

Útvonalkijelölés és forgalomelvezetés több tartományú kapcsolt optikai hálózatokban

SZIGETI JÁNOS*, TAPOLCAI JÁNOS***, RÉTVÁRI GÁBOR,
LÁPOSI LEVENTE, CINKLER TIBOR***

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

Kulcsszavak: GMPLS, optikai útvonalválasztás, optikai PNNI, kapcsolt optikai hálózatok szimulációja

Cikkünkben ismertetjük azon útvonalválasztási technikákat, melyek esélyesek vagy legalábbis hatást gyakorolnak a jövő többretegű, több tartományú, több szolgáltatást támogató hálózatainak útvonalválasztási technikáira. E többretegű hálózatokban a dinamikus útvonalválasztáshoz szükséges, hogy az optikai eszközök is támogassák a kapcsolási funkciót. Bemutatjuk, hogy milyen szabványosítások születtek, és a jelenleg elterjedt protokollok milyen módosításokat igényelnek. Az áttekintés után ismertetjük saját fejlesztésű szimulációs környezetünket, mely segítségével értékeljük ki javasolt új módszereinket, példaként az információ-terjesztés késleltetésének hívásblokkolásra gyakorolt hatását vizsgáljuk.

1. A GMPLS-ről

1. Áttekintés

Napjainkra nyilvánvalóvá vált, hogy a jelenlegi hálózati infrastruktúra képtelen megbirkózni azokkal a kihívásokkal, melyeket a mind nagyobb volumenű és mind változatosabb minőségi követelményeket támasztó adatátviteli igények jelentenek. A szakértők ennek egyik okát az architektúra túlzott rétegződésében látják, mivel a mai adatátviteli hálózatokban egyszerre van jelen a csomagkapcsolt IP és a virtuális áramkör alapú technika, mint az ATM vagy az MPLS (*MultiProtocol Label Switching*), a gerinchálózatban pedig többnyire az időosztásos SONET/SDH rendszer biztosít hozzáférést a fizikai réteg erőforrásaihoz. Míg az egymásba ágyazott infrastruktúra egységes menedzsmentje így szinte lehetetlenné válik, addig a rendszer összteljesítményét többnyire a leggyengébb láncszem korlátozza feleslegesen.

Az előrejelzések azt mutatják, hogy a felhasználói forgalom domináns része továbbra is IP alapú lesz, azonban a QoS követelmények igen sokrétűvé válhatnak. Pillanatnyilag az IP forgalom számára QoS-t, a szolgáltató számára pedig forgalom-menedzsmentet (Traffic Engineering, [1]) biztosító adatátviteli szolgáltatások bevezetésére az MPLS [2] tűnik a legnépszerűbb választásnak. Így kézenfekvő egy olyan vezérlési sík (control plane) definiálása és szabványosítása, mely

MPLS-alapokon teszi lehetővé a jövő heterogén optikai hálózatainak költséghatékony üzemeltetését és menedzsmentjét. Ez a technológia a GMPLS (*Generalized MPLS*, [3]).

A GMPLS keretrendszer a különböző hálózati rétegeket nyálábolási (multiplexálási) képességük és adatátviteli sebességük szerint többszintű hierarchiába szervezve kezeli, ahol az alsóbb rétegek a felsőbb rétegek forgalmát transzparens módon adatátviteli csatornába (tunnel) nyálábolják. Az egyes csatornákat általánosított címkével azonosítjuk és ezeket a rétegeket az IP alapú útvonalválasztási funkció virtuális összeköttetésként érzékeli. A címke adott hálózati rétegben nyeri csak el konkrét jelentését: lehet IPv6 flow label, MPLS címke, ATM VPI/VCI, időrés azonosító egy időosztásos rendszerben, hullámhossz egy frekvenciaosztásos rendszerben (DWDM) vagy akárgy bizonyos szál egy üveg-szálás térosztásos architektúrában.

A GMPLS keretrendszer elemeit a táblázatban, illetve az 1. ábrán foglaljuk össze.

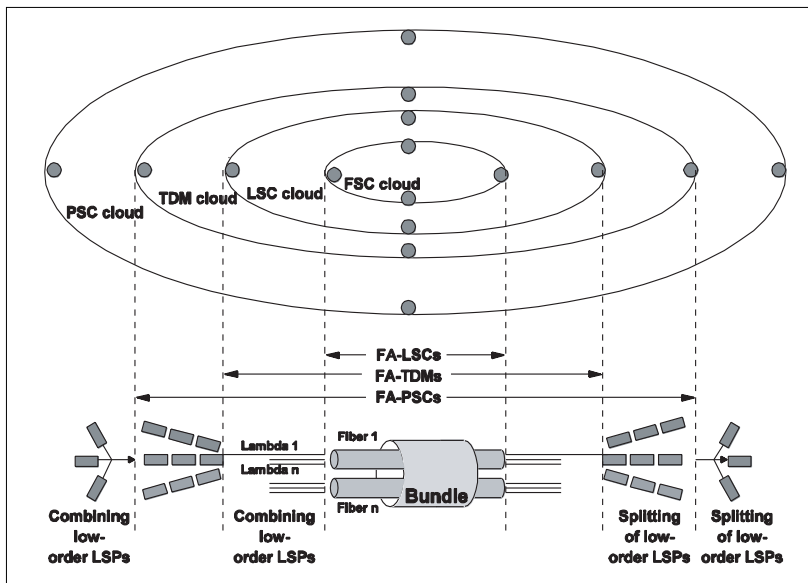
A GMPLS szabványosítása az Internet Engineering Task Force (IETF) Common Control and Measurement Plane (CCAMP) munkacsoportjában történik. A definiált

Kapcsolási tér	Infrastruktúra	Nyalábolás	Címke	Eszköz	GMPLS elnevezés
Csomag, cella	IP, ATM, Frame Relay, Ethernet	Csomag-szint	shim header, ATM VPI/VCI	IP router, ATM switch	Packet-switching capable (PSC)
Idő	PCM, SONET/SDH, stb.	TDM	időrés	digital cross-connect (DCS), add-drop multiplexer (ADM)	TDM capable (TSC)
Hullámhossz, frekvencia	Transzparens	WDM, FDM	Lambda (hullám-hossz)	DWDM ADM/OXC	Lambda-switching capable (LSC)
Fizikai tér	Transzparens	SDM	üveg-szál	OXC	fiber-switching capable (FSC)

* A szerzőt az ETIK (www.etik.hu) támogatta.

** A szerzőt az OTKA a T 42559 számú szerződés keretében támogatta.

*** A szerzőt az MTA János Bolyai Alapítványa, az OM OTKA a 42211számú Posztdoktori Szerződés keretei közt, valamint az ETIK támogatta.



1. ábra GMPLS hierarchia

kiterjesztések két fontos területre különülnek el: az adatátviteli sík (data plane) módosításaira illetve a vezérlési sík módosításaira. Az alábbiakban vázlatosan áttekintjük ezeket a módosításokat.

2. GMPLS: adatátviteli sík

A GMPLS általánosítja az MPLS címke fogalmát. Míg az MPLS-ben egy címke egy bizonyos virtuális áramkört jelöl és lehetővé teszi a virtuális áramkörben haladó IP csomagok gyors kapcsolását, addig – mint azt az előző fejezetben láttuk – a GMPLS-ben egy címke gyakorlatilag bármilyen olyan forgalmi egységet azonosíthat, amelyet adott hálózati réteg egységesen kezel. A GMPLS-ben egy címke-kapcsolt útvonal (LSP, Label-Switched Path) két, azonos rétegbeli eszköz között kifeszített tetszőleges virtuális áramkört jelölhet. Így megvalósítható a rétegek egységes menedzsmentje, mert az útvonalválasztó vagy a hálózatmenedzsment szoftvernek már nem kell az egyes architektúrák sajátosságaiával törődni, hanem elég egy adott virtuális áramkört az általánosított címkével azonosítani. Az MPLS-től eltérően a GMPLS lehetővé teszi a jelzési és az adatátviteli csatornák logikai és/vagy fizikai szétválasztását (out-of-band signaling), mivel például az optikai kapcsolóeszközök nagy többsége nem képes a sávon belüli jelzési információ kinyerésére és kezelésére.

3. GMPLS: jelzési sík

A GMPLS legfontosabb célterülete az ASON környezet. Ahhoz, hogy lehetővé váljék az automatikus LSP kiépítés, menedzsment és lebontás függetlenül a hálózati réteg konkrét megvalósításától, számos tekintetben ki kell terjeszteni a hagyományos MPLS jelzési protokollokat (CR-LDP, RSVP-TE, [4], [5], [6], [7]). Ezek tartalmazzák az alapvető MPLS forgalommenedzsment funkciókat [8], úgy mint explicit forrás-routing (strict/loose), útvonalrögzítés (route-pinning), QoS támogatás, hurokdetektálás, és preemptálhatóság. A GMPLS megvaló-

sítása azonban olyan gyökeres változtatásokat követel, mint a sávon kívüli jelzésrendszer, a kétirányú LSP vagy az általánosított címke bevezetése. A kétirányú LSP-k koncepciója nemcsak felhasználói igényeket elégít ki, de lehetővé teszi olyan alapvetően kétirányú média integrálását is a GMPLS keretrendszerbe, mint a SONET/SDH [9]. Hasonlóan, az optikai rendszerek mind hatékonyabb kezelése érdekében került bevezetésre a javasolt címke (suggested label) és a kiterjesztett hibakezelés (error notification) fogalma.

A hagyományos MPLS jelzési protokollok GMPLS általános kiterjesztését a [10] ismerteti, míg a protokoll-specifikus kiterjesztéseket a [11] és az [12] szabványok specifikálják.

Az IP alapú útvonalválasztó protokollok [13] folyamatos bővítésen mennek keresztül annak érdekében, hogy megfeleljenek napjaink új kihívásainak, például a QoS útvonalválasztásnak, stb. Hasonlóan, a GMPLS útvonalválasztási funkciók is a hagyományos IP routing protokollok kiterjesztéseként valósíthatóak meg [14], [15]. Ezen kiterjesztések központi kérdése a skálázhatóság, hiszen a DWDM bevezetésével az útvonalválasztó protokollnak képesnek kell lenni két kapcsolóeszköz között párhuzamos csatornák akár százait is kezelni. Ezenkívül fontos szempont a sávon kívüli jelzések vagy az egyes rétegek eltérő granularitású címketerének megfelelő használata illetve a védelem és helyreállítás (protection and restoration) biztosítása meghibásodások esetére.

A GMPLS útvonalválasztási kiterjesztéseinek lényege, hogy az LSP-k virtuális összeköttetéseként kerülnek meghirdetésre a hálózatban, pontosan specifikálva azok nyalábolási képességeit és védelmi tulajdonságait (osztott, 1:1, 1+1, stb). Az útvonalválasztó algoritmus ezek után különösebb módosítások nélkül is képes figyelembe venni ezeket az LSP-eket útvonalválasztási döntése meghozatalakor. A sávon kívüli jelzések továbbítására szolgáló jelzési csatornák is megjelennek az útvonalválasztási információk között, azonban speciális attribútumok biztosítják, hogy ezekre adatforgalom ne kerülhessen. Az esetlegesen igen nagyszámú párhuzamos összeköttetés számára nem kell interfészenként egyedi IP címet lefoglalni (ami súlyos skálázhatósági és menedzsment nehézségeket vetne fel), hanem ezek ún. számozatlan (unnumbered) interfészek közötti virtuális összeköttetésekbe vonhatók össze (link bundling). Fontos megjegyezni, hogy míg a GMPLS útvonalválasztási architektúra már szabványosított és kereskedelmi forgalomban kapható [16], addig maga az útvonalválasztási algoritmus, mely védelemmel ellátott hatékony és QoS szempontjából is megfelelő útvonalak kiszámítására is képes, még nem került definiálásra. A GMPLS útvonalválasztási specifikumainak igen jó összefoglalása olvasható a [17]-ben.

