Szegmensalapú védelmi megoldások GMPLS környezetben

GRICSER ÁDÁM, PÁNDI ZSOLT

BME, Híradástechnikai Tanszék

gricser@hit.bme.hu, pandi@hit.bme.hu

Reviewed

Kulcsszavak: WDM, GMPLS, hibatűrő hálózatok, szegmensalapú védelem

A fényvezetős hálózatok egységes menedzsment síkjaként javasolt Generalized Multi-Protocol Label Switching-et (GMPLS) leíró ajánlások egyre finomabb képet festenek az egyes vezérlési feladatok lebonyolításáról. Külön foglalkoznak a hibatűrő kapcsolatok felépítésének lehetőségeivel és támogatásával. Ezen a vonalon a többszörös hibákkal szemben is robusztus megoldások kérdéskörét felvető igények miatt a kutatók figyelme a közelmúltban a szegmensalapú védelmi módszerek felé fordult. A cikk e két terület lehetséges kapcsolódási pontjait kísérli meg vázlatosan tárgyalni kitérve néhány védelmi módszer működésére és bemutatva a GMPLS környezetben való alkalmazásuk néhány fontos kérdését.

1. Bevezetés

A távközlési szolgáltatások esetében már a kezdetektől fogva fontos szempont volt a szolgáltatás rendelkezésre állása. Így volt ez akár a telefonhálózatok, akár a nagy sávszélességű Internet kapcsolatot biztosító hálózatok esetében. A megbízhatóság különösen lényeges szempont létfontosságú összeköttetések esetén, valamint nagy kapacitású, sok igényt kiszolgáló hálózatokban, ahol egy hálózati elem meghibásodása kapcsolatok sokaságának megszakadását okozhatja. Ez utóbbi érv is jelzi, hogy a hullámhossz-multiplexált (WDM) hálózatok esetében is fontos kérdésről van szó.

A hálózatok hibatűrésének növelésére számos megoldást kidolgoztak már, amelyeket többféle szempont szerint is csoportosíthatunk. Ha azt vesszük figyelembe, hogy a hiba esetén szükségessé váló tartalék erőforrások aktiválásához szükséges lépések (útvonal-választás, jelzés, erőforrás választás és erőforrás hozzárendelés [1]) mekkora része kezdődik meg a hibaesemény bekövetkezése után, akkor egy olyan skálát állíthatunk fel, amely az összes lépést a kapcsolat felépítésével egyidőben végző védelemtől a csak a hiba bekövetkeztekor reagáló teljesen dinamikus helyreállításig terjed.

Amennyiben a tartalék erőforrásoknak a meghibásodott komponensek pótlására történő felhasználását tekintjük, a hibás komponens közvetlen környezetének közreműködését igénylő lokális védelemtől a kapcsolat helyreállítását a végpontok közreműködésével végző globális megoldásokig állíthatunk fel intuitív sorrendet.

Az utóbbi skálán nagyjából középen elhelyezhető, szegmensalapú védelmi megoldások kutatása a közelmúltban egyre nagyobb hangsúlyt kapott. Ezek a két végletnek tekinthető védelmi kategória közötti átmenetként foghatók fel az igényelt erőforrások száma, a helyreállításhoz szükséges idő, a védelem aktiválódása esetén bekövetkező csomagvesztés és a biztosított rendelkezésre állás szempontjából is. Ez utóbbi különösen fontos a többszörös meghibásodásokkal szemben robusztus megoldások iránti érdeklődés élénkülése miatt [2,3].

Napjainkra az optikai szálak hatalmas sávszélességét egyre jobban kihasználó adatátviteli eljárások fejlődése és a már használatban levő berendezések sokfélesége, különböző technológiai eredetű korlátozásai és vezérlési kötöttségei elengedhetetlenné tették egy egységes vezérlési sík, a korábban már sikerrel alkalmazott Multi-Protocol Label Switching (MPLS) általánosítását jelentő GMPLS kidolgozását [4,5]. Az eddig megjelent ajánlások igyekeznek a működés feltételeit érintő átfogó kérdéseket megválaszolni, de számos konkrét részlet még tisztázásra vár. Ezek közé tartozik a szegmensalapú védelmi megoldások alkalmazása is [6]. Az üzemeltetés miként jének kidolgozásával párhuzamosