CSOMAGKAPCSOLT HÁLÓZATOKON NYÚJTOTT SZOLGÁLTATÁSOK MINŐSÉGBIZTOSÍTÁSÁNAK MÓDSZEREI ÉS METRIKÁI

a Ph.D. értekezés tézisfüzete

Varga Pál

Témavezetők:

Tatai Péter
és
Gordos Géza, DSc.

BUDAPESTI MŰSZAKI ÉS GAZDASÁGTUDOMÁNYI EGYETEM
TÁVKÖZLÉSI ÉS MÉDIAINFORMATIKAI TANSZÉK
2010.

1. fejezet

Bevezetés

A mai felhasználók a számítógép előtt ülve legtöbbször észre sem veszik, hogy hálózati szolgáltatásokat vesznek igénybe. A távoli szervereken futó alkalmazásokat úgy használják, mintha azok a helyi gépre lennének telepítve.

A szolgáltatói hálózat üzemeltetése és karbantartása az operátorok "rejtett" tevékenységei közé tartoznak. A hálózat- és szolgáltatás-menedzsment mindig is összetett feladat volt, még az operátorok saját hálózatán belül is. Több-operátoros környezetben a kielégítő szolgáltatás nyújtása igen nagy kihívás. Valós környezetben a felhasználó adatai számos operátor hálózatán haladnak keresztül, amíg elérik a kiszolgáló csomópontot.

A végponttól végpontig (end-to-end) történő szolgáltatásminőség-biztosítás megfelelő módszereket és mérőszámokat kíván annak érdekében, hogy időben felismerjük a hibákat és megtaláljuk azok okait. Az itt ismertetendő téziseim a hálózati szolgáltatások minőségbiztosításának témakörében mutatnak rá megoldandó problémákra és javasolnak azokra megoldásokat. A bevezetendő szolgáltatásminőség-biztosítási keretrendszer beleillik a tudományterület jelenlegi fejlődési irányába, segítségével az operátorok minden hálózati és szolgáltatás-felügyeleti igényüket kielégíthetik. A keretrendszer bevezetése mellett új vizsgálati módszereket és minősítő metrikákat is bemutatok.

A disszertáció új eredményei a következőkben mutatkoznak meg: az aktív és passzív hibamenedzsment módszerek integrálása; a tradicionális Quality of Service (QoS) mércék továbbfejlesztése; valamint a felhasználói elégedettség (Quality of Experience, QoE) korrelálása a maghálózati mérési eredmények kiértékelésével. Mindezeken túl az új mérési és kiértékelési módszereket beillesztettem egy jelenlegi autonóm hálózati menedzsment koncepcióba is, mely bevezeti a hálózati tudás-sík fogalmát.

A disszertációm a hálózat- és szolgáltatásminőség-biztosítás mérési módszereire és metrikáira, valamint a hálózat- és szolgáltatás-menedzsment vizsgálati eredményeinek kiértékelésére összpontosít.

A 2. fejezetben a kutatási célokat mutatom be, a 3. fejezetben pedig egy rövid áttekintést adok a tézisek kidolgozási módszertanával kapcsolatban. A 4. fejezetben az új eredményeket tézisek formájában összegzem.

Az 5. fejezetben a bemutatott eredményeim néhány ismert, gyakorlati alkalmazását sorolom fel. Ezután az irodalmi hivatkozások és a saját publikációim listái következnek.

2. fejezet

Kutatási célok

A disszertációm célja egy olyan integrált infokommunikációs hálózat és szolgáltatás-menedzsment keretrendszer bevezetése, amelyet könnyű a gyakorlatban is alkalmazni, majd e keretrendszer részeként új módszerek és mérőszámok bemutatása. Ezek kiterjednek a hálózati szűk keresztmetszetek vizsgálatára, a gyors és pontos hibaok-kereső módszerekre, a felmerülő mérőszámok számítási pontosságának és komplexitásának ellenőrzésére is. Az eredményeket az autonóm hálózatok menedzsmentjének területére is kiterjesztem.

Ezen célok elérése érdekében a következő irányokban végeztem kutatást:

- összetett hálózati szolgáltatások magas minőségű VoIP és többoperátoros end-to-end Ethernet üzemeltetési és karbantartási követelményeinek és korlátainak vizsgálata;
- szolgáltatásminőség-biztosítási keretrendszer definiálása, megvalósítása és validálása;
- hálózati forgalmi mérések végzése és kiértékelése az akadémiai gerinchálózaton és internet-szolgáltatók maghálózataiban, annak érdekében, hogy meghatározzuk a nagysebességű interfészeken haladó adatok on-the-fly kiértékelésének határait;
- egyedi, Petri-háló alapú hibaok-analízis módszer kidolgozása, ami az emberi szakértő problémamegoldó hozzáállását modellezi;
- a keretrendszer és a Petri-háló alapú hibaok-analízis módszer kialakítása és validálása valós esetekben, VoIP és többoperátoros Ethernet szolgáltatásokra;
- az M/G/R-PS tömegkiszolgálási modell és a csomagbeérkezési időkülönbségek (packet interarrival times, PIT) eloszlásának vizsgálata a hálózati szűk keresztmetszetek feltárásához, valamint a ennek korrelálása a felhasználó elégedettségi szintjével (Quality of Experience, QoE);
- forgalmi analízis módszerek kutatása és definiálása a monitor-síkon, beleértve térbeli és időszakos és vizsgálatokat, az alkalmazások azonosítását és a forgalmi mátrix számítását.

Kutatásom az infokommunikáció területére korlátozódik, energetikai, vagy egyéb rendszerek csomagkapcsolt hálózataira nem feltétlenül alkalmazhatók az eredményeim.

3. fejezet

Módszertan

A hálózati QoS (Quality of Service) és tulajdonképpen a felhasználói QoE is javítható a hálózati folyamatok és a szolgáltatások állapotának folyamatos, hatékony kontrollálásával. Ennek eléréséhez egy összetett és integrált szolgáltatásminőség-biztosítási keretrendszer kifejlesztésére volt szükség. A történeti áttekintést, valamint a jelenleg rendelkezésre álló ilyen rendszereket és hiányosságaikat a disszertációban részletezem.

Definíció: Szolgáltatásminőség-biztosítás – Ebben a disszertációban a szolgáltatásminőség-biztosítás (Service Assurance, SA) egy általánosított értelmezését használjuk: magában foglalja mindazon funkciókat, amelyek hozzájárulnak a menedzselt hálózatot használó infokommunikációs szolgáltatások fennakadásmentes működéséhez.

A szolgáltatások hatékony és tényszerű teljesítmény-menedzsmentje csak az azokat működtető csomópontoktól fizikailag független monitorozó rendszer használatával érhető el. Ezen eszközök fő funkciója a monitorozott interfészeken történő adatgyűjtés, az adatok feldolgozása és forgalmi statisztikák számítása.

Az adatfeldolgozást keret, csomag és folyam-szinten (pl. Ethernet, IP és TCP protokollok szintjén) is végeztem, erre az adott tézisek ismertetése során kitérek. Emellett a QoE és forgalmi mix vizsgálatok során az alkalmazási réteg adatait is vizsgáltam.

Az 1. téziscsoportban egy olyan SA keretrendszert alakítottam ki, amely lehetővé teszi a jelenlegi hálózati- és szolgáltatás-menedzsmentben felmerülő problémák kezelését. A 2. téziscsoportban egy egyedi hibaok-analízis (Root Cause Analysis, RCA) módszert vezetek be, amely akár a keretrendszeren belül, akár attól függetlenül használható. Ezeket az eredményeket empirikusan nyertem, szimulációkkal és valós mérésekkel támasztottam alá a módszerek működését.

Az egyik legkritikusabb szolgáltatásminőség-romboló hatást a hálózati szűk keresztmetszetek okozzák. Ezeket gyakran tervezetlen, tüskeszerű forgalmi csúcsoknak köszönhetjük, melyek a topológia gyenge pontjain jelennek meg. Az ilyen szűk keresztmetszeteket nehéz detektálni és a jelenlétük okát talán még nehezebb feltárni.

A 3. téziscsoportban különböző módszereket alakítottam ki a hálózati szűk keresztmetszetek passzív monitorozással történő detektálására, majd összehasonlítottam ezek képességeit. Munkám a hálózati forgalom csomag-szintű analízisén alapult, melyek során megfigyeltem a szűk keresztmetszetek viselkedését és hatásait. A kialakított mérőszámokat (M/G/R-PS-alapú késleltetési tényező, a PIT kurtosis és skewness) analitikus módszerekkel vezettem be és működésüket szintén bizonyítottam szimulációkon és valós méréseken keresztül is.

A tudás-síkkal (Knowledge Plane) kapcsolatos kutatásaim integrálják a hálózat-monitorozásban szerzett tapasztalataimat és az SA keretrendszer kialakítása során használt módszereket. A fenti eredményeimet itt az autonóm hálózatok nézőpontjából általánosítom, különös tekintettel a monitor-sík feladataira. Mindezeket a 4. téziscsoportban foglalom össze.

4. fejezet

Új eredmények

4.1. A szolgáltatásminőség-biztosító keretrendszer

---

1. Téziscsoport - Létrehoztam és a gyakorlatban is verifikáltam egy olyan egyedi, integrált szolgáltatásminőség-biztosító keretrendszert csomagkapcsolt hálózatokhoz, amely minden szóba jövő bejövő esemény-típust figyelembe vesz; definiálja és szétválasztja a szűrési, eseménykorrelációs és hibaok-analízis funkciókat; valamint bevezeti a szűrési módszerek egy olyan minimális halmazát, amelyek hatékony hibajegy-generáláshoz vezetnek. [J2] [J4] [C4]

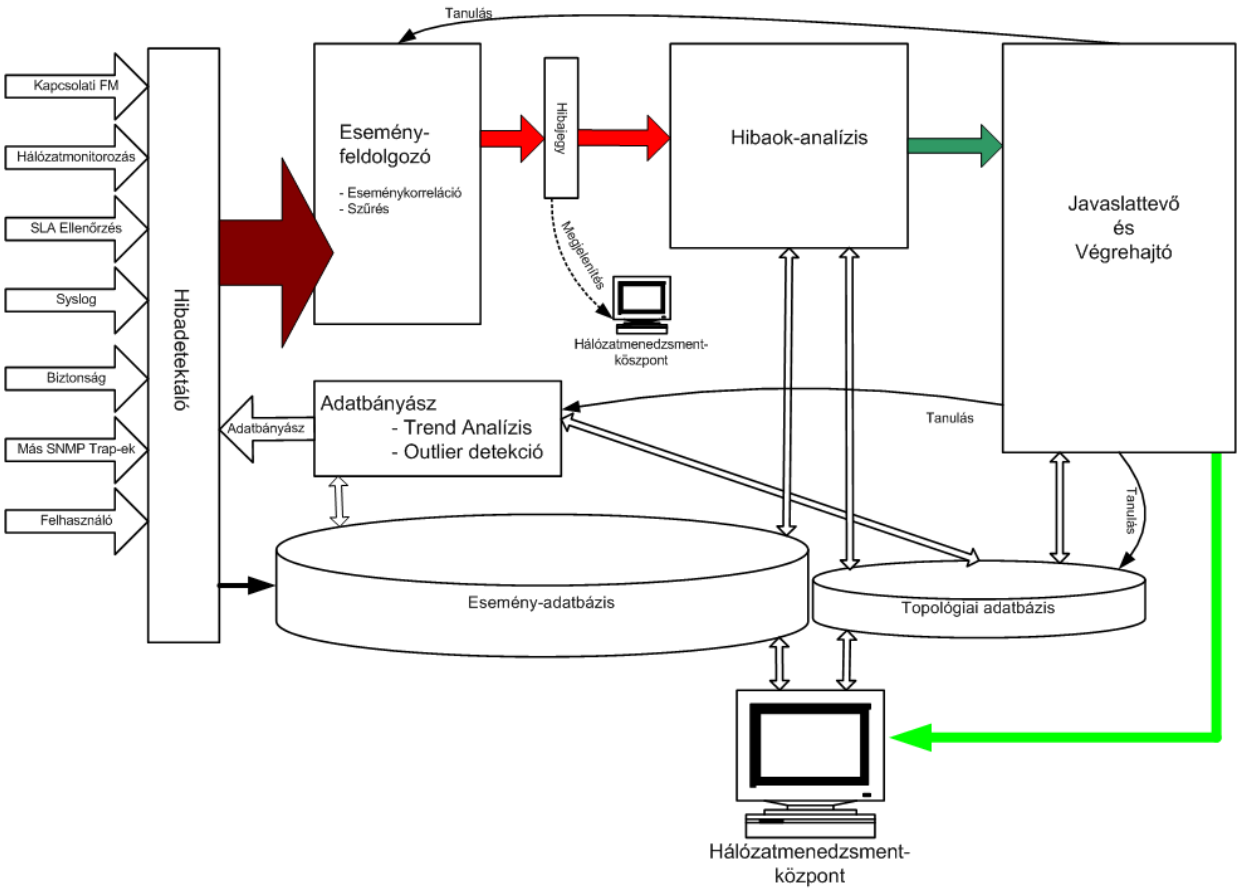
Ez a fejezet az általam bevezetett, integrált szolgáltatásminőség-biztosítási (Service Assurance, SA) keretrendszer funkcióit, az itt alkalmazott módszereket és megoldásokat mutatja be. A keretrendszer abból a szempontból egyedinek tekinthető, hogy a felügyeletére bízott szolgáltatáskör minden lehetséges eseményforrását és eseményét kezeli, és ez alapján javasol hibaelhárító lépéseket a rendszeren belül – így biztosítva annak szolgáltatásait.

Ezt az SA keretrendszert egy technológiákon átívelő, integrált eszközrendszerként is lehet értelmezni, amely többek között kihasználja a hagyományos hibamenedzsment (Fault Management, FM) a kapcsolati hibamenedzsment (Connectivity Fault Management, CFM), a teljesítmény-monitorozás (Performance Monitoring, PM) [ITU92] és a szolgáltatásszint-ellenőrzés (Service Level Specification Verification) [AETP04] eszközeit, módszereit és vizsgálandó mércéit.

A keretrendszer áttekintése

1.1. altézis - Definiáltam egy általános, bármilyen hálózati szolgáltatás esetében alkalmazható szolgáltatásminőség-biztosítási keretrendszert, amely proaktívan segíti a szolgáltatás-minőséggel kapcsolatos problémák kiküszöbölését, és lefedi az esemény-jelzési, az esemény-előfeldolgozási, a hibaok-analízis, az adatbányászati és a döntési funkciókat.

A bemutatásra kerülő általános szolgáltatásminőség-biztosítási (Service Assurance, SA)



4.1. ábra. Az eseményfeldolgozó és hibajegykezelő rendszer elemeinek kapcsolódása

keretrendszer lényegét az általa végrehajtott információ-kezelési folyamaton keresztül foglalhatjuk össze (4.1. ábra). Az egyes modulok működését a disszertáció részletezi.

Egy komplex hibamenedzsment rendszernek az alábbi funkciókat kell megvalósítania:

- észleli és összegyűjti a hálózat működése során kialakuló hibaüzeneteket,
- segít a hibaüzenetek szűrésében,
- diagnosztikai teszteket futtat a hibaforrás felderítésére, hibajavításra tesz javaslatot.

A hálózatmenedzselő alkalmazás a felügyeleti központban figyeli a hálózatot, hibajelenségekre "vadászva". A megjelenő hibákat a

- hibadetektálás,
- hibajel-feldolgozás,
- hibaok-meghatározás és hibajavítás

lépésein keresztül kezeli (4.1. ábra). A folyamat eredménye egy hibajavítási javaslattétel. Az operátor ez alapján elkezdheti a hiba okának megszüntetését. Ha a hibaok-meghatározás

során a rendszer nem képes egészen pontosan eljutni a hiba okáig, a folyamat naplójának vizsgálatakor az operátor látja az elvégzett lépéseket és azok eredményeit, így ezek ismétlése nélkül további irányokban keresheti a hiba okát.

Mint a 4.1. ábrán is látható, hibajelek (események) különféle forrásokból érkezhetnek a hibadetektálóhoz.

A Hibadetektáló ezeket adott mező-formátumú eseményekké képezi – majd egyrészt eltárolja az adatbázisban, másrészt továbbküldi őket a Hibajel-feldolgozóhoz.

Az Adatbányász modul az eltárolt események halmazán dolgozik (korábbi eseményeket is figyelve) és ha szükséges, új hibajeleket generál.

Miután az események átjutottak a *korrelátor*on és a *szűrő*kön, már csak azokat a hibajegyeket (alarmokat) kapja meg az NMC (Network Management Center, Hálózatmenedzsment-központ), amelyekkel mint hibajelenséget jelző hibajegyekkel foglalkozni kell. A Hibaok-meghatározó (Root Cause Analysis, RCA) modul azonnal elkezd ezeken dolgozni, a hiba gyökere után kutatva. Ha ezt megtalálta, a hiba okának leírása a Javaslattételi modulhoz kerül. Ez eldönti, hogy automatikus javító-lépéseket indít, vagy "csak" a javaslattételi leírást és az elvégzett ellenőrző lépések naplóját bocsátja az emberi szakértő rendelkezésére. Az emberi szakértő ezek alapján végrehajtja a szükséges intézkedéseket, vagy ellenőrzi az automatikus javító-lépések hatékonyságát. A modell több tanulási visszacsatoló ágat is tartalmaz, ezek is külön jelölésre kerültek a 4.1. ábrán.

A következő részben röviden összefoglalom, hogyan működik a feldolgozó-folyamat, és bemutatom az SA keretrendszer moduljainak működését.

Hibadetektáció

A hibadetektálás célja a hálózatot, vagy annak szolgáltatásait veszélyeztető hibajelenségek minél hamarabbi érzékelése és az ezekről szóló jelentések továbbítása hibafeldolgozásra. A hibajel-adatbázis kialakításához ezen státusz-információt tartalmazó üzenetek mellett az SA keretrendszer aktív ellenőrző elemeinek jelzéseit is felhasználjuk. Ezen adatbázis kialakításánál azzal a nehézséggel találkozunk, hogy a különböző hibajel-források által küldött hibajelek különböző formátumban érkeznek. A későbbi munka megkönnyítése érdekében ezeket a hibajeleket egységes formátumba kell rendeznünk, továbbá kezelői felületet kell biztosítanunk a vizsgálatukra. Az így átalakított hibajeleket a hibafeldolgozás során már könnyen tudja kezelni a rendszer. Az esemény-forrásoktól érkező különféle eseménytípusok a 4.1. ábra bal oldalán láthatók, ezeket a disszertációban részletezem.

Trendanalízis és kilógó adatok vizsgálata

Ez a modul a hibajel-adatbázis adatain dolgozik. Folyamatosan trendanalízis algoritmusokat futtat, és figyeli azokat a kilógó adatokat is, amelyek nem illeszkednek be a periodikus adatmintákba. A különös jelenségekről speciális hibajelet generál.

Hibajel-feldolgozás

1.2. altézis - Esemény-feldolgozó algoritmust hoztam létre, amely világosan szétválasztja az eseménykorrelációs, esemény-szűrési és hibaok-analízis funkciókat,

maximalizált számosságú eseményhalmazt állít elő korreláció segítségével, majd ebből szűri ki a megfelelő hibajegyeket, így hibaok-analízist már csak hibajegyekre nem pedig események halmazára kell elvégezni.

A hibadetektálótól érkező esemény-leírás típusú rekordok képezik a hibajel-feldolgozás bemeneti adathalmazát. Az adatbázis manuális feldolgozása meghaladja az üzemeltető operátor lehetőségeit, hiszen egy absztrakt és valódi értelemben is többszörözött, másodpercenként akár több tucatnyi rekorddal növekvő adathalmazról van szó.

A hibajel-feldolgozás egy automatizált adatfeldolgozó folyamat, melynek eredményeként hibajelek helyett csak a hibajegyeket (alarmokat) tárjuk az operátor elé. A hibajeleket a későbbi hasznosítás érdekében az adatbázis tárolja. Feldolgozásuk a korrelátor modulban kezdődik. A redundancia-mentesítést, és a "lényeg kiemelését" a szűrő modul végzi.

Az eseménykorreláció a szűrésnél magasabb szintű feldolgozási módszer, amely különböző hibajelek közti összefüggések felderítésére hivatott. Több hibajel rövid időn (néhány percen) belüli beérkezése esetén módunk van egy sokkal specifikusabb hibajel-leírást adni. A korrelátor alkalmazása során nem veszítünk hibajelet: a szabálynak megfelelően mind a bementi, mind az új, specifikus hibajelet továbbküldi (a szűrő modulba, amely megfelelő módon nyomja majd el ezeket). A szabályokat az operátor a szűrőszabályokhoz hasonló módon szabadon változtathatja. Az esemény-korrelátor végső célja, hogy lehetőség szerint átfogóbb hibajelet generáljon, számos hibaok-elemet vonjon össze egy eredendő okká.

A legegyszerűbb hálózat-felügyeleti algoritmus a szűrés. A jelenlegi hibamenedzsment-rendszerekben használt szűrési algoritmusok közül [Mei97] a szabály alapú szűrést választottam munkatársaimmal. Ennél a módszernél a szűrőmodul egyenként megvizsgálja a beérkező hibajeleket, hogy talál-e rájuk alkalmazható szabályt. Amennyiben ilyen szabály nincs, a hibajelből alapértelmezés szerint hibajegyet generál. Minden más esetben az alkalmazott szűrőszabálynak megfelelően jut tovább, vagy nyomódik el a hibajel.

A hibaok-analízis (RCA) gyakran homályos definíciók mentén összekeveredik az irodalomban az esemény-korrelációval, ami helytelen. Az eseménykorreláció nem mutatja meg a hiba okát, csak annak egy nagyon kifinomult szimptómáját jeleníti meg. Egy másik megvilágítási módja a megkülönböztetésüknek a bemenő adathalmazuk típusán alapszik: míg az eseménykorreláció eseményekből dolgozik és végül kifinomult hibajegyeket generál, addig az RCA hibajegyeket (alarmokat) fogad be, és ezek alapján a hiba okának a leírását nyújtja a kimenetén.

Ebben az értelmezésben az eseménykorrelációs, a szűrő és a hibaok-analízis (RCA) modulok hibafeltárás szempontjából leghatékonyabb összekapcsolása épp ebben a sorrendben történik.

Eseménykorreláció

A kezelést és átláthatóságot megnehezítő komplexitás csökkentése érdekében az SA keretrendszerben használt eseménykorrelátor szabály-alapú. Ha egy korrelációs szabály illeszkedik az eseményhalmazra, akkor egy új, speciális esemény generálódik.

Szűrés

1.3. altézis - A létező nagyszámú esemény-szűrő halmazok vizsgálata alapján megmutattam, hogy létezik a szabály-alapú funkciók olyan kis elemű halmaza (számlálók, redundancia-szűrők, dominancia-szűrők, teljes elnyomó), amely eseménykorrelációval együtt alkalmazva szignifikánsan csökkenti a tévesen generált hibajegyek számát, miközben a valódi hibát jelző hibajegyeket hibaok-analízisre bocsátja.

A következő négy szabály-alapú szűrőmodul alkalmazásával – ha ezek az esemény-korrelátor kimeneti adatait is megkapják – szignifikánsan csökkenthető a később feldolgozandó hibajegyek száma. Mivel ez a módszer csökkenti a redundáns RCA-feldolgozás lehetőségét, összességében növeli annak hatékonyságát. A megvizsgált, nagy számú egyéb típusú szűrők közül egyik alkalmazása sem vezet a hibajegygenerálás hatékonságának növekedéséhez.

Ennek az az oka, hogy alapértelmezésben a csekély fontosságú események mind **elnyomó**dnak, kivéve azok, amelyek adott időn belül nagy számossággal mutatkoznak (lásd **számláló**k). Ezzel szemben minden magas prioritású eseményből hibajegy készül, kivéve, ha ezek többen vannak (lásd **redundancia)**, vagy ha adott időszakon belül korábban előfordult már magasabb prioritású, hasonló típusú esemény (lásd **dominancia)**. A számláló típusú szűrő és az eseménykorrelátor célja a kialakuló események számának maximalizálása, míg a három elnyomó-típusú szűrő hatására csak a valóban fontos jelenségekről lesz hibajegy.

- *Számlálók* - akkor adnak alamrmot, ha legalább adott számú ugyanolyan esemény érkezik adott időszakon belül. Azoknál az alacsony-prioritású eseményeknél jelentős a használata, melyek egyedi előfordulása nem, míg nagy tömegű megjelenése hibára utal;

- *Redundancia szűrők* - az esemény első elfordulásakor alarmot generálnak, aztán adott ideig elnyomják a hasonló beérkezéseket. Alkalmazásuk kritikus vagy magas prioritású események beérkezésekor hasznos;

- *Dominancia szűrők* - legalább két eseményazonosító megadása (például A és B) segítségével dolgoznak. Ha A-t átengedik (magas prioritás), akkor az ezután adott időn belül érkező B (alacsonyabb prioritás) esemény minden előfordulását elnyomják;

- *Elnyomó szűrő* - egyszerűen elnyomja az adott azonosítójú eseményeket. Előfordul, hogy hibafeltárás szempontjából érdektelen események (pl. konfigurációs állomány átírásának naplózása) is eljutnak a rendszerbe, amelyekből sohasem kell hibajegyet generálni.

