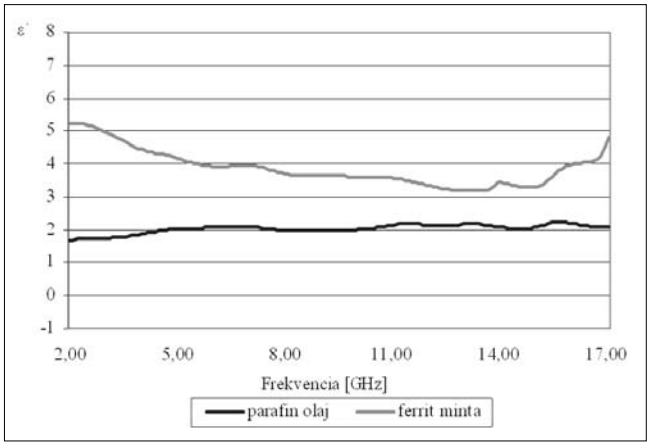
5. ábra
A két minta relatív permeabilitásának valós része



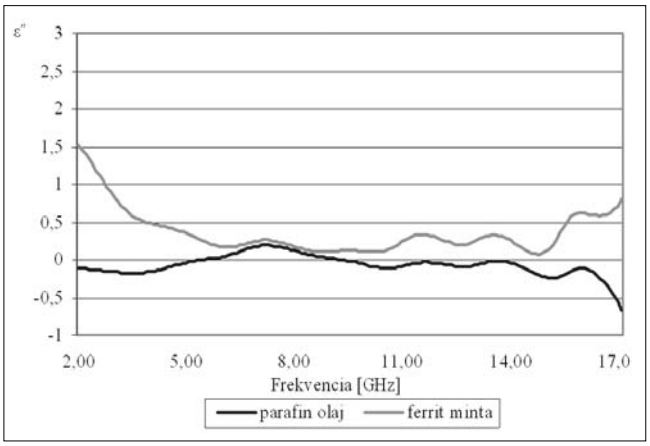
6. ábra
A két minta relatív permeabilitásának képzetes része



7. ábra
A két minta relatív permittivitásának valós része



8. ábra
A két minta relatív permittivitásának képzetes része



mittivitás valós része pedig 3 és 6 körül változik. Az anyag dielektromos és mágneses veszteségeit a *6. és a 8. ábrák* szemléltetik. Látható, hogy ezek 0 és 1 között változnak a 2-17 GHz-es frekvenciatartományon.

4. Összefoglalás

A közölt cikk fő célja, hogy bemutasson egy általunk újonnan kifejlesztett mérési eljárást, melynek segítségével anyagminták elektromágneses paramétereit lehet meghatározni. Az eljárás fő előnye, hogy lehetővé teszi szilárd, folyékony vagy porszerű minták komplex permittivitásának és permeabilitásának egyidejű meghatározását. A komplex értékek meghatározása skalár mennyiségek méréséből történik, ami különleges érdemeket kölcsönöz a módszernek.

Sok más eljárással szemben itt nem kell a mérés bizonytalanná válásával számolni azokon a frekvenciákon, amelyeknél a félhullámhossz a minta hosszának egész számú többszöröse. További előny, hogy a mérés elvégzéséhez nem szükséges a minta hosszának előzetes ismerete.

Irodalom

[1] C. C. Courtney, William Motil,
„One-Port Time-Domain Measurement of the Approximate Permittivity and Permeability of Materials,”
IEEE Trans. on Microwave Theory and Techniques, Vol. 47, No.5, May 1999.

[2] James Baker-Jarvis,
„Transmission/Reflection and Short-circuit Line Permittivity Measurements,”
National Institute of Standards and Technology, Issued July 1990.

[3] C. C. Courtney,
„Time-domain measurement of the electromagnetic properties of materials,”
IEEE Trans. on Microwave Theory and Techniques, Vol. 46, No.5, May 1998, pp.517–522.

[4] Ding Sun,
„Measurement of complex permittivity and permeability of microwave absorber ECCOSORB MF-190,”
Pbar note 576, Fermi lab, August 1997.

[5] Madhan Sundaram et al,
„Measurement of Complex Material Properties using Transmission/Reflection Method”,
SNS-CONF-ENGR-133.

[6] M. Nicolson, G. F. Ross,
„Measurement of the intrinsic properties of materials by time-domain techniques,”
IEEE Trans. Instrum. Meas., Vol. IM-19, Nov. 1970, pp.377–382.

[7] Jakab László, Károlyi Gergely:
„Nanoferritek anyagparamétereinek vizsgálata mikrohullámú tartományban”
TDK, 2006.

[8] Fodor György,
„Hálózatok és Rendszerek”,
ISBN 963-420-810 X, Műegyetemi Kiadó, Budapest, 2004, Ch.1.4, pp.204–221.