A sávon kívüli jelzésrendszer és a nem csomagkapcsolt hálózati rétegek egységes menedzsmentje olyan kulcsfontosságú problémákat vet fel a GMPLS-ben, mint a dedikált jelzéscsatornák menedzsmentje, vagy az általánosított címkék konzisztenciájának biztosítása a szomszédos kapcsolóelemek között. Ezekre a feladatokra a GMPLS egy speciális protokollt, az LMP-t (Link Management Protocol [18]) használja. A kétirányú dedikált jelzéscsatornák igény szerint felépíthetők és lebontathatók, folyamatos fenntartásukról az LMP Hello protokoll gondoskodik (Control Channel Management). A számozatlan interfészek címezését, védelmi tulajdonságait és prioritását (Link Property Correlation) és az összeköttetések működőképességének biztosítását, illetve hiba esetén a hiba helyének azonosítását és a hiba-kezelést is az LMP végzi.

A GMPLS bevezetése számos nehézséget róhat a szolgáltatóra, ezért a költségek leszorítására az IETF CCAMP munkacsoport módszereket dolgozott ki a GMPLS kisebb lépésekben történő bevezetésére [19]. Mivel a GMPLS által orvosolni kívánt problémák egyre sűrűbben jelentkeznek napjaink heterogén adatátviteli hálózataiban, ezért az architektúra mind fokozottabb elterjedésére lehet számítani az elkövetkező években.

2. OSPF-BGP – mint működő megoldás

Az optikai hálózatok útvonalválasztásához egy lehetséges alternatíva az IP (*Internet Protocol*) központú vezérlési modell. Ennek létjogosultsága az IP hálózatok elterjedtségében rejlik, ami az optikai hálózatok felett is gyakran alkalmazott réteg. További előnyt jelentenek az IP megbízható, jól működő útvonalválasztó protokolljai (*routing protocol*). Egy meglévő, működő megoldást mindig könnyebb fejleszteni, kiegészíteni, mint a komplett rendszert valami újra cserélni. Emiatt látjuk célszerűnek részletesen foglalkozni az IP hálózatokkal, a protokolljaival és azok lehetséges továbbfejlesztésével.

A legjobban adaptálható megoldás az OSPF-BGP útvonalválasztó protokoll páros. Két útvonalválasztó protokoll kombinációja azért szükséges, mert különböző feladatokra tervezeték őket. Az OSPF (*Open Shortest Path First*) egy Interior Gateway Protokoll (IGP), amely az autonóm rendszereken (AS – *Autonomous Systems*) belüli kommunikációban játszik szerepet. A BGP (*Border Gateway Protocol*) egy Exterior Gateway Protokoll melynek az AS-ek közötti együttműködésben van szerepe. Az autonóm rendszerek a nagy hálózatokat (skálázhatósági és adminisztrációs) szempontból szétbontják kisebb egységes menedzsmentet (és routingot) működtető hálózatokra.

Az IP csomagkapcsolt hálózatokban az összes OSPF útvonalválasztó (*OSPF router*) minden egyes bejövő csomagra külön-külön mindig elvégzi az útvonalválasztást. Az OSPF egy ún. *szakaszállapot* (link-state) protokoll, melyet az IETF fejlesztett ki. A link-state protokollok működése két részből áll. Először

minden router felderíti a hálózat topológiáját, majd a kapott gráfban minden csúcshoz megkeresi a legrövidebb elérési utat és az úthoz tartozó első szakaszt, amelyen továbbítani fogja a csomagot.

Az elosztott struktúra miatt fontos, hogy az útvonalválasztókban levő topológia megegyező legyen, és így a legrövidebb út kiszámításakor mindenhol ugyanazt az eredményt kapjuk, különben inkonzisztencia alakul ki, ami odáig fajulhat, hogy egy csomag két vagy több csomópont alkotta hurkon körbe-körbe kering, és így a célállomást sosem éri el.

Az útvonalválasztás konvergenciája kritikus a rendszer stabilitása szempontjából. A hálózat topológiáját a szakaszok állapotát leíró rekordok (link-state records) terjesztésével tudatják egymással az állomások. A szakaszok állapotát leíró rekordokat szétküldik a hálózatban, ezt nevezzük flooding mechanizmusnak. A hálózat csomópontjai a kapott rekordokat feljegyzik saját topológiai adatbázisukba, majd továbbadják. Ha olyan rekordot kapnak, amely már szerepel az adatbázisban, de annál régebbi verziójú, akkor eldobják. Ezzel megakadályozzák, hogy egy-egy rekord örökké keringjen a hálózatban.

Amikor egy szakasz meghibásodik, a két végén levő csomópont észleli ezt, és mindketten körbeadnak egy üzenetet, hogy a kérdéses szakasz költsége végtelen. Mivel erről mindenki értesül, a topológiai adatbázisok szinkronban maradnak. Az OSPF link-state működése miatt nagy hálózatokat nem célszerű építeni, hiszen a flooding mechanizmus túlságosan leterheli a hálózatot. A probléma megoldására az egyes OSPF útvonalválasztókat *tartományokba* (*Area*) lehet szervezni. Valamennyi tartomány egy speciális tartományhoz az Area 0-hoz kapcsolódik és az útvonalválasztók topológia adatbázisa egy tartományon belül azonos. Az egyes területek között kitüntetett ún. Area Border Routerek (ABR) gondoskodnak az információk cseréjéről.

Az OSPF hierarchia a szerkezeti kötöttsége miatt nem bővíthető a gyakorlatban. Ezért a hierarchiabővítés következő lépcsőfoka az AS-ek közötti együttműködést megvalósító BGP lesz. A BGP az Internet növekedésével fejlődött ki mostani formájára. Jelenleg a BGP negyedik verzióját használjuk, amely 1995 márciusában készült el [RFC1771].

A BGP elsődleges funkciója a hurkok megszüntetése a hálózatban. Erre egy, az OSPF-ben látottól eltérő megoldást, az út-vektorokat (path vectors) használja. A módszer lényege, hogy minden terjesztett útvonalban a célpontig vezető teljes utat leírjuk. Így a hurokmenteséget minden útvonalválasztó könnyen ellenőrizheti: ha egy kapott útvonalban már szerepel, eldobja a csomagot. Így nincs szükség az egész Internetben egységes költség definiálására, minden router a teljes útvonalat saját szempontjai szerint pontozza. Az eljárás hátulütője a nagy memóriaigény.