A tranziens hálózati hibák kiszűrése az SA keretrendszerben a szűrőmodulok alapértelmezett viselkedése során, a verifikációs periódus jelenlétének segítségével valósul meg. Ha a hibajelként beérkezett hálózati állapotjelzés törlése is megérkezik a verifikációs periódus alatt, akkor a modul a hibát tranziensként értelmezi, és nem generál belőle hibajegyet.

Hibajegy megjelenítés

Az eseményfeldolgozó kimenetei maguk a hibajegyek. Minden hibajegyre külön RCA-mechanizmus indul.

Hibaok-analízis (Root Cause Analysis)

A modul feladata, hogy a hibajegy-leírók alapján feltárja a hiba okát. A disszertáció hibaok-analízissel foglalkozó fejezete részletezi a kutatott és használt módszereket, és bemutatja a második téziscsoportban megjelenő párhuzamos hibaok-kereső módszer működését is.

Végrehajtók és Adatbázisok

A folyamat végén a **Javaslattevő és Végrehajtó** ad javaslatot a hiba javításának lépéseire a felderített hibaok ismeretében; az **Esemény-adatázis** minden, a keretrendszer felé küldött, vagy belül generálódott eseményeket eltárol; a **Topológiai Adatbázis** a csomópontokkal kapcsolatban eltárolja a hálózati címeket, típusokat (funkciókat), és a csatlakozó csomópontok listáját (melyik interfészen, milyen hálózati címen).

4.2. Adatvezérelt hibaok-analízis

---

2. Tézis - Kialakítottam egy új, adatvezérelt, párhuzamos, Petri-hálókon alapuló hibaok-analízis módszert és megmutattam, hogy alkalmas különböző szolgáltatás-minőség-biztosítási esetek megoldására. [J2] [J4]

Ebben a téziscsoportban egy egyedi, adatvezérelt hibaok-analízis módszert vezetek be, amely akár az SA keretrendszer részeként, akár függetlenül megvalósított eszközként is használható. A módszer alapjai a Petri-hálók, és folyamatában a hálózati szakértők problémamegoldó hozzáállását követi.

Az 1. és 2. téziscsoport gyakorlati alkalmazásait a VoIP szolgáltatás-menedzsment témakörében és egy többoperátoros Ethernet hordozóhálózat hibafelderítési esettanulmányán keresztül demonstrálom a disszertációban.

2.1. altézis - Hálózati szakértők hibaok-keresési módszereinek modellezésével kimutattam, hogy a Petri-hálók hatékonyan használhatók a párhuzamosított hibaok-keresési folyamat forgatókönyvének reprezentációjára. [J2] [J4]

A rendszer-szakértők akár előre definiált lépésekkel, akár a helyszínen improvizálva, de mindenképp valamilyen logikus terv szerint keresik a megjelenő hibajegyek okát. Eldöntik, hogy

- milyen méréseket kell elvégezni,
- mi után kell kutatni az eseménynaplókban vagy más adatbázisokban, és
- az eredmények függvényében milyen további lépésekre van szükség a hibaok feltárása során.

Akár tudatosan vagy tudattalanul, a szakértők hamar megszerzik a vizsgálatok elvégzéséhez hiányzó bemeneti adatokat (pl. IP-címek, interfész-azonosítók). A párhuzamos ellenőrző és lekérdező folyamatok aszinkron módon fejeződnek be, így a szakértőnek folyamatosan vizsgálnia kell a különféle jellegű bejövő adatokat és sorozatosan döntenie kell, milyen további

vizsgálatokat kell még elvégeznie. Az *adatvezérelt* vezérlési architektúrák épp az ilyen típusú problémák kezelésére lettek kialakítva, így az emberi szakértő szimultán jellegű adatfeldolgozási módszereinek modellezésére is alkalmasak.

Egy, az emberi szakértő viselkedésének modellezésén alapuló RCA algoritmusnak a következő követelményeknek kell megfelelnie:

- a hibajegy leírásából ki kell tudnia szűrni a kulcsfontosságú paramétereket;
- ezen adatok felhasználásával aktív diagnosztikai ellenőrzéseket kell tudnia indítani;
- a független ellenőrzések, rutinok és folyamatok párhuzamos végrehajtását kell tudnia kezelni;
- amint a vizsgálat eredménye elérhető, új rutinok futtatását kezdeményezi az új információk alapján;
- az előző lépést mindaddig ismétli az újonnan elvégzendő ellenőrzésekkel és eredményeikkel, amíg a hiba oka nem körvonalazódik.

A kezelhetőség és skálázhatóság kérdései elvezetnek a szakértők "üzemi gyakorlatának" ökölszabályaihoz: ha csak kevés számú hibajegy-típus létezik (így érdemes kialakítani a rendszert), akkor lehetőség van minden típusra külön "akciótervet" (vagy forgatókönyvet) készíteni. Ez az akcióterv lesz az alapja az *adatvezérelt* RCA-leírásoknak. A legismertebb adatvezérelt végrehajtási rendszer a Petri-háló.

Az adatvezérelt hibaok-analízis keretrendszer

2.2. altézis - Megalkottam és validáltam egy egyedi, adatvezérelt, párhuzamosított hibaok-analízis módszert, amely modellezi az emberi szakértő viselkedését, és újszerű módon a Petri-hálókat az aktív hibaok-analízis lépések ütemezésére használja, szemben az ismert gyakorlattal, amely az események terjedésének leírására használja ezeket. [J2] [J4]

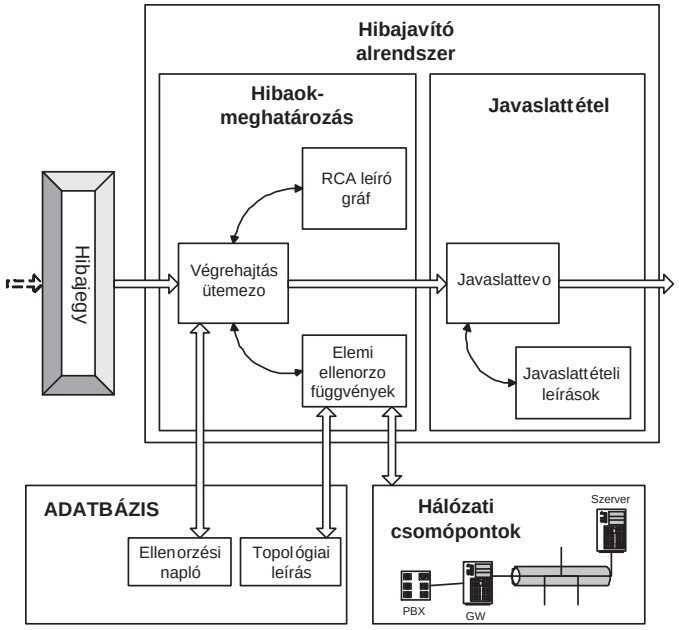
A hálózatmenedzsmentben a hibakorrelációval kapcsolatban ismertek a Petri-hálók alkalmazásai [AFB+97]. Ezek azonban az esemény-propagáció követésére, és ezek alapján az események korrelálására használják a Petri-hálókat, nem pedig aktív ellenőrző lépések kezdeményezésének ütemezésére, ahogyan a következőkben láthatjuk.

A hibajelek szűrésével és korrelálásával a hiba jellegét (és esetleg helyét) aránylag jól leíró hibajegye(ke)t kapunk. Ezekben a hibajegyekben változóként szerepel a hibajegy azonosítója, típusa, és szerencsés esetben - további paraméterek mellett - a hibát okozó eszközök halmazszerű leírása. A hibajegyek kiértékelésének célja a hibaok(ok) meghatározása, majd javaslattétel a hiba javítására. A 4.2. ábra az RCA ütemező belső felépítését jeleníti meg.

Minden hibajegy-típushoz tartozik egy Petri-háló formájú RCA-leíró gráf. Ez grafikusan ábrázolja az hibaok kiértékeléshez szükséges lépések (elemi függvények) kapcsolatát: mely adatok rendelkezésre állása esetén mely lépéseket lehet végrehajtani (erre mutat példát a később részletezendő 4.3. ábra). A folyamat kezdetén az ütemező az alarm típusától

függően kiválasztja a megfelelő RCA-leírót (Petri-hálót), majd az adatok rendelkezésre állásának ütemében lépteti végig rajta a hibaok-kereső folyamatot. Amint minden ellenőrző lépés (elemi függvény) eredményét megkapta, és nincs több végrehajtandó lépés, a hibaok-meghatározási folyamat eredményét a javaslattevő felé továbbítja. Ez a végeredményhez rendeli a megfelelő javaslattételi leírást, és az operátor rendelkezésére bocsátja azt.

A fenti folyamat központi eleme az RCA-leíró gráf. Erre az aktív RCA módszerek sorában újszerű megoldásként a Petri-hálós leírást javaslom.



4.2. ábra. A Petri hálókon alapuló, aktív ellenrzések végrehajtását ütemező RCA modell

Petri-hálókon alapuló RCA módszer

A javasolt RCA-végrehajtó módszer aktív ellenőrző lépések, adatbázis-lekérdezések és egyéb folyamatok végrehajtását ütemezi, az ezen feladatok végrehajtásához szükséges bemenő adatok rendelkezésre állásának függvényében.

A Petri-hálók ebben az esetben a hibaok-keresés "forgatókönyvének" tekinthetők. A folyamat során minden hibajegyhez hozzárendelünk egy saját, végrehajtandó Petri-hálót, amelyen végiglépkedve megtaláljuk a hiba okának legvalószínűbb helyét.

A megoldás lényege, hogy az aktív ellenőrzési feladatok (a Petri-háló "átmenetei") konkurens módon, az adatok (a Petri-háló csomópontjai) rendelkezési állásának ütemében hajtódnak végre. Ha egy adat(halmaz) rendelkezésre áll, az ezt reprezentáló csomópontba jelzés, "token" kerül. Egy adott ellenőrzés akkor kerül végrehajtásra, ha az összes bemeneti adata rendelkezésre áll (minden bemeneti csomópontjában van "token"). Az ellenőrzés végrehajtásának eredményeképpen előállnak a kimeneti adatok, azaz a kimeneti csomópont(ok) "token"-nel lesznek ellátva. A gráfba külön adatlekérdező lépéseket lehet bevezetni annak érdekében, hogy egy adott ellenőrző-függvény összes bemeneti változója rendelkezésre álljon. Amikor egy adott elemi függvény kiértékelésre kerül, a "token" megjelenik a kimenetén (az

ehhez tartozó adat más elemi függvények bemenete lehet). A végrehajtás ütemező minden ütemben megvizsgálja, hogy van-e az RCA-gráf átmenetei (elemi függvényei) között olyan, amelynek minden bemenetén van "token", s ha talál ilyet, elindítja az adott elemi függvény kiértékelését. Ha az utolsó (tipikusan a végső kiértékelést végző) elemi függvény kimenetén is megjelenik a "token", a végrehajtás ütemező átadja az eredményeket a javaslattevőnek, és megszünteti az RCA-entitást.

Mivel egyes mérések elvégzése, vagy bonyolultabb adatbázis-lekérdezések visszatérése időbe kerül, számos, ugyanahhoz a hibajegyhez tartozó ellenőrző folyamat párhuzamosítható ezzel a módszerrel.

A Petri-hálók nem-determinisztikus természetéből fakadóan kiválóan alkalmasak az emberi szakértő hibaok-keresési munkamenetének modellezésére.

2.3. altézis - Új leírókat és elemi ellenőrző függvényeket alakítottam ki az új, Petri-hálókon alapuló hibaok-analízis rendszerben, melyek segítségével megmutattam, hogy a módszer többféle hálózati szolgáltatás (multi-domain Ethernet, VoIP) esetén is hatékonyan alkalmazható. [J2] [J4] [C4]

A következő esettanulmányok az RCA-leíró kialakítási lehetőségeinek a validálása során, a koncepció gyakorlati létjogosultságának alátámasztásához készültek. Emellett segítenek az RCA folyamat végrehajtásának megértésében is. A következőkben a többoperátoros Ethernet-környezeten alapuló hálózati szolgáltatás, valamint a VoIP szolgáltatás-minőség során fellépő hibaesetek okának felderítésére mutatok be egy-egy példát.

1. esettanulmány: Ethernet szolgáltatások, kapcsolódási hiba

Először vizsgáljunk egy alapvető kapcsolati hibaesetet. Az SA-keretrendszerbe többek között az aktív CFM (Connectivity Fault Management) hibaesemény-forrásból is érkezhet ilyen típusú jelzés. A hibajegyhez tartozó, Petri-hálós RCA-leíró a 4.3. ábrán látható.

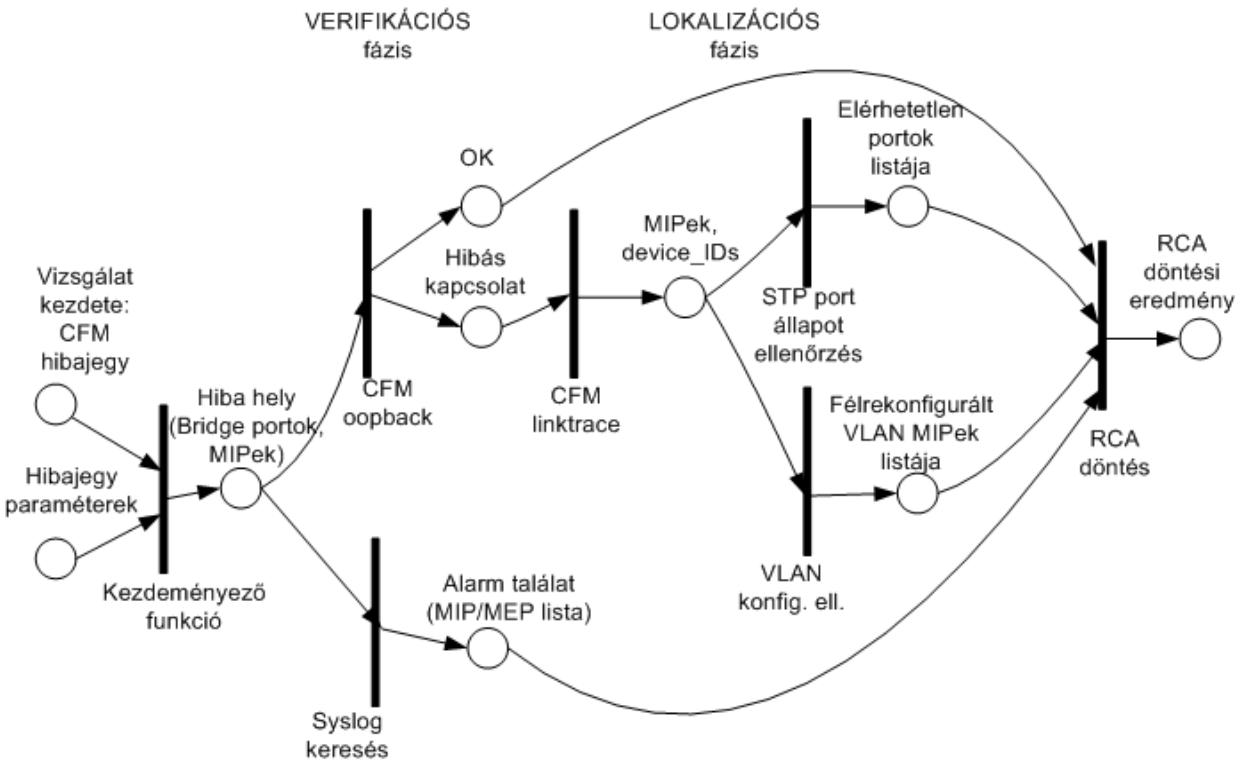
A végrehajtást a CFM hibajegy megjelenése indítja. A Petri-háló rögtön többfelé ágazik: aktív hibaok-keresési függvények meghívására és passzív adatbázis-lekérdezésre.

Ezen elemi ellenőrző függvények kiértékelése után mind közelebb jutunk a hiba okához. Ha konkrétan arra utaló Syslog-jelzéseket találtunk, ezek segítségével az eredményben a hiba oka szépen meghatározható (pl. működésképtelen interface). Ha az ellenőrzés során kiderült a hiba helye, a VLAN- és STP-ellenőrző folyamatok visszatérésével a hiba oka tovább pontosítható. A végső kimenet egy szabály-alapú döntés segítségével áll elő, a megelőző vizsgálatok eredményei alapján.

2. esettanulmány: VoIP szolgáltatás, magas csomagvesztés

Ez az RCA esettanulmány a VoIP-szolgáltatók számára készült teljes hibamenedzsment-rendszer egyik RCA-leíróját mutatja be. Az egyik legösszetettebb feladat a "magas csomagvesztéshez" tartozó hibajegyhez megtalálni a hiba okát. A 4.4. ábra az ide vonatkozó Petri-hálót jeleníti meg.

Az elemi ellenőrzések párhuzamos végrehajtása egyértelműen lerövidíti az RCA-végrehajtáshoz szükséges időt – ez nyilvánvalóan elősegíti a hibajavítás idejének csökkentését is. A VoIP-szolgáltatásokhoz kialakított SA-rendszeren végzett vizsgálatok során azt tapasztaltuk,



4.3. ábra. A "CFM kapcsolódási hiba" hibajegyéhez tartozó Petri-háló [J4]

hogy a hibaok-keresés átlagos ideje a Petri-hálós, párhuzamosított módszerrel átlagosan *fele* volt a hagyományosan, sorosan ütemezett feladatvégrehajtásokkal működő megoldás átlagos idejének.

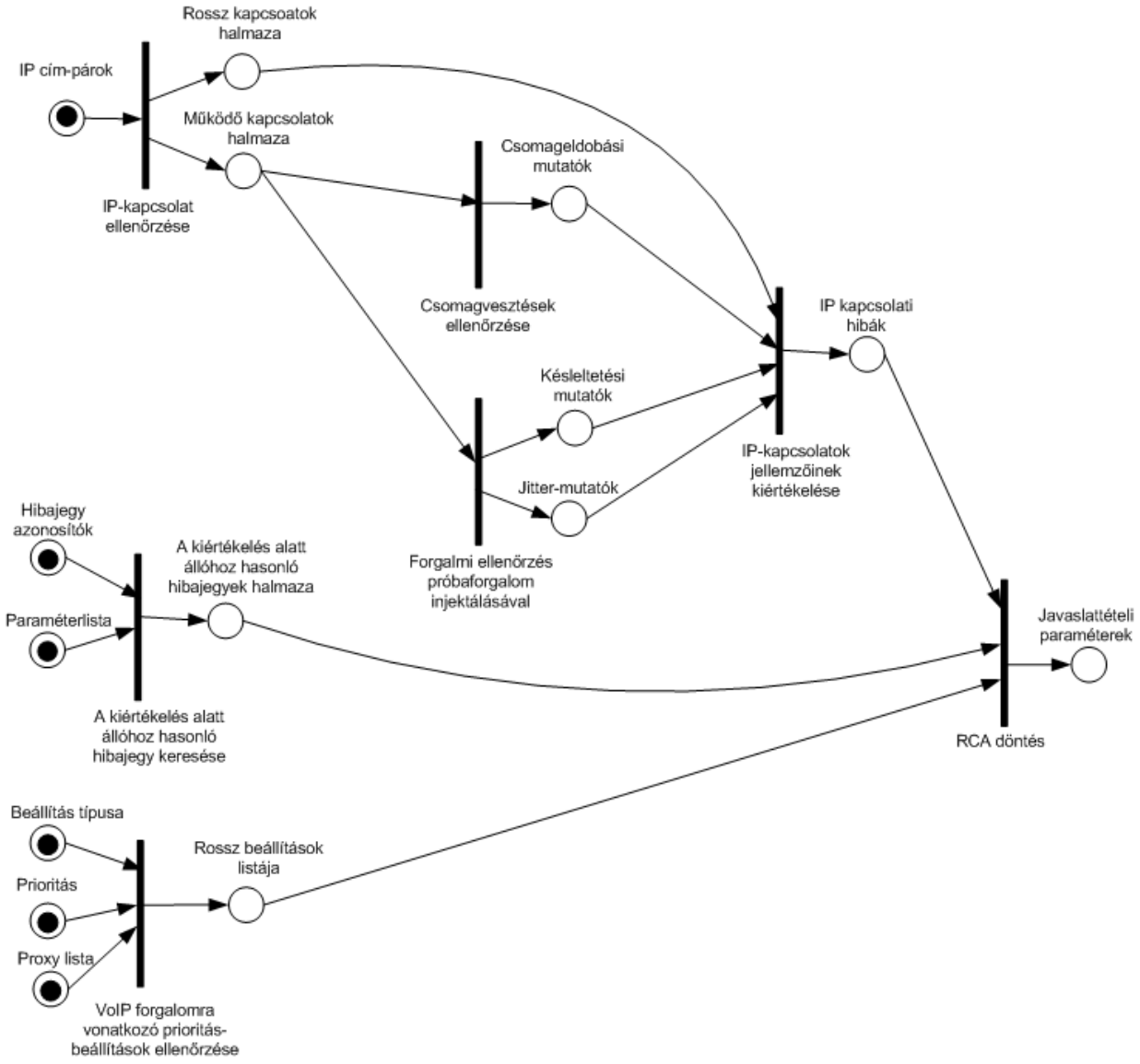
4.3. Hálózati szűk keresztmetszetek és az általuk generált események

---

3. Tézis - Definiáltam egy olyan új, az aggregált hálózati kapcsolatokon, passzív mérések során használható, hálózati szűk-keresztmetszetek detektálására alkalmas mérőszámot és ehhez kapcsolódó módszert, amely a korábbiaknál jóval hatékonyabb; ezt szimulációkkal, majd élő hálózati mérésekkel is demonstráltam.

Egy adott hálózati link passzív monitorozása, a megfigyelt csomagok időbélyeggel együtt való regisztrálása rengeteg hasznos adatot szolgáltat a hálózat állapotát célzó elemzésekhez. A szűk keresztmetszetű hálózati erőforrások felderítésére számos lehetséges mérőszám kínálkozik.

Az egyik lehetséges módszer az, ha a regisztrált beérkező csomagokat érkezési idejük szerint sorrendbe állítjuk és megvizsgáljuk az egyes csomagok érkezése közötti időkülönbségeket. Vizsgálataimból kiderült, hogy a csomag-beérkezési időkülönbségek (packet interarrival time



4.4. ábra. A "magas VoIP csomagvesztés" hibajegyhez tartozó Petri-háló [J2]

- PIT) valószínűségi sűrűségfüggvényének (probability density function - PDF) negyedik centrális momentuma (kurtosis) értékes információkat szolgáltat a vizsgált linken fellépő torlódásról és annak mértékéről. Emellett az M/G/R–PS tömegkiszolgálási modell késleltetési faktora (delay factor) is hasznos jelzőszám bizonyos esetekben. A vizsgált mércék gyakorlati alkalmazhatóságát szimulációk és valós hálózati mérések során is verifikáltam, valamit megvizsgáltam, melyikük mennyire alkalmazható a felhasználói elégedettséget becslő jelzőszámként.

Definíció: Hálózati szűk keresztmetszet – Egy hálózati kapcsolatot akkor tekintek "szűk keresztmetszetnek", ha a hozzá érkező csomagok folyamatos, komoly sorbanállásra kényszerülnek, és a véges sorhosszak következtében esetenként eldobásra is kerülnek.

Ezt egy másik nézőpontból is vizsgálhatjuk: tegyük fel, hogy egy felhasználó hasonló

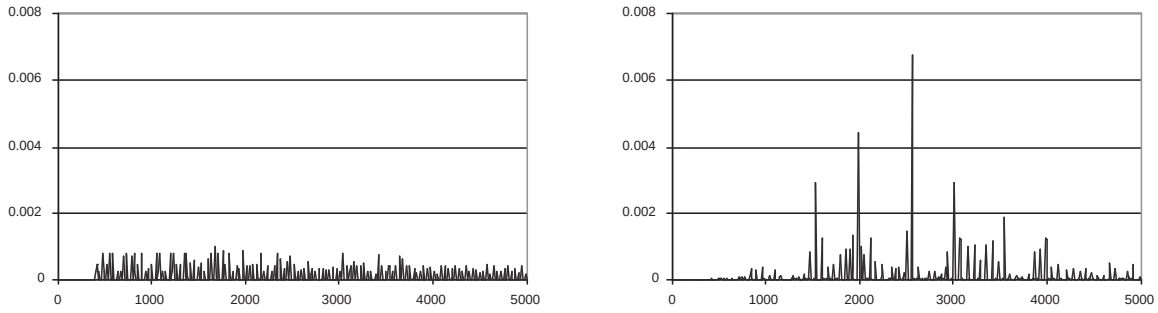
hálózati szolgáltatásokat vesz igénybe az a és a b szerveren is (ezeknek hasonló a kiszolgálási teljesítményük). A felhasználó az a szervert az A úton, míg a b szervert a B úton éri el. Ebben az esetben ha a felhasználó elégedett az a szerver kiszolgálási idejével, míg a b szerver felől érkező válaszok késleltetésével elégedetlen, akkor a B útvonal szűk keresztmetszet(ek)et tartalmaz – legalábbis többet, mint az A útvonal.

3.1. altézis - Definiáltam a csomagszintű "PIT-kurtosis" metrikát passzív mérés-alapú hálózati szűk-keresztemetszet detekcióhoz, és megmutattam, hogy korábban használt mérőszámokhoz képest a "PIT-kurtosis" mérőszám értékhatárai élesebbek. [J3] [C3]

Definíció: Csomagbeérkezési időkülönbség (Packet Interarrival Time, PIT) – A hálózati kapcsolat egy adott pontján megfigyelt, egymás után érkező két csomag első bitjének beérkezése között mért időkülönbség.

A PIT és a csomagközi szünet (Inter-Packet Gap, IPG) fogalma közötti különbség megértése nagyon fontos. Utóbbi az az időkülönbség, amely a megfigyelt két csomag közül az előző utolsó bitje és az őt követő csomag első bitje között eltelik. Ez valóban "csomagközi szünet", hiszen ebben az időszakban nem továbbítódik csomag a kapcsolaton.

A PIT eloszlásának alakulása hálózati szűk keresztmetszetek felismerésének lehetőségét rejti magában. Minél több csomagnak kell sorban állnia, annál többen fogják elhagyni a csomópontot szorosan egymás után. Ez a viselkedés a PIT sűrűségfüggvényben kicsúcsosodáshoz vezet, tüskék kezdenek el megjelenni bizonyos tipikus beérkezési idők esetén. Ahogyan a sorbanállás kezd torlódássá fajulni, úgy lesz egyre dominánsabb az adott környezetben elérhető legkisebb PIT értékhez tartozó érték tüskéje. Csekély kihasználtságú, egyenletes forgalmú linkek esetén nem jelenik meg egyetlen módusz sem a PIT sűrűségfüggvényen, így az laposnak tűnik, ahogyan azt a 4.5.a. ábra is mutatja. Másrészről, kezdődő torlódásnál tüskék jelennek meg egyes PIT értékeknél, mint azt a 4.5.b. ábra is mutatja. Ezt a csúcsosságot az eloszlás negyedik centrális momentuma – a kurtosis – is jelzi: egyre pozitívabb értékeket vesz fel.



a. PIT PDF - nincs sorbanállás

b. PIT PDF - enyhe torlódás

4.5. ábra. PIT sűrűségfüggvény egy aggregált kapcsolaton, sorbanállás nélküli (balra) és enyhe torlódásos esetben (jobbra) [J3]

A kurtosis, az eloszlás negyedik centrális momentuma a normális eloszláshoz képesti

csúcsosságot vagy laposságot jelzi. A 4.1 egyenlet a "kurtosis excess" definícióját mutatja [KK51]. A mérőszám használata széles körben elterjedt a matematikai statisztikában. A függvény értékkészlete a normális eloszlással való könnyebb összehasonlítás érdeklében normalizálva van. Definíció szerint a "kurtosis proper" a negyedik centrális momentum, ebben nem szerepel a -3 mint normalizáló faktor.

$$\gamma_2 = \frac{E[(\xi - E(\xi))^4]}{\sigma^4} - 3. \tag{4.1}$$

Amennyiben tehát egy csomópont több különböző sebességű link forgalmát fogadja, (és épp nincs sorbanállás, vagyis a csomagok gyakorlatilag késleltetés nélkül tovább haladhatnak) az adott csomópont kimenetén a PIT PDF görbéje lapos lesz, mivel az adott csomópontot a csomagok teljes mértékben véletlenszerűen hagyják el, úgy ahogyan érkeztek. Ha azonban valamelyik becsatlakozó link terhelése elkezd nőni, az azt megelőző csomópontban sorbanállás lép fel: a csomagok a csomópontból közvetlenül egymást követve kerülnek rá erre a linkre. Minél több linken történik sorbanállás a sűrűségfüggvény (PDF) egyre "tüskésebb" lesz: meredek felfutású, lokális maximumok jelennek meg, mivel sok csomag érkezése között azonos időközök lesznek.

3.2. altézis - Szimulációk és valós, szolgáltatóknál végzett nagysebességű hálózati mérések alapján igazoltam a PIT-kurtosis metrika hatékonyságát. [J3] [C3]

Hálózatszimulációs eszközként az OPNET-et használtuk, mivel korábbi hálózati vizsgálataink során már beláttuk alkalmazhatóságát. A szimulációs periódus 15 percben határoztuk meg, a forgalom összetétele szimulált ISP-nként (Internet Servics Provider, Internetszolgáltató) különböző volt, és az aggregációs hálózatban vegyesen jelent meg e-mail, ftp, http and adatbázis-hozzáférés típusú forgalom.

A vizsgálatok során további megerősítést nyert, hogy a **pozitív PIT kurtosis hálózati szűk keresztmetszetre utal**, míg a negatív kurtosis a csekélyebb kihasználtságú, torlódásmentes kapcsolatok jellemzője. A nullához közeli kurtosis-t nehéz kiértékelni, de ez biztosan valamilyen torlódást takar a hálózatban.

Annak érdekében, hogy a passzív méréseken alapuló szűk keresztmetszet metrikákat megvizsgáljuk, számos méréssorozatot hajtottunk végre az egyik jelentős magyarországi szolgáltató hálózatában. Az adatok gyűjtésére és tárolására a Network Associates' Sniffer és Snifferbook Ultra eszközöket használtuk a Gigabit Ethernet interfészekre kapcsolva. Számos mérést végeztünk forgalmas órákban és azokon kívül is. Kapcsolódtunk a szolgáltató Internet Data Center-éhez, valamint maghálózati és hálózat-határi switch-ekhez és útvonalválasztókhoz. A mérések során hálózati szűk keresztmetszetek jelenlétében is gyűjtöttünk forgalmi adatokat.

A 4.1 táblázat néhány mérésre foglalja össze a PIT kurtosis számított értékeit. Az eredmények megfelelnek a korábban támasztott elvárásoknak. Torlódásmentes hálózati kapcsolatok esetében negatív értékeket kaptunk. Az útvonal torlódásának időszakában (ekkor nem a monitorozott link, hanem a monitorozó egységtől két ugrásnyira lévő ATM kapcsolat volt torlódott) a kurtosis pozitív értékeket vett fel, ami komoly szűk keresztmetszet jelenlétére utal. Ebben az időszakban jelentős csomagvesztést és 90%-os hálózati kihasználtságot figyeltünk meg.

4.1. táblázat. PIT kurtosis értékek az operátor hálózati kapcsolatain

Link name	normal conditions	OpR_1 overloaded
OpR_0 - $OpSW$	-0.46420	-0.45571
OpR_1 - $OpSW$	-0.06267	1.15119
OpR_2 - $OpSW$	-0.11180	-0.13289

3.3. altézis - Egy olyan elemző módszert alakítottam ki, amely segítségével hálózati szűk keresztmetszeteket lehet detektálni egy távolabb lévő, aggregált hálózati kapcsolat mérésével. [C2] [T1]

A hálózati szűk keresztmetszetek passzív monitorozással történő behatárolását nagyban korlátozza a tény, hogy az operátorok hálózatában kivitelezhetetlen minden egyes hálózati kapcsolat bemonitorozása. A gyakorlatban általában nagyon kisszámú nagysebességű aggregált kapcsolat passzív monitorozására van lehetőség hálózati szegmensenként. Ennek ellenére ha a topológia és az irányítási stratégia ismert, kevés méréssel és a mérések célzott "térbeli" és "időszaki" feldolgozásával a hálózati szűk keresztmetszetek felderíthetőek a szegmensben.

A folyamat első lépéseként az elemzendő forgalmat folyamokra kell bontani. Erre alkalmas módszer többek között az "5-tuple" alapú azonosítás, amelynél egy folyamot a küldő és a fogadó IP címei, a küldő és a fogadó portszámai és a használt kapcsolati protokoll (pl. TCP vagy UDP) azonosít. A topológia és az irányítási adatok alapján a folyam tipikus útja meghatározható ("térbeli", spatial analízis). Emellett a csomagbeérkezési időközök folyamonként és linkenként is külön-külön meghatározhatók ("időszakos, temporal analízis).

Amikor aggregált kapcsolaton vizsgáljuk, a PIT PDF mindig viszonylag lapos, az aggregálási szinttől függően. Az említett domináns tüskék akkor kezdenek feltűnni, ha a csomagokat a *küldési irány szerint elhatároljuk egymástól*. Gyakorlatilag ez irányonkénti szűréshez vezet (IP címtartományokra, MPLS címkékre, VPN azonosítókra). A folyamat addig folytatandó (egyre finomabb szűréssel), amíg a problémát okozó kapcsolatot fel nem fedezzük. Vizsgálataink során a hálózati topológia (beleértve az útvonalválasztók címeit és a használatos IP-címtartományok végződési helyeit) ismert volt. Ha ezek nem állnak rendelkezésre, a módszer akkor is működik, ellenben csak a méréssel szomszédos kapcsolatokra korlátozódik.

3.4. altézis - A hálózati szűk-keresztmetszet-detekcióhoz illesztettem, és a feladatra validáltam az M/G/R-PS beérkezési modellen alapuló "delay factor" mérőszámot. [C2] [C8]

A kapcsolati szintű folyamok beérkezési késleltetési faktora (delay factor) alapvető indikátorként alkalmazható számos hálózat-menedzsmenttel kapcsolatos vizsgálatban. Ez a mérőszám az M/G/R–PS tömegkiszolgálási modell egyik formulájának segítségével számítható, melynél csak a folyam beérkezési intenzitásának, a folyamok méretének és a link kapacitásának ismeretére van szükség. Az eredeti számítási módszernek vannak ugyan bizonyos korlátai abból következően, hogy a gyakorlatban előforduló kapcsolati szintű folyamok nem mindig felelnek meg az M/G/R–PS modell peremfeltételeinek; ezeket a kivételeket a számítás során kezelni kell, torzító hatásukat figyelembe kell venni.

Az M/G/R–PS késleltetési faktor (delay factor, DF) egy, eredetileg elasztikus folyamokra (lásd például [RPBP00]) definiált mérőszám: a folyamok átlagosan hálózaton töltött átviteli ideje (sojourn time) és az adott linken elérhető ideális átviteli idő hányadosa.

A DF a folyamok közötti beérkezési időkülönbségek felhasználásával is számítható. Az M/G/R–PS modell szerint a folyamokat (R) számú szerver szolgálja ki; ezt az értéket így határozhatjuk meg:

$$R = \lfloor C/r_{peak} \rfloor, \tag{4.2}$$

ahol C az adott aggregált link kapacitása, r_{peak} pedig a folyamok maximális átviteli sebessége – utóbbit a felhasználók hozzáférési sebessége határozza meg.

A modell szerint a hálózaton töltött idő (sojourn time) átlagos ideje az M/G/R–PS kiszolgáló-rendszerben:

$$E\{T(x)\} = \frac{x}{r_{peak}} \left(1 + \frac{E_2(R, R\rho)}{R(1-\rho)}\right) = \frac{x}{r_{peak}} \cdot f_R, \tag{4.3}$$

ahol x az átvitt folyam mérete, ρ a kapcsolat kihasználtsága, R a szerverek száma, f_R pedig a késleltetési tényező (DF). Az E_2 Erlang második formuláját jelzi. A kihasználtság a tömegkiszolgálásban gyakran használt módon, a beérkezési intenzitásból (λ_e), az átlagos folyam-méretből (x_{mean}), és a kapcsolat kapacitásából (C) számítható [RPBP00]:

$$\rho = \frac{\lambda_e \cdot x_{mean}}{C}. \tag{4.4}$$

Az M/G/R–PS modell M/G/1–PS modellé egyszerűsíthető abban az esetben, ha az r_{peak} csúcssebesség az aggregált link kapacitásánál nagyobb, vagy egyenlő vele. [RPBP00]. Itt ez az eset áll fenn. Ekkor a következő összefüggés – amely a 4.3 formulából adódik – egyetlen szerverrel is felírható:

$$f_R = 1 + \frac{E_2(R, R\rho)}{R(1-\rho)}. \tag{4.5}$$

Erlang második formulája az $R = 1$ feltételezéssel tovább egyszerűsödik, mivel $E_2(1, \rho) = \rho$. Ezek után a 4.5 összefüggésből ez adódik:

$$f_1 = DF = 1 + \frac{\rho}{1-\rho} = \frac{1}{1-\rho}. \tag{4.6}$$

Az M/G/R–PS modell alapján számított késleltetési faktor működésének ellenőrzéséhez a szimulációs vizsgálatok mellett több mérést is végeztünk, valós operátori környezetben. Egy ilyen vizsgálat környezete és eredményei a következők.

A passzív monitorozási mérés során a Gigabit Ethernet kapcsolaton 640 Mbit/s átlagos forgalom volt jelen (64% kihasználtság). Mivel a monitorozott hálózat topológiájáról korlátozottan álltak csak rendelkezésre az információk, a vizsgálatban szereplő útvonalválasztó routing-tábláját kellett elemeznünk, és egyszerűsített, egy-hopra kiterjedő topológiát használtunk. Ezen mérés során összesen 11 kapcsolatról (az operátor maghálózati linkjeiről) származó adatforgalmat gyűjtöttünk és elemeztünk munkatársaimmal. A késleltetési faktorral kapcsolatos beérkezési időn alapuló elemzéseket magam végeztem.