[9] Csernoch János,
„Komplex dielektromos állandó és komplex permeabilitás mérése mikrohullámú módszerekkel”,
Orion MFO 11., Budapest, 1969.

Introduction of electronic administration at the Hungarian National Communications Authority

Keywords: digital signature, frequency management, HNCA

The paper deals with the introduction of electronic administration in the frequency management of the Hungarian National Communications Authority. Introduces the issues related to the implementation of digital signatures, the operational process of the implemented system and the lessons learned from its operation.

Log analysis

Keywords: information technology, monitoring, log correlation analysis, forensics

Gathering and analyzing information is as old as human civilization. In our days computers revolutionized this process, yet they have also become the source of serious problems. To solve most of these problems, it is necessary to thoroughly analyze logs of processes and events of the information systems. Log analysis can provide the company management with further important information, with its help future trends may be predicted. IT systems however generate a vast amount of log information, the adequate analysis of which is impossible within normal operation. Thus several log analysis solutions appeared in the market, among which the log analysis service supported by human intelligence provides the greatest added value.

Planning of secure Wi-Fi networks

Keywords: Wi-Fi site survey, wireless controller, RF planning, WLAN security, EAP-TLS, Wi-Fi coverage

The increased use of mobile computers has entailed the large-scale penetration of wireless networks. When applying license-free wireless LAN frequencies in business networking, it is essential to use an adequate form of reliable security as well as the radio frequency preplanning and measurements. In this article we discuss the planning, measuring, implementing and supervising of a wireless LAN system on the example of a network system established in a multinational company environment.

Information technology in measurement systems at HNCA

Keywords: measurements, HNCA, measurement informatics

The authors present the challenges the Directorate of Measuring Affairs at the Hungarian National Communications Authority faces thus putting in perspective the complex IT systems that support their efficient and effective operation. They provide an overview of the current status of the systems, that of the development underway and planned, and also describe how the expected results can support the investments.

Bandwith management of NGN services in LAN/MAN environment

Keywords: NGN, TCP, UDP, codec, QoS, DiffServ, self similarity, wavelet, fractal, entropy

Strict QoS guarantees are required for NGN (Next Generation Network) networks. The DiffServ mechanism is applied mostly for classification of protocol data units of real time and conventional information streams in LAN/MAN environment. An interesting research question is the behaviour of VoIP traffic characteristics of the delay and the jitter sensitive IP telephony for different voice codecs. We analyze Ethernet traffic generated by G.711, G.723, G.728 and Wideband (G.722) voice codecs. The self similar, fractal and multifractal properties of popular TCP based services (http, ftp, telnet etc.) in LAN environment are well known for fifteen years. In this paper we study the effect of UDP based current voice mechanisms on the self similarity of the Ethernet data traffic. UDP traffic of the IP phones are evaluated in congested and congestion free environment respectively using sophisticated methods of entropy and wavelet analysis. The proposed evaluation method is applied to the characterization of VoIP traffic.

Note-based sound source separation of polyphonic recordings

Keywords: polyphonic music, separation, instrument print, energy split

Decomposing a polyphonic musical piece to separate instrument tracks has always been a challenge. Isolating the tracks is out of reach of today's technology. This article proposes a novel method for the separation of monophonic musical recordings. System architecture is given, that uses samples of real instruments for reinserting the missing data to the system, thereby allowing for the separation and correction of recordings that cannot be retaken.

One-port measurement method for determining complex parameters of materials

Keywords: complex permeability and permittivity, CMPS, scalar measurements, one-port measurement, nanoferrite

The paper presents a new measurement method developed by the authors for high frequency measurements of electric and magnetic parameters of materials called „Complex Material Properties from Scalar data". The specific advantage of the proposed method is that complex quantities can be obtained from scalar data which is important for its simple and economical implementation.

Summaries • of the papers published in this issue

Contents

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

Hirdetési árak
Belív 1/1 (205x290 mm) FF, 120.000 Ft + áfa
Borító II-III (205x290mm) 4C, 180.000 Ft + áfa
Borító IV (205x290mm) 4C, 240.000 Ft + áfa

Cikkek eljuttathatók az alábbi címre is
Szabó A. Csaba, BME Híradástechnikai Tanszék
Tel.: 463-3261, Fax: 463-3263
e-mail: szabo@hit.bme.hu

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

2008-as előfizetési díjak
Közületi előfizetők részére: bruttó 32.130 Ft/év
Hazai egyéni előfizetők részére: bruttó 7.140 Ft/év
HTE egyéni tagok részére: bruttó 3.570 Ft/év

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

www.hte.hu
Felelős kiadó: NAGY PÉTER
Lapmenedzser: DANKÓ ANDRÁS

HU ISSN 0018-2028
Layout: MATT DTP Bt. • Printed by: Regiszter Kft.