Minden út-vektorban szerepel az AS-ek egy listája, és ki van egészítve különböző attribútumokkal. A BGP útvonalválasztók nem csupán a szomszédos AS-ben levő BGP útvonalválasztókkal építenek ki kapcsolatot,

hanem a saját AS-ükben lévővel is. Az előbbieket külső, az utóbbiakat belső partnereknek nevezzük (external peer, internal peer). A belső kapcsolatra a hatékony információterjesztés miatt van szükség, mert ha az útvonalválasztó út-vektorokat kap egy külső partnertől, akkor azokat el kell juttatnia az AS összes többi BGP útvonalválasztójához, hogy azok továbbadhassák.

Természetesen a BGP átadja az elérhetőségi információt az OSPF-nek, hogy az OSPF útvonalválasztók is tudjanak a külső célpontokról, de az út-vektorok átadása a BGP kapcsolaton zajlik. Ezen keresztül egyeznek meg a BGP útvonalválasztók abban is, hogy több lehetséges külső útvonal közül melyiket használja az AS (ezt adják át az OSPF-nek) és hogy mit terjesszenek kifelé. Szigorú harmóniának kell uralkodnia ugyanis abban, hogy milyen útvonalat adnak át az OSPF-nek és milyen hálózatok elérhetőségét terjesztik kifelé, hiszen a kintről érkező csomagokat a belépő útvonalválasztótól az AS-en keresztül az OSPF fogja eljuttatni a kilépő BGP útvonalválasztóhoz.

Az IETF kiterjesztette az OSPF-et optikai hálózatokra [20], a BGP optikai hálózatokon való alkalmazhatóságának kutatása (OBGP [21]) jelenleg háttérbe szorult.

3. PNNI alkalmazása optikai hálózatokban

A PNNI (*Private Network to private Network Interface*) egy „link-state” útvonalválasztó protokoll, amelyet az ATM Forum (<http://www.atmforum.org>) hozott létre és szabványosított az ATM (*Asynchronous Transfer Mode*) hálózatok összekapcsolási és útvonalválasztási problémáinak megoldására.

Bár az ATM kapcsolatorientált, mégis szükség van egy a datagram jellegű hálózatokban megszokott útvonalválasztásra a kapcsolat felépítésekor, hiszen ilyenkor még nincs semmiféle kiépült útvonal, amit a jelzés követhetne.

Ilyen módon számos hasonlóságot mutat az OSPF-BGP útvonalválasztási protokollokkal, azonban a PNNI minden eddiginél összetettebb. Egyrészt a skálázhatóság követelménye, másrészt pedig a QoS (*Quality of Service – Szolgáltatásminőség*) támogatás miatt. Viszont pontosan ezek a tulajdonságok azok, amelyek egy optikai hálózati útvonalválasztó protokollnál jó kiindulópontot jelentenek.

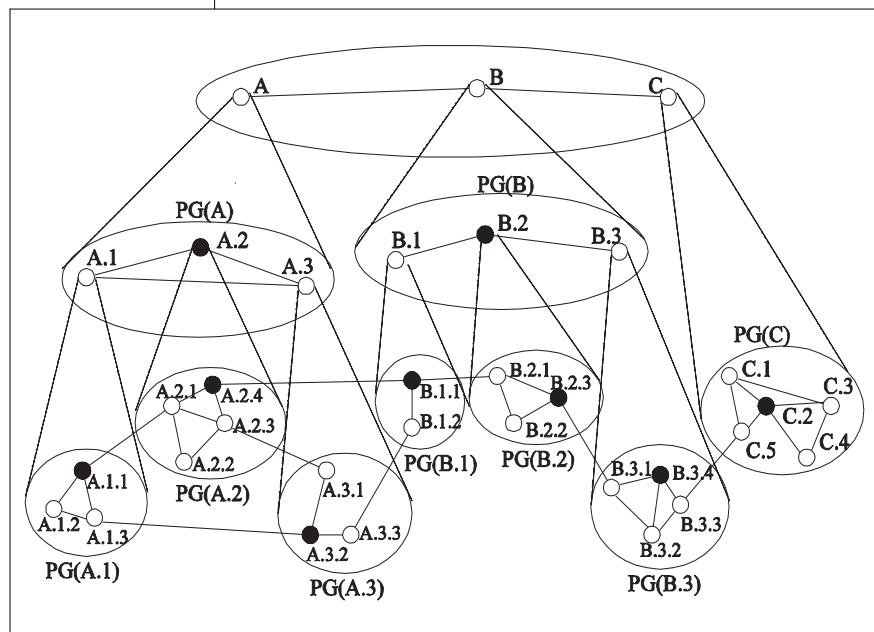
A PNNI protokoll két részből tevődik össze: a PNNI útvonalválasztó protokollból és PNNI jelzési protokollból. Cikkünkben csak a PNNI útvonalválasztó funkciójára térünk ki, amelynek feladata hálózati topológia és elérhetőségi információk terjesztése az ATM kapcsolók között.

Tekintsük át a PNNI jellemzőit!

1. Link State

A PNNI link-state protokoll, azaz minden kapcsoló információkat tárol a hálózat topológiájáról. Ez azonban nemcsak a szakaszok, hanem a kapcsolók adatait is tartalmazza, minthogy ez is befolyásolhatja a rendelkezésre álló erőforrásokat. Az adatok minőségi paramétereit is tartalmaznak, mint a maximális késleltetés, késleltetés-ingadozás, cellavesztés, sávszélesség stb. Ezeket az információkat PTSEs (PNNI Topology State Elements) üzenetek formájában terjesztik a kapcsolók egymás között. Így minden kapcsoló áttekinthető képpel rendelkezik a hálózat képességeiről és éppen aktuális terheltségéről. Ezek a leírások nagyon egyszerűen kiterjeszthetők lennének további (pl.: hullámhossz) információkkal is. Hasonlóan érvényes ez a kapcsolókra vonatkozóan, ahol pedig a hullámhossz konverziós képességeit lehetne hirdetni a hálózatban.

A PNNI a szomszédok, és a szakaszok felderítését a Hello protokoll segítségével végzi. A Hello és PTSE csomagokat periodikus rendszerességgel adják egymásnak a kapcsolók. A PTSE-k terjesztése az OSPF-ben leírtakhoz hasonlóan történik.



2. ábra PNNI hierarchia

2. Hierarchikus topológia

Mint láttuk az OSPF-nél, egy link-state protokoll nem szolgálhat ki korlátlan méretű hálózatot, a topológiai adatbázis mérete miatt. A PNNI viszont a QoS támogatás mellett a nagy hálózatokban igényelt skálázhatósági követelményeknek is meg kíván felelni. Ezt hierarchia szintek bevezetésével oldották meg. A 20 byte-os ATM címek 13 byte-ja csak a hálózatok címzését szolgálja, vagyis 104 szint definiálható ilyen módon.

Egy PNNI hierarchia szint logikai állomásokból áll, amelyek logikai szakaszokkal vannak összekapcsolva. A legalsó szinten a fizikai kapcsolóknak és fizikai szakaszoknak lesznek a logikai kapcsolók és a szakaszok. Ezek úgynevezett PG (Peer Group) csoportokat alkot-

nak Azonos PG-ben lévő kapcsolók topológiai adatbázisa megegyezik, és a csoport topológiájáról minden információt tartalmaz.

A PG-k maguk is PG-kba szerveződnek, ezáltal alakítva ki egy újabb hierarchia szintet. A hierarchia egyel magasabb szintjén a csoportok logikai kapcsolóként jelennek meg. Fizikailag ez olyan módon valósul meg, hogy az egyes csoportok kapcsolói kiválasztanak (prioritás érték szerint megszavaznak) egy kitüntetett kapcsolót, amelyet *PGL-nek (Peer Group Leader)* nevezünk. A PGL feladata, hogy képviselje a csoportot a következő hierarchia szinten, és az összes általa kapott információt megossza a csoport kapcsolóival. Továbbá a PGL feladata, hogy a csoport topológiai adatbázisát összefogja (aggregálja) és ezt továbbítsa a vele egy hierarchia szinten lévő összes kapcsolónak.

Az aggregálást magában foglalja a címek összegzését valamint a topológia aggregációt is. A topológia összegzésekor az egyes csoportok közötti fizikai szakaszokat összevonjunk egyetlen virtuális szakasszá, illetve a csoportot egyetlen komplex csomópontként reprezentáljunk a hierarchia egyel magasabb szintjén. A hierarchia minden egyes szintjén a címek is aggregálásra kerülnek egyre rövidebb prefixekké, hasonlóan az IP címzéshez. Így az aggregáció révén csökkenteni tudjuk a jelzésrendszer forgalmát. A PNNI előnye még, hogy automatikusan konfigurálódik az ATM kapcsolók címzése alapján.

3. QoS és forgalomszabályozás

Az erőforrás igények kezelésének nehézségeit az ATM hálózatok (vagyis a PNNI) azzal oldja fel, hogy az elosztott adatbázisú útvonalválasztók helyett úgynevezett source routing mechanizmust használ. Ilyenkor a hívás a teljes útvonalát a forrás útvonalválasztó határozza meg. Minthogy az útvonalválasztónak a saját topológiai adatbázisa alapján kell megbecsülnie, hogy mely kapcsolókon keresztül épülhet fel a kapcsolat, szükség van egy általános CAC (*Call/Connection Admission Control*) függvényre, amivel a döntést végző kapcsoló modellezheti egy távoli kapcsoló viselkedését. A PNNI erre specifikált egy Generic CAC (GCAC) függvényt, amelynek segítségével a topológia gráfból a QoS igényeknek nem megfelelő útvonalakat kizárhatjuk. A fennmaradó útvonalakból kiválasztva a kapcsoló elkészíti a DLT-t (Designated Transit List), amely leírja, hogy a hívásfelépítésnek mely kapcsolókon kell keresztülhaladnia. Ezen az útvonalon minden kapcsoló az aktuális (Actual) CAC (ACAC) függvényével leellenőrzi, hogy a hívást valóban képes-e vállalni. A hálózat állapota ugyanis időközben megváltozhatott, illetve a PG-ok közötti összesítések miatt sokkal pontosabb adatok állhatnak az érintett kapcsolók rendelkezésre. A forrás útvonalválasztó tehát mindössze egy (a rendelkezésre álló információk alapján) optimális utat próbál „tippelni”. Ha az egyik kapcsoló visszautasítja a hívást, akkor egy jelzésüzenet visszafelé haladva felszabadítja a lefoglalt erőforrásokat egy kapcsolóig, ahonnan más irányban újra megpróbál eljutni a hívott félhez.

Ezt a PNNI specifikáció Cranckback néven említi.

A PNNI egy potenciálisan erős jelölt arra, hogy tartományközi optikai útvonalválasztó protokollok alapja legyen. A PNNI támogatja a QoS útvonalválasztást. Hátánya viszont, hogy rendkívül összetett protokoll és talán ennek következményeképpen az optikai kapcsoló iparban alacsony a részesedése a PNNI alapú optikai útvonalválasztó megoldásoknak. Ennek következményeképpen a már meglévő optikai kapcsolók és a PNNI alapú kapcsolók között az együttműködés problémás lehet.

4. Tanszékünkön fejlesztett hálózati modell bemutatása

A Budapesti Műszaki Egyetem Távközlési és Média-informatikai Tanszékén régóta folynak már kutatások, amelyek azt vizsgálják, hogyan lehet távközlő hálózatok megbízhatóságát növelni, vagyis hogy egy esetleges meghibásodás minél kisebb fennakadást okozzon az átvitelben. Az optikai hálózatok vizsgálata is eme kutatások keretében indult.

Az előző fejezetekben képet vázoltunk arról, hogy a világ a jelenleg elérhető és megvalósítható technológiák segítségével hogyan igyekezik megoldani nagy kiterjedésű optika hálózatokban a forgalomelvezetés feladatát. Az OSPF/BGP elv az IP hálózatok miatt a gyakorlatban széles körű elterjedtségének örvend, viszont nem fektet hangsúlyt az összeköttetések védelmére, különféle védelmi stratégiák kialakíthatóságára. A GMPLS lehetővé teszi ugyan, hogy az útvonal meghatározását teljes hosszában a forrás végezze el saját adatbázisa és számítása alapján, így kiegészíthető védelemmel, viszont ez egyelőre csak tartományon belül megoldott, azaz tartományok határain átvívelő összeköttetések védelme még nyitott probléma. A PNNI nagyon jól kezeli a hálózat skálázhatóságát, de a hálózati csomópontokban tárolt topológiaiinformáció ahhoz túlságosan vázlatos, hogy védelmi módszereket optimálisan alkalmazzunk benne.