Mivel a méréshez használt eszköz memóriakapacitása erősen korlátozott volt, a megszakításmentes mérési intervallumok maximális hosszát ez határozta meg. Az elemzés egy periódusból állt, mely az egész mérési időszakra kiterjedt – így minden linkre minden mérce

4.2. táblázat. Az operátori hálózatban tapasztalt késleltetési tényezők

	linkA	linkB	linkC	lindD	linkE	linkF	linkG	linkH	linkI	linkJ	linkK
f_1	1.439	1.045	1.129	1.002	1.004	1.000	1.002	1.003	1.001	1.000	1.000
f_S	777.1	1084	813.6	759.9	697.3	1894	474.7	780.6	98.26	536.1	867.7

egyetlen értékét kaptuk. Az eredményeket a 4.2 táblázat foglalja össze; az f_1 a folyamok beérkezési idején alapuló, míg az f_S a "sojourn time"-on alapuló késleltetési faktort takarja.

Az f_1-re vonatkozó eredmények alapján megállapíthatjuk, hogy szűk keresztmetszetre utaló jeleket látunk a *linkA* és a *linkC*, irányában, ahol az értékek 1.439-re és 1.129-re adódtak. Ezeket MLL-ekhez (Managed Leased Line) kapcsolódó irányokként azonosította az operátor. Minden más kapcsolat torlódásmentesen továbbította a forgalmat, a késleltetési faktor értéke azoknál századra kerekítve 1 volt.

Az f_S metrikát vizsgálva feltűnik, hogy a késleltetési faktor szignifikánsan magasabb mint 1. Néhol még a komolyabban kihasznált kapcsolatokon is kisebb késleltetési tényező mutatkozott, mint az alacsony kihasználtságúakon. Ennek az a magyarázata, hogy a folyamok hálózaton töltött ideje (sojourn time) tág határok között mozoghat és a gyorsabbak nem tudják kiegyensúlyozni néhány extrém módon lassú folyam hatását. A mérce szórásával kapcsolatos túlzott érzékenysége miatt tehát sajnos nem alkalmas szűk-keresztmetszetek detektálására.

Miután a késleltetési faktor metrikát tovább finomítottuk az adattömeg formázásával, azt találtuk munkatársaimmal, hogy az így kialakult módszerrel [C8] még a fent leírtaknál is pontosabban indikáló mérőszámot kapunk. Az algoritmus azonban nagyon számításigényes, emiatt egyelőre nem használtuk hálózati szűk keresztmetszetek on-the-fly detekciójához.

3.5. altézis - Összehasonlítottam a "PIT-kurtosis"-t más lehetséges szűk-kereszt- metszet-mérőszámokkal, és megállapítottam, hogy a "PIT-kurtosis" mutatja ki a leginkább a szűk keresztmetszeteket. [J6] [C5]

Miután számtalan olyan metrikát megvizsgáltam, ami alkalmas lehet a hálózati szűk keresztmetszetek passzív monitorozással történő detektálására, azt találtam, hogy ezek különböző megbízhatósággal működnek különböző valós környezeti körülmények között. A *csomagvesztési ráta, sebesség-átlagok, folyamszintű áteresztőképesség szórása, késleltetési tényezők* kombinálása a végső döntést pontosabbá tehetik. Mindazonáltal *PIT kurtosis* használatát az esetek döntő többségében önmagában is elegendőnek találtam, mivel könnyű kiértékelni, nem nagy a számításigénye (gyors algoritmus), és a többieknél pontosabb eredményt nyújtott.

A magas *csomagvesztési ráta* egyes linkeken szűk keresztmetszet jelenlétére utal.

Az additív tulajdonságai miatt azonban ez a mérce önmagában nem használható jól a szűk keresztmetszetek indikálására, inkább csak egy komplex, több mércéből álló kiértékelő-logika részeként.

A *folyamsebesség-átlag* egy áteresztőképesség-jellegű mérce a kapcsolati szintű folyamok sebességének átlagát mutatja meg. Ez bizonyos helyzetekben jelezheti a szűk keresztmetszet jelenlétét, de leginkább csak akkor, ha a folyamsebességek szórása kicsiny, és sűrűségfüggvényük eléggé szimmetrikus.

Normális esetben (ha nincs durva torlódás a folyamok útjában) a *folyam-szintű áteresztőképesség szórására* elasztikus forgalom esetén magas értékeket várunk. Szűk keresztmetszet jelenlétekor azt feltételezhetjük, hogy ezek egyenlő részben osztoznak a sávszélességen, így áteresztőképességükre hasonló értékeket kapunk - ami csekély szóráshoz vezet csak. Elmélete szempontjából ez egy ígéretes metrika, bár számításigényes. A valós mérések során azonban többször adott hibás eredményt a szűk keresztmetszetek feltételezett jelenlétével kapcsolatban, így gyakorlati hatékonysága nem eléggé megalapozott.

A *késleltetési faktorok* pontosságáról az előző fejezetekben már esett szó: az M/G/R–PS alapú késleltetési faktor önmagában kicsit pontatlan, és bár előformázott adathalmazon jó indikátorként működik, ilyen előfeldolgozási igény mellett [J6] túlságosan számításigényes módszer.

A *skewness*, vagyis ferdeség az eloszlás harmadik centrális momentuma az átlagértékhez képesti aszimmetria jelzőszáma. A PIT eloszlásra számítva azt várjuk, hogy – mivel szűk keresztmetszetek esetén gyakrabban követik gyors egymásutánban a csomagok egymást – a sűrűségfüggvény az átlagtól balra vesz fel magasabb értékeket, ily módon lesz ferde. Ez a PIT skewness értékében egyre pozitívabb mutatók megjelenésén keresztül mutatkozik meg. A szimulációk során ez a mérce is jól mutatta a durva szűkítés jelenlétét, bár néhány esetben a kisebb sorbanállások esetén is szűk keresztmetszetet indikált, indokolatlanul. A valós mérések során minden esetben pozitív értékeket adott, így gyakorlati használhatósága erősen megkérdőjelezhető.

3.6. altézis - A hálózati szűk keresztmetszeti mércék és az érzeti szolgáltatásminőség (Quality of Experience (QoE)) közötti kapcsolatot vizsgálva megmutattam, hogy a magas "PIT-kurtosis" alacsony QoE-re utal. [C7] [J6] [C5] [C6]

A hálózatot használóknak és a hálózati szolgáltatásokat üzemeltetőknek sokszor eltér a véleménye a hálózat használhatóságát illetően. Az érzeti szolgáltatásminőség (Quality of Experience, QoE) vizsgálatával a felhasználó oldaláról minősíthetünk – ám a QoE mérése tömegeket célzó szolgáltatásoknál igen nehezen kiértékelhető, komplex feladat. Vizsgálataim alapján arra a következtetésre jutottam, hogy a szűk-keresztmetszet detektálásra használható mérőszámok alkalmasak lehetnek a QoE becslésére is. Ennek bizonyítására egy olyan mérési elrendezésben vizsgáltam munkatársaimmal a hálózati jellemzőket, amelyben a kialakított szűkítés mértéke változtatható. Az elemzések során megállapítottuk, hogy a tipikus QoS jellemzők, mint a throughput és a (TCP) csomagvesztés igazából kevés korrelációt mutatnak az QoE jellemzőkkel, azaz a felhasználó szempontjából érzékelt szolgáltatás-minőséggel. Ez már önmagában is érdekes eredmény. Megállapítottam továbbá, hogy az általam korábban bevezetett delay factor mérőszám, és különösen a PIT kurtosis mérce alkalmas lehet a felhasználói elégedettséggel kapcsolatos vizsgálatok alátámasztására. A valós mérések során egy aggregált hálózati kapcsolat képességeit szándékosan leszűkítettük, miközben azt a felhasználók folyamatosan használták. A minőségromlás számos szolgáltatás esetében (beleértve az audio streaming-et, peer-to-peer forgalmazást, Skype beszélgetéseket, Webböngészést) egyértelműen érezhető volt – ezt foglalja össze a 4.3. táblázat.

A mérések során a szűkítésen áthaladó csomagokat egy passzív monitorozó eszköz segítsévével rögzítettük. Több mérőszámot is használtunk annak érdekében, hogy valamelyik segítségével erős korrelációt tudjunk kimutatni a szűk keresztmetszet jelenléte és a szolgálta-

ABW	Video stream	Audio stream	Skype	P2P [kBps]	Web böngészés
7.0 Mbps	jó	jó	jó	33-95	jó
5.0 Mbps	esetenkénti blokkosodás	jó	jó	33-90	jó
4.5 Mbps	pici szünetek key-frame váltáskor	jó	jó	33-88	lassú
4.0 Mbps	másodpercnyi szünetek	jó	jó	12-14	lassú
3.5 Mbps	rossz; szünetek és blokkosodás gyakori	pici szünetek	szaggat	3-10	nagyon lassú
2.5 Mbps	nagyon rossz; élvezhetetlen	sok szünet	szaggat	3	használhatatlan

4.3. táblázat. A hálózati szolgáltatások érzeti minsége különféle szkítések esetén

tásminőség-romlás között. Ezen mércék között volt csomag- és folyambeérkezési-időkülönbségeken alapuló, csomagvesztésen alapuló, és olyan is, amelyik számításához a csomagméret ismeretét is felhasználtuk.

Az 4.6.a ábra a mérési elrendezést jeleníti meg, kiemelve a mesterséges szűkítés és a passzív mérőberendezés helyét. A 4.6.b ábra néhány érdekes mérési eredményt mutat be – a hét mérési alesetből kettő eredményeit emeltem ki példaképpen: a 7 és a 4.5 Mbps keskenyre szűkített aggregált link esetét. Amikor a rendelkezésre álló sávszélesség (available bandwidth, ABW) 7 Mbps volt, a hálózat még nem volt túlterhelve: minden alkalmazás rendesen működött, a felhasználók nem panaszkodtak. Ezzel szemben a 4.5 Mbps szűkítés esetén néhány alkalmazásnál már jelentkezett a szolgáltatásminőség-romlás. A kiértékelés során megállapítottuk, hogy az átlagos csomagvesztési arány, mint mérőszám, nem indikálja jól a torlódás mértékét. Hasonlóképpen az áteresztőképesség (throughput) sem alkalmas erre: a két bemutatott esetnél majdnem ugyanakkora ez a mérőszám. Ezekkel szemben az M/G/R–PS alapú késleltetési tényező, és méginkább a PIT kurtosis szignifikáns különbséget jelez a két eset között.

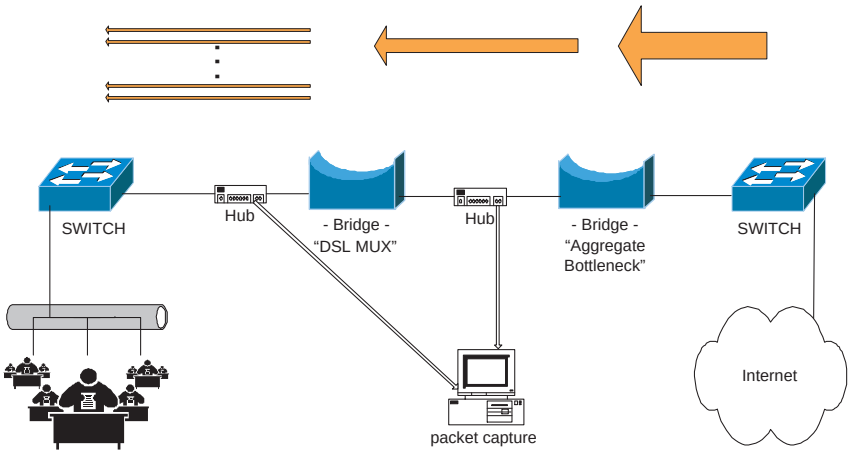
4.4. A tudás-sík és az SA keretrendszer összekapcsolása

---

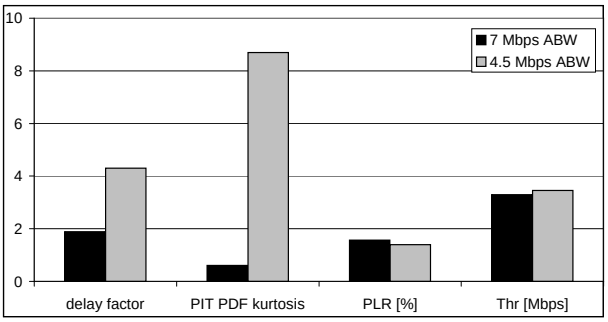
4. Tézis - Az autonóm hálózatok tudás-síkjában (Knowledge Plane) használható speciális monitorozási szolgáltatásokat definiáltam és hatékony forgalmi analízis módszereket vizsgáltam, különös tekintettel a forgalmi mix és a forgalmi mátrix elemzésekre. [J5] [J7]

A szolgáltatásminőség-biztosítási keretrendszer hibamenedzsment oldaláról és teljesítményvizsgálatok oldaláról történő megközelítése magában rejti a lehetőséget, hogy ez a keretrendszer akár gyakorlati megvalósítása is lehet bizonyos autonóm hálózati koncepcióknak. Az önmenedzselő, ön-konfiguráló és ön-optimalizáló hálózatok egyik lehetséges kialakítási módja a tudás-sik (Knowledge Plane, KPlane) bevezetésén keresztül valósul meg.