Ezeket a megfontolásokat vettük figyelembe hálózati modellünk kialakításakor, melyben ötvözni próbáltuk a meglévő technikák előnyös tulajdonságait.

1. Információ aggregálása és terjesztése

Az útvonalválasztó algoritmusok nem közvetlen a hálózaton, hanem annak absztrakt, logikai képén keresnek egy pontpár között összeköttetést.

Az egyes tartományoknak kétféle logikai képeről beszélünk. Belső képről, amit a tartományon belül minden forrás ugyanolyannak ismer, és ami hűen tükrözi a fizikai sík tulajdonságait, valamint a tartományon kívülre terjesztett, külső képről, ez az, amilyenek a többi résztvevő az adott tartományt látja. Teljes belső hálózati képet tartományon kívülre, vagyis idegen tartománynak terjeszteni nem célszerű. Egyrészt azért, mert igen gyakran a kapcsolódó szomszédos hálózat egy konkurens szolgáltató tulajdona, aki elől üzleti szempontból jobb,

ha minél több információt rejtünk el, másrészt pedig teljes topológiai információ terjesztése hamar skálázhatósági problémához vezet. A külső képet tehát úgy célszerű megalkotni, hogy a belső hálózati képet olyannyira tömörítjük (aggregáljuk), hogy csak az útvonalválasztáshoz elengedhetetlenül szükséges információk legyenek benne.

Aggregált információ

Lássuk, mik legyenek ezek a szükséges információk! Elsősorban az elérhetőségről kell tudnunk, hogy az egyes távoli tartományokat milyen úton érhetjük el. A PNNI hierarchikus topológiájából is ilyen információt kaphatunk, és részleges megoldást (csak egyféle elérési útvonallal) kínál a BGP-4 is. Ezekkel összhangban az elérhetőséget mi is a két pont közti összekötő éllel (*aggregált éllel*) jelöljük. Mivel a forrásban az útvonalat hullámhossz szinten határozzuk meg, az elérhetőséget is hullámhosszonként kell megadnunk. Tehát egy aggregált él egy hálózati eszköz kimenő hullámhosszáról (esetleges hullámhossz konvertereken keresztül) egy másik eszköz bemeneti hullámhosszának elérhetőségére vonatkozik. Elérhetőségi paraméterként három dolgot adunk meg:

- költség, ami az optimalizáláshoz szükséges, és a kapcsolat kiépítésének anyagi költségét reprezentálja;
- kapacitás, ami a blokkolás elkerüléséhez nyújt gyakorlati segítséget;
- késleltetés, ami szolgáltatásminőség biztosítása esetén kerül előtérbe, ám egyelőre nem foglalkozunk ezzel a paraméterrel.

A tartomány képeit legegyszerűbben gráf-terminológiával élve írhatjuk le. A külső kép tulajdonképpen egy olyan gráf, mely aggregált információkat tartalmaz, így gyakran *aggregált gráfnak* is nevezzük. Ez tartalmazza a tartomány határán levő hálózati csomópontokat az egyes hullámhosszokon külön-külön egy-egy csúcsként jelölve. Ezeket a csúcsokat kötjük össze aggregált élek és az opcionálisan beszűrt kiegészítő, ún. *virtuális csúcsok* segítségével. Az összekötés módja tartományra van bízva, nincs rá általános szabály. Ha a tartomány nem kíván bonyolult számításokat végezni, nem vezet be virtuális csúcsokat, hanem az aggregált gráfban egyszerűen összeköti az egymásból elérhető csomópontokat, s a virtuális élek költségét legrövidebb út algoritmus alapján számítja ki, az így talált legrövidebb út késleltetését állítja be késleltetésnek, a kapacitást pedig *maximális folyam* algoritmussal nyeri.

Világos, hogy ez a megoldás igen hamar skálázhatósági korlátokba ütközik, mert n határmenti csomópont és l hullámhossz esetén $(n*(n-1)/2)*(l^2)$ aggregált él lesz a gráfban. Mivel napjaink hálózataiban n alacsony (1-6) szokott lenni, inkább a szorzat második tényezőjének, a hullámhossztól függő komponens lezoritását kell megcélozni. Ha a tartomány úgy dönt, hogy külső forgalomelvezetési kérések esetén nem engedélyez hullámhossz-konverziót, az aggregált élek maximális száma $1/l$ -ed részére csökken az eredetinek.

Szintén kedvező aggregált gráf alakítható ki abban az esetben, ha a hálózat mindegyik határmenti csomópontja képes hullámhossz-konverzióra. Ilyenkor a csomópontot jelölő l darab csúcs mellé elhelyezünk egy virtuális csúcsot, ezt összekötjük az eredeti l csúccsal (ahol az összekötő él paraméterei: konverziós költség, hullámhossznyi kapacitás, konverziós késleltetés), s a tartomány belsejében az elérhetőséget csak a virtuális csúcsok között vizsgáljuk. Így $(n*l) + (n*(n-1)/2)$ virtuális él fog az aggregált gráf maximálisan tartalmazni.

Kísérleteink azt mutatják, hogy a tartomány külső képének nem kell valós belső állapotokat tükröznie. Folytathat a tartomány óvatos politikát, magáról mérsékelt mennyiségű információt terjesztve, ám ezzel vállalja azt, hogy kevesebb igény fog rajta áthaladni, így az üzleti haszna is kisebb lesz a szolgáltatónak. Akár azt a stratégiát is választhatja a tartomány, hogy nem vesződik külső kép számításával, és egy nagyon egyszerű, statikus képet szolgáltat magáról. A kívülről érkező kéréseket vagy el tudja vezetni, vagy nem, viszont utóbbi esetben számolnia kell azzal, hogy intelligens útvonalválasztó algoritmusok az adott tartományt előbb-utóbb megbízhatatlannak fogják nyilvánítani. Mindazonáltal ez a terület még mélyebb vizsgálatokat igényel.