A témát felvető [CPRW03] szerzői azzal érvelnek, hogy az operátorok és a felhasználók oldalán is egyre több problémát okoz a tradicionális Internet komolyabb optimalizációjának hiánya. Az adatátvitel szempontjából transzparens maghálózatnak nincsenek ismeretei a rajta keresztülvitt adatokról, és még ha az intelligens határpontok (edge node) fel is figyelnek



a. Mérési összeállítás és a forgalmi arányok



b. Mérőszámok átlagértékei

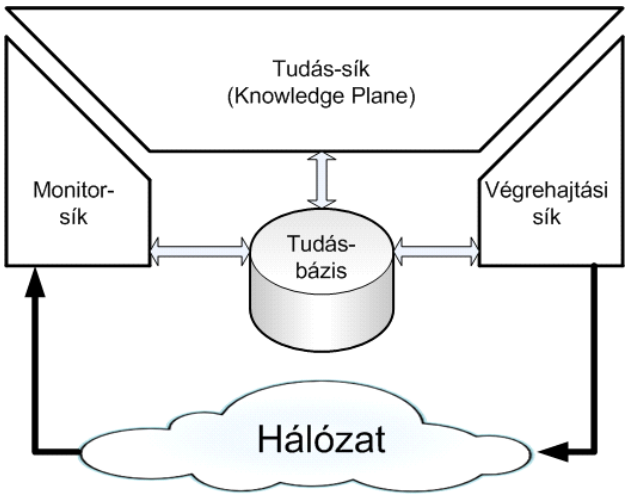
4.6. ábra. Mérési elrendezés és eredmények két, vizsgált szűkítési esetben [C7]

valamilyen probléma létezésére, nincs képességük annak meghatározására, hogy mit kellene tenni a megoldás érdekében.

A hálózat állapotáról és az átvitt forgalom jellegéről úgy szerezhetünk tudomást, ha gyűjtjük és feldolgozzuk az ezzel kapcsolatos adatokat. Ezek alapján már tehetünk lépéseket a felismert problémák megoldása felé – akár a korábban ismertetett SA keretrendszer használatával is. A témában kiindulópontnak tekinthető [CPRW03] cikk szerzői a használandó tudás kezelését az újonnan bevezetendő tudás-síkon (Knowledge Plane, KP) keresztül javasolja, mely kiegészíti a jelenlegi adat-síkból (Data Plane) és a vezérlési síkból (Control Plane) álló hálózati absztrakt teret. Az IST-MUSE projekt keretein belül a tudás síkot a gyakorlati megvalósítás felgyorsítása érdekében tovább bontották [VdMS+06], és bevezették helyette a monitor-sík, a tudás-sík és a végrehajtási sík (Monitor Plane (MPlane), Knowledge Plane (KPlane), Action Plane (APlane)) fogalmát, valamint bevezették az ezeket összekötő tudásbázist (Knowledge Base). Ezek és a hálózat kapcsolatát a 4.7. ábra szemlélteti.

Bár az elosztott tudás-sík koncepcióját a hálózatmenedzsment számos területén alkalmazzák, a forgalomanalízisből származó adatok KPlane-ben történő felhaszná- lásáról alig van jelzés az irodalomban. A következkben bemutatom (i) az SA ke- retrendszer és az elosztott tudás-sík kapcsolatát (ii) az MPlane-ben bevezetett skálázható forgalomanalízis koncepciót és (iii) a forgalmi mix és a forgalmi mátrix számítási módszereinek bizonyos részleteit.

4.1. altézis - Megmutattam a kapcsolatot a korábban általam megalkotott



4.7. ábra. A monitor-, tudás- és végrehajtási síkok kapcsolata a hálózattal [J7]

szolgáltatásminőség-biztosító keretrendszer és a jelenlegi autonóm-hálózati koncepciók: az MPlane, KPlane és APlane között.

Az SA keretrendszer bemenetén forgalmi- és státuszinformációk jelennek meg, míg kimenetén javaslat-tételi vagy automatikusan elvégzendő utasítások. Ugyanez igaz a tudás-sík (Knowledge Plane) megvalósított változazaira is. Az MPlane megfelel a hibadetektáló alrendszernek és interfészeinek, valamint a hibafelfeldolgozó alrendszernek. Az RCA és adatbányászati alrendszerek a KPlane funkcióját látják el. Az APlane műveletei megfeleltethetők a javaslattevő és végrehajtó alrendszernek és interfészeinek. A tudásbázist az AS keretrendszerben az eseményjelző és topológiai adatbázisok biztosítják.

Az MPlane fő funkciója az, hogy teljes és részletes rálátást biztosítson a hálózatra és szolgáltatásaira. Minden elem szintjén (hozzáférési csomópontok, útvonalválasztók, kapcsolók, tartalomszolgáltató szerverek, linkek stb.) monitorozza az elemek állapotát és a forgalmi paramétereket.

Bár a hálózati csomópontokba beépített monitorozó modulok jelenléte kényelmesnek tűnhet az adatgyűjtés szempontjából, ezek felépítésükből adódóan képtelenek nagy granularitású információk megosztására. Ezen okból kifolyólag a kiterjedt, magas terhelésű hálózatok forgalmi analízisére a passzív monitorozás módszere sokkal alkalmasabb.

4.2. altézis - Definiáltam egy olyan, széles határok között skálázható, elosztott adatgyűjtő és -elemző architektúrát az MPlane számára, amely még nagysebességű maghálózati kapcsolatoknál is alkalmazható.

A forgalom méretétől és az analízis mélységétől függően a részletes forgalmi vizsgálatot egy vagy több processzor tudja elvégezni. Annak érdekében, hogy a rendszer lépést tudjon tartani a folyamatosan növekvő forgalmi mennyiségekkel és a vizsgálatok egyre komplexebb jellegével, elosztottan kell működnie. Az elosztási hierarchia első szintjén gyűjtőállomások (capture probes) fogadják a csomagokat, időpecsételik és szűrik őket, majd az elosztási szabálytól és környezettől függően továbbítják az információkat a második szinten lévő egységeknek, a monitoroknak.

A gyűjtőállomások legfontosabb funkciói

- *Csomagok időpecsételése.* A hardware (firmware) segítségével adott időpecsét sokkal nagyobb pontosságú, mint a software-es, mivel eliminálja az operációs rendszer által bevezetett késleltetést;

- *Hardware-szintű szűrés.* A nagy sebességű hálózati forgalom (jelenleg 10Gbps vagy afelett) nem ad lehetőséget a forgalom on-the-fly szűrésére software-esen. A pontosan definiált, alacsony szintű szűrők nagyon hasznosak: drámai módon képesek csökkenteni a vizsgálandó adattömeg mennyiségét;

- *Beérkező csomagok csonkolása.* A hálózati forgalom-analízis legtöbb típusához nincs szükség a teljes IP-csomagra, csak annak kezdő szeletére;

- *Az előfeldolgozott adatok továbbítása.* A fentiek alapján kialakuló, tömörített csomaginformációt stukturálva kell továbbítani a monitoroknak, veszteségmentes csatornán.

4.3. altézis - Megvizsgáltam, kiválasztottam és használtam olyan hatékony algoritmusokat, amelyek segítségével forgalmi mix és forgalmi mátrix formában lehet analízis-eredményeket juttatni a KPlane-nek.

Forgalmi mátrix

A forgalmi mátrix egy hálózat-tervezési és fejlesztési eszköz. Kialakítása során alapvető folyamszintű QoS-statisztikák készülnek és rendelődnek össze forrás- és célútvonalakkal, hálózati szegmensekkel, vagy végpontpárokkal. Az analízis első lépéseeként a folyamok egy adat-n-es (n-tuple) alapján kerülnek definiálásra és így épülnek be vagy frissítődnek a folyam-adatbázisban. Leggyakoribb az 5-tuple használata (forrás- és cél-IP címek, forrás- és cél-portok, kapcsolati protokoll). Miután a megcélzott adatstuktúra tisztázásra került, maga a forgalmi mátrix-számítás kis komplexitású feladttá válik. Ilyen algoritmusokat találunk a [T3] forrásban. A mérés eredményét a statisztikák periodikus megjelenítése során is lehet használni, mellyel alátámaszthatók a hálózat-tervezési vagy szolgáltatás-marketing tevékenységek.

A jelenlegi forgalmi mátrixok normális esetben is tartalmazhatnak százezres nagyságrendű végpont-párokat. Különleges kihívás ilyen adatmennyiséget úgy ábrázolni, hogy az emberileg érthető legyen. Míg a nyers adatokat elérhetővé kell tenni a tudásbázisban, addig a vizuális megjelenítéshez elengedhetetlen valamiféle ésszerű csoportosításuk. Egy jó megoldás lehet a mátrix elemeinek hálózati szegmensenként való reprezentációja.

Forgalmi mix

A forgalmi mix analízise tulajdonképpen a hálózati alkalmazások azonosítását, eloszlásuknak meghatározását és az alkalmazásonkénti QoS meghatározását jelenti. A folyamokat statisztikai mutatók és ha szükséges, viselkedési heurisztikák segítségével osztályozzuk. Jelenleg az operátorok leginkább a következő alkalmazások minősítése iránt érdeklődnek: video stream, video konferencia, audio stream, VoIP és Peer-to-peer (P2P). Azt, hogy egy alkalmazás melyik forgalmi osztályba tartozik, statikus azonosítók (pl. portok), dinamikus

azonosítók (pl. változó portok, ujjlenyomatok), vagy csomagszintű, időszakos vagy térbeli, statisztika-alapú kiértékelési módszerek segítségével határozzuk meg. A saját forgalomanalízis gyakorlatomban alkalmazott VoIP, video és P2P azonosítási módszerek leírása sorrendben a [BMM+07], [T2], és [KBFc04] forrásokban található meg.

Amint a folyam meghatározásra került (pl. az 5-tuple alapján), különféle mérőszámok kerülnek kiszámításra a forgalmi osztály meghatározása érdekében. Ezek a mérőszámok a következők:

- *áteresztőképesség, throughput* - másodpercenként átvitt adatmennyiség;
- *csomagvesztés, packet loss* - az elküldött és ebből megérkezett csomagok számának különbsége;
- *csomagszintű késleltetés, packet delay* - a topológiától és a hálózati terheléstől függően a csomag beérkezése és elküldése között késleltetést tapasztalhatunk; emellett a csomagközi késleltetést is számításba vesszük;
- *csomagkésleltetési szórás, packet delay variation* - a csomagszintű késleltetések több adat-párra vonatkozó szórása;
- *körbefordulási idő, round-trip-time* - az interaktív alkalmazások gyors válaszokat igényelnek, ennek jelzőszáma ez a paraméter;
- *soron kívül érkező/duplikált csomagok, out of order/duplicated packets.*

5. fejezet

Az eredmények gyakorlati hasznosítása

Az 1. tézisben bemutatott szolgáltatásminőség-biztosítási keretrendszer először VoIP szolgáltatásokra volt prototípusként megvalósítva, az IKTA-00092-2002 program keretein belül. Eredményeit az Ericsson, a Kovax és a BME-TMIT hasznosította direktben. A keretrendszert ezután általánosítottam és többoperátoros Ethernet szolgáltatásokra is alkalmaztam. Utóbbit az IST-MUSE projekt hasznosította, melyben "Európa majdnem minden nagyobb, a szélessávú hozzáférés fejlesztésében szerepet játszó intézmény és vállalat" érdekelt volt.

A 2. tézisben bevezetett Petri-háló alapú RCA módszer a fenti SA keretrendszer központi eleme. Ennek köszönhetően az IKTA és az IST-MUSE programok résztvevői is használták. Alkalmazásuk részeként a Petri-hálók ütemezőjét is implementálni kellett, különféle Petri-háló alapú leírókat kellett kifejleszteni a felmerülő hibajegyekhez, és természetesen az elemi ellenőrző rutinokat is ki kellett alakítani.

A passzív monitorozáson alapuló hálózati szűk-keresztmetszeteket detektáló módszer, amely a 3. tézis alapja, először a BME-TMIT és az NTT-DoCoMo kutatólaboratóriumai használták párhuzamosan. Míg a szimulációk az M/G/R-PS-alapú késleltetési faktor használhatóságát sikeresnek mutatták erre a feladatra, a valós hálózati tesztek, melyeket a Magyar Telekom telephelyén végeztünk, már nem voltak mindig meggyőzőek. Később, amikor a PIT kurtosis módszerét kifejlesztettem, ezt is alávetettük a valós hálózati teszteknek. Ezen méréssorozatok és vizsgálatok során a PIT kurtosis-t a korábbi mércéknél sokkal alkalmasabbnak találtuk a hálózati szűk-keresztmetszetek detektálására. Mindezek mellett a PIT kurtosis számítási algoritmusa beépült az SGA1GEM eszközbe, amely egy hálózati QoS-tesztelő környezetet nyújt, Gigabit Ethernet kapcsolódási képességekkel. Ez a termék a Jedlik kutatási és fejlesztési program (NKFP2-00015/2005) támogatásával került kifejlesztésre. Az eszközt és a szűk-keresztmetszet detekciós módszert és metrikákat később számos éles feladat során is használtuk.

Az MPlane elosztott hálózat-analízis koncepciójának egy megvalósítása a SCALOPES C-board (mint gyűjtőállomás) és az elosztott monitorozó egységek. A kisfogyasztású C-board eszköz az ARTEMIS SCALOPES kutatási-fejlesztési projekt [T3] részeként valósult meg. Ez egy önálló, FPGA-alapú hardware, 2x 10 Gbps Ethernet és 16x 1 Gbps Ethernet interfészekkel felszerelve. A monitor-sík részeként használva ez előfeldolgozza a csomagokat, de ahelyett, hogy egyetlen CPU-nak adná tovább, elosztja azokat több monitor egység felé, 1 Gbps Ethernet interfészein. Ezek az egységek végzik a forgalmi analízis jelentősebb részét és szolgáltatják azok eredményeit a tudásbázis felé. Ezen vizsgálatok részei a forgalmi mix és

forgalmi mátrix számítások, amelyeket a 4. tézis is tárgyal. Ezt az eszköztárat használják az EUREKA projektben a CELTIC TIGER2 résztvevői. Itt az IP, GMPLS és Ethernet vezérlési folyamatok korrelációját a tudás-sík végzi, a monitor-sík által szolgáltatott forgalom-analízis eredményeinek alapján.

Köszönetnyilvánítás

Szeretném megköszönni mindazok segítségét, akik támogattak kutatásaim során. Külön köszönetemet szeretném kifejezni a következőknek:

- Tatai Péternek, aki megosztotta velem szakmai látásmódját, és folyamatos motivációval látott el kutatásaim és mérnöki munkám során,
- Gordos Gézának, aki bevezetett a híradásipari mérnökség területére, és folyamatosan támogatott tanulmányaim során,
- Marosi Gyulának, aki magas szintű mérnöki munkájával és személyes bátorításával segített kiszélesíteni képességeim határait,
- Moldován Istvánnak, Kún Gergelynek, Osváth Lászlónak és Bíró Józsefnek a kutatási területemmel kapcsolatos gyümölcsöző eszmecseréinkért, amelyek a távközlés, a szolgáltatás- és hálózatmenedzsment, valamint a sorbanállás elméletének területén segítettek eligazodni,
- minden kollégámnak az Ericsson-nál, Tecnomen-nél, AITIA-n and BME-n, mindazokért a kihívásokért, amelyekkel mérnökként és emberként is szembesültem,
- J.P. Martin-Flatin-nek, Aiko Pras-nak, Vattay Gábornak, Végh Jánosnak valamint munkáim számtalan névtelen ellenőrének, a segítőkész javaslataikért és kritikus megjegyzéseikért,
- és végül, de nem utolsó sorban családomnak, szeretetükért és mindazokért a csodálatos lehetőségekért, amelyek megadatottak nekem.

Köszönöm.

Irodalomjegyzék

[AETP04] A. Asgari, R. Egan, P. Trimintzios, G. Pavlou, Scalable monitoring support for resource management and service assurance. In *IEEE Network*, November/December2004.

[AFB+97] A. Aghasaryan, E. Fabre, A. Benveniste, R. Boubour, and C. Jard. A Petri net approach to fault detection and diagnosis in distributed systems/ In *Proceedings of the 36th IEEE Conference on Decision and Control, IEEE CDC'97*, San Diego, CA, USA, 1997.

[BMM+07] D. Bonfiglio, M. Mellia, M. Meo, D. Rossi, and P. Tofanelli. Revealing skype traffic: When randomness plays with you. In *SIGCOMM*, Japan, 2007.

[CPRW03] D.D. Clark, C. Partridgeo, J.C. Ramming, and J.T. Wroclawski. A knowledge plane for the internet. In *Conference on Applications, technologies, architectures, and protocols for computer communications*, Karlsruhe, Germany, 25–12 August 2003.

[Mei97] D.M. Meira A Model For Alarm Correlation in Telecommunications Networks Dilmar Malheiros Meira, 1997.

[IEE07] IEEE standard for local and metropolitan area networks - virtual bridged local area networks - amendment 5: Connectivity fault management, IEEE802.1ag, 2007.

[ITU92] ITU-T Recommendation X.700 - Management Framework for Open systems Interconnection (OSI) for CCITT Applications, 1992.

[KBFc04] T. Karagiannis, A. Broido, M. Faloutsos, and Kc claffy. Transport layer identification of p2p traffic. In *SIGCOMM*, Sicily, Italy, 2004.

[KK51] J. F. Kenney and E. S. Keeping. *Mathematics of Statistics*, volume 2. Princeton, NJ: Van Nostrand, 2nd edition, 1951.

[Kle75] L. Kleinrock. *Queuing systems, volume 1: Theory.* John Wiley and Sons, Inc., 1975.

[RPBP00] A. Riedl, M. Perske, T. Bauschert, and A. Probst, *Dimensioning of IP access networks with elastic traffic*, First Polish-German Teletraffic Symposium (PGTS 2000), Dresden, Germany, 2000.

[VdMS+06] B. De Vleeschauwer, W. Van de Meerssche, P. Simoens, F. De Turck, B. Dhoedt, P. Demeester, E. Gilon, K. Struyve, and T. Van Caenegem. On the enhancement of qoe for iptv services through knowledge plane deployment. In *Broadband Europe*, Geneva, Switzerland, 11–14 December 2006.

[ZO98] A. P. Zwart, O.J. Boxma, *Probability, Network and Algorithms (PNA), chapter Sojourn Time Asymptotics in the M/G/1 processor sharing queue*, PNA-R9802 ISSN 1386-3711, 1998.

Saját Publikációk

[J] **Folyóiratcikkek és könyvfejezetek**

[J1] P. Varga, I. Moldován, and G. Molnár. Komplex hibamenedzsment megoldás VoIP-szolgáltatások felügyeletéhez. *Híradástechnika*, 60,10:50–55, October 2005.

[J2] P. Varga, I. Moldován, and G. Molnár. Complex fault management solution for voip services. *Infocommunications Journal*, 60,12:15–21, December 2005. selected papers.

[J3] P. Varga. Analyzing packet interarrival times distribution to detect network bottlenecks. In *EUNICE 2005: "Networked Applications" 11th Open European Summer School.*, pp.17–29. Springer, 2006.

[J4] P. Varga and I. Moldován. Integration of service-level monitoring with fault management for end-to-end multi-provider ethernet services. *IEEE Transactions on Network and Service Management*, 4:28–38, 2007.

[J5] P. Tatai, P. Varga, and Gy. Marosi. Távközlő hálózati folyamatok monitorozása. *Híradástechnika*, 62,8:49–55, August 2007.

[J6] P. Varga, G. Kún, and G. Sey. Towards estimating quality of experience with passive bottleneck detection metrics. In *Advances in Information Systems Development: New Methods and Practice for the Networked Society*, pp.115–125. Springer, 2007.

[J7] P. Varga and L. Gulyás. Traffic analysis methods to support decisions at the knowledge plane. *Infocommunications Journal*, 65,10, October 2010.

[J8] P. Varga, I. Moldován, D. Horváth, and S. Plósz. A low power, programmable network platform and development environment. In *Advances of Network- Embedded Management and Applications*, Chapter 2., pp.19–36. Springer, 2010.

[J9] P. Varga, A. Kőrösi, A. Gulyás, and J. Bíró. Stochastic Bounds on the Expected Loss Ratio in Deterministic Queuing System Models. to appear.

[C] **Konferenciacikkek**

[C1] P. Varga, G. Kún, P. Fodor, J. Bíró, D. Satoh, and K. Ishibashi. An advanced technique on bottleneck detection. In *IFIP WG6.3 Workshop, EUNICE 2003*, Balatonfüred, Hungary, 2003.

[C2] P. Varga and P. Tatai. Advanced Methods in GPRS Network Analysis. In *IFIP WG6.3 Workshop, EUNICE 2004*, Tampere, Finland, 2004.

[C3] P. Varga and G. Kún. Utilizing higher order statistics of packet interarrival times for bottleneck detection. In *IFIP/IEEE Workshop on End-to-End Monitoring Techniques and Services (E2EMON)*, Nice, France, 2005.

[C4] P. Varga, I. Moldován, and G. Molnár. Voip szolgáltatások hibamenedzsmentje. In *14. NIIF Networkshop*, Szeged, Hungary, 2005.

[C5] P. Varga, G. Kún, and G. Sey. A qos mérőszámok és a felhasználói elégedettség közötti kapcsolatok. In *15. HTE Távközlési és Informatikai Hálózatok Szeminárium*, Eger, Hungary, 2006.

[C6] P. Varga, G. Kún, and I. Moldován. Correlation of advanced bottleneck metrics and quality of experience. In *9th IEEE/IFIP Asia-Pacific Network Operations and Management Symposium, APNOMS*, Busan, Korea, 2006.

[C7] P. Varga, G. Kún, G. Sey, I. Moldován, and P. Gelencsér. Correlating user perception and measurable network properties: Experimenting with qoe. *Autonomic Principles of IP Operations and Management*. Lecture Notes in Computer Science, LNCS 4268, pp.218–221, Springer, 2006.

[C8] G. Kún, and P. Varga. Utilizing MGR-PS Model Properties for Bottleneck Characterization. In *World Telecommunications Congress, WTC 2006*, Budapest, Hungary, 2006.

[C9] P. Varga, J. Bíró, M. Martinecz, and Z. Heszberger. QoS Provision for Bufferless Statistical Multiplexing. In *International Conference on Telecommunication Systems, Modeling and Analysis: ICTSM 2009.*, Dallas, TX, USA, 2009.

[C10] S. Plósz, I. Moldován, P. Varga, and L. Kántor. Dependability of a network monitoring hardware. In *3rd IARIA International Conference on Dependability, DEPEND 2010*, Venice, Italy, 2010.

[T] **Műszaki Tanulmányok**

[T1] P. Varga, I. Moldován, T. Dinh Dang, Cs. Simon, G. Kún, and P. Tatai. Developing a passive measurement-based methodology for detecting network bottlenecks in ip networks. Technical report, Study for Hungarian Telecom, in Hungarian, 2004.

[T2] P. Varga, L. Kovács, I. Moldován, A. Illés, G. Kún, G. Sey, and G. Turzó. Analysis of media communication over the internet. Technical report, BME Report for Hungarian Telecom, 2007.

[T3] P. Varga, I. Moldován, G. Kródi, G. Sey, L. Kovács, D. Horváth, and S. Plósz. Report on new architectural platform and specification of example sw code for analysis. Technical report, ARTEMIS SCALOPES Deliverable DA1.3., AITIA, BME, 2010.

[R] **Mások által hivatkozott publikációim**

[R1] C. Marquezan, A. Panisson, L. Granville, G. Nunzi, and M. Brunner. Maintenance of monitoring systems throughout self-healing mechanisms. *Managing Large-Scale Service Deployment*, 20,2:57–70, Lecture Notes in Computer Science, LNCS 5273, pp.176–188, Springer, 2008., cited [J4]

[R2] C. Jagadish and T. A. Gonsalves. Distributed control of event floods in a large telecom network. *International Journal of Network Management*, 20,2:57–70, John Wiley and Sons, 2009., cited [J4]

[R3] M. Miyazawa and T. Otani. Real-time root cause analysis in OSS for a multi-layer and multi-domain network using a hierarchical circuit model and scanning algorithm Source. In *11th IFIP/IEEE international conference on Symposium on Integrated Network Management*, IEEE Press, 2009., cited [J4]

[R4] N. Pogkas, N. Ploskas, G. Panagopoulos, and N. Fleischer. VICTORY open-source middleware framework and prototypes of P2P network entities. *Deliverable 3.3, IST-VICTORY*, 2009., cited [C7]

[R5] E. Ibarrola, F. liberal, I. Taboada, and R. Ortega. Web QoE Evaluation in Multi-agent Networks: Validation of ITU-T G.1030. In *5th IARIA/IEEE International Conference on Autonomic and Autonomous Systems*, Valencia, Spain, 2009., cited [C7]

[R6] O. Dini, P. Lorenz, A. Abouaissa, and H. Guyennet. Dynamic Feedback for Service Reputation Updates. In *6th IARIA International Conference on Autonomic and Autonomous Systems*, Cancun, Mexico, 2010., cited [C7]