Információ terjesztése

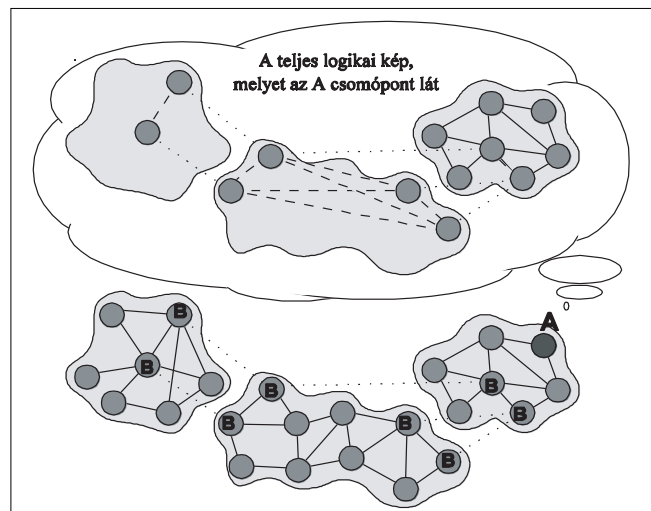
Több tartományból álló hálózatban nem várhatjuk el, hogy egy csomópont minden tőle távol történő eseményről értesüljön, még akkor sem, ha ez alapvetően befolyásolná útvonalkijelölési döntéseit. Minden csomópont a távoli tartományokban lejátszódó események hatásairól kétféleképp értesül:

- amikor forrásként egy másik tartományba irányított kapcsolatának kiépítése blokkolódik;
- amikor távoli tartományról külső képet kap.

Mi az utóbbival foglalkozunk részletesen.

Az aggregált gráfo(ka)t a tartomány valamilyen belső stratégia alapján megalkotja, és a határmenti csomópontok ezt rendszeres időközönként elküldik külső ügyfeleknek. Arra, hogy mekkora legyen a frissítési periódus, az utolsó fejezetben (5) végeztünk vizsgálatokat.

3. ábra Belső és külső logikai képek illesztése



Ha egy határmenti csomópont egy távoli tartományról új külső képet kap, akkor azt terjeszti mindenfelé, kivéve arra, amerről kapta, így a tartománybeli csomópontok ez alapján frissítik a teljes hálózati (belső és több külső) képüket.

A nem határmenti csomópontok pedig tartományon belül gondoskodnak arról, hogy egy külső kép minden csomóponthoz eljusson mihamarabb.

2. Forgalmkötegelés támogatása

A forgalmkötegelés [22] (grooming) lehetősége akkor kerül előtérbe, amikor több, egy hullámhossz kapacitásánál lényegesen kisebb sávzélességű igényt kell elvezetni. Sokat nyerhetünk, ha ezeket a kis igényeket – TDM technikával – egyetlen hullámhosszban tudjuk továbbítani. Viszont az igények kötegelésére nem minden csomópont képes, csak az olyan kapcsolók, amelyek az optikai mellett az elektromos rétegben is dolgoznak.

Tartományon belül természetesen a forrás számára ismert, hogy mely kapcsolók támogatják a forgalmkötegelést, melyek nem, viszont ezt az információt kifelé terjeszteni hiba lenne. Ehelyett megelégszünk azzal, ha grooming szempontjából egy tartományról csak anynyi információt közlünk, hogy mely határcsomópontok között van rá lehetőség.

A kötegelés jellemzője, hogy terhelt hálózat nagyban támogatja, mert ha két forgalmat egy hullámhosszba tud összefogni, akkor nyer egy hullámhossznyi szabad kapacitást. A támogatás abban jelentkezik, hogy a hálózat olcsóbban szállítja a kötegelt forgalmat. Ennek tükrében mi is a költség paraméternél fogtuk meg a groomingot.

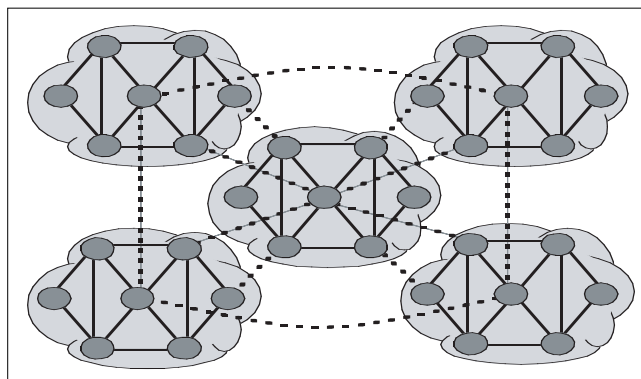
Minden tartomány, mely támogatja a forgalmkötegelést, készít egy hullámhossznál finomabb felbontású (*sub-lambda*) aggregált gráfot kifejezetten az egy hullámhossz kapacitásánál kisebb sávzélességű külső igények számára, melyben az építőelemek (csúcsok, élek) ugyanazok, mint előző alfejezetben bemutatottak, persze a virtuális él kapacitása itt valós és használt érték lesz.

5. Eredmények és értékelésük

Jelenleg, kezdeti fázisban azt vizsgáljuk, hogyan lehet a tartományközi útvonalválasztást és forgalomelvezetést megoldani. Tudjuk, hogy a külső képek periodikusan frissülnek, ezért az útvonalválasztást csak állott információ alapján végezhetjük el. De vajon mekkora mértékű állottságot engedhetünk meg, vagyis milyen időközönként frissítsük a külső képet? Erre kerestük első tesztünkben a választ.

A vizsgált hálózat

A vizsgált hálózat 5 tartományból, tartományonként 7 csomópontból áll, és mindegyik csomópont képes az elektromos rétegben is dolgozni. A topológiát a 4. ábra mutatja.



4. ábra A teszhálózat topológiája

Az egyes pontpárok közti forgalom mennyiségével kapcsolatban megkötöttük azt, hogy egy forrásból átlagosan háromszor akkora forgalom fog egy tartományon belüli célhoz tartani, mint tartományon kívülihez. Így, mivel minden forráshoz 6 tartományon belüli és 28 tartományon túli cél tartozik, összességében számottevő (69%) lesz a tartományközi forgalom aránya.

Látható, hogy minden tartománynak 3-5 határmenti csomópontja van, a külső képek konstruálására nem alkalmaztunk intelligens algoritmust, hanem megelégszünk a virtuális csúcsok nélküli, hullámhosszanként a minden csúcsból minden csúcsba közvetlen aggregált éllel való leírással.

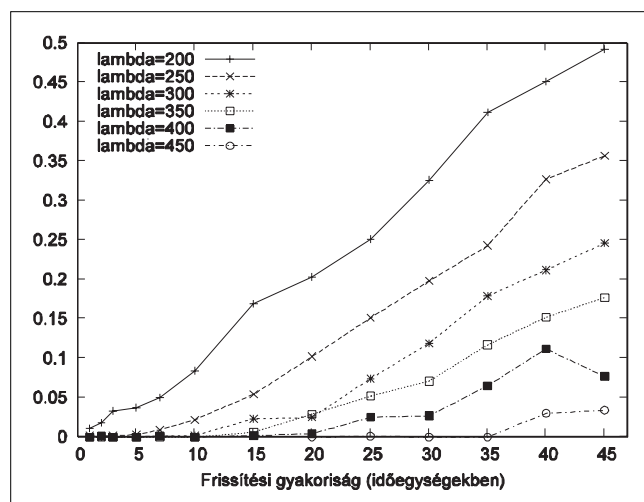
Szimuláció

Megvizsgáltuk, hogy bizonyos hálózati terheltség mellett mekkora információfrissítési késleltetésnél tapasztalhatunk jelentős blokkolási arányt.

Az igények hossza átlagosan 10 időegység. A lambda paraméter segítségével az igények érkezésének gyakoriságát befolyásoljuk. Azt kell látnunk, hogy alacsony forgalom mellett viszonylag hosszabb frissítési periódusokkal is élhetünk anélkül, hogy a rendszerben komolyabb mennyiségű igény kiépítése blokkolódna. Frissítési időköz és blokkolási arány között az összefüggés nagyjából lineáris.

5. ábra

Blokkolási arány az információ állottságának függvényében



Összefoglalás

A közeljövőben várható a többretegű, több tartományból álló hálózatok terjedése, noha az alkalmazandó útvonalválasztási megoldás még nyitott kérdés. Várhatóan, tekintettel az IP fontos szerepére és az IP forgalom mennyiségére részben IP specifikus lesz; a megoldatlan IP-problémák miatt várhatóan az ATM féle PNNI-ből is meríteni fog, azonban az optikai alsó rétegek miatt több optikai jellemzőt is figyelembe kell venni. Cikkünk egyik célja e problémakör bemutatása volt.

Másik célunk a saját fejlesztésű szimulációs rendszer működésének bemutatása volt, melyet az útvonalválasztási technikák fejlesztésére, kiértékelésére használunk. Példaként bemutattuk, hogy hogyan befolyásolja a blokkolási valószínűséget a terjesztett információ gyakorisága különböző hálózat terheltségek mellett. A kívánt gyakoriság beállítása egy kompromisszum az alacsony blokkolás és a túl gyakran árasztott információ szakasz és processzor kapacitásra gyakorolt terhelése között.

Irodalom

- [1] D. Awduche, A. Chiu, A. Elwalid, I. Widjaja, and X. Xiao, "Overview and Principles of Internet Traffic Engineering." IETF RFC 3272, 2002.
- [2] E. Rosen, A. Viswanathan, and R. Callon, "Multiprotocol Label Switching Architecture." IETF RFC 3031, 2001.
- [3] L. Berger, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling, Functional Description." IETF RFC 3471, 2003.
- [4] R. Braden, L. Z. S. Berson, S. Herzog, and S. Jamin, "Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification." IETF RFC 2205, 1997.
- [5] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels." IETF RFC 3209, 2001.
- [6] L. Berger, D. Gan, G. Swallow, P. Pan, F. Tommasi, and S. Molendini, "RSVP Refresh Overhead Reduction Extensions." IETF RFC 2961, 2001.
- [7] B. Jamoussi, "Constraint-based LSP Setup using LDP." IETF RFC 3212, 2002.
- [8] D. Awduche, J. Malcolm, J. Agogbua, M. O'Dell, and J. McManus, "Requirements for Traffic Engineering Over MPLS." IETF RFC 2702, 1999.
- [9] G. Bernstein, E. Mannie, and V. Sharma, "Framework for GMPLS-based Control of SDH/SONET Networks." draft-ietf-ccamp-sdhsonet-control-02.txt, 2003.
- [10] A. Banerjee, J. Drake, J. Lang, B. Turner, D. Awduche, L. Berger, K. Kompella, and Y. Rekhter, "Generalized multiprotocol label switching: An overview of signaling enhancements and recovery techniques," IEEE Communications Magazine, vol. 39, pp.144–151, July 2001.
- [11] L. Berger, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling, Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions." IETF RFC 3473, 2003.
- [12] P. Ashwood-Smith and L. Berger, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling, Constraint-based Routed Label Distribution Protocol (CR-LDP) Extensions." IETF RFC 3472, 2003.
- [13] J. Moy, "OSPF Version 2." IETF RFC 2178, 1998.
- [14] D. Katz, D. Yeung, and K. Kompella, "Traffic Engineering Extensions to OSPF Version 2" draft-katz-yeung-ospf-traffic-09.txt, 2003.
- [15] S. Jamadagni, "OSPF extensions for flexible CSPF algorithm support" draft-satish-ospf-cspf-support-00.txt, 2003.
- [16] L. Berger and Y. Rekhter, "Generalized MPLS Signaling – Implementation Survey." draft-ietf-ccamp-gmpls-signaling-survey-04.txt, 2003.
- [17] A. Banerjee, J. Drake, J. Lang, B. Turner, K. Kompella, and Y. Rekhter, "Generalized multiprotocol label switching: An overview of routing and management enhancements," IEEE Communications Magazine, vol. 39, pp.144–150, Jan 2001.
- [18] J. Lang, "Link Management Protocol (LMP)." draft-ietf-ccamp-lmp-10.txt, 2003.
- [19] X. Shao, T. H. Cheng, and K. Veerayah, "Requirements for MPLS over GMPLS-based Optical Networks (MPLS over GMPLS)." draft-xushao-ipo-mplsovergmpls-00.txt, 2003.
- [20] R. Coltun, "The OSPF opaque LSA Option" IETF RFC 2370, 1998.
- [21] M. Blanchet, F. Parent, B. St-Arnaud, "Optical BGP (OBGP): Inter-AS lightpath provisioning" draft-parent-obgp-01.txt, 2001.
- [22] T. Cinkler, "Traffic- and λ Grooming" IEEE Network, pp. 16-21, March/April 2003, Vol. 17, No.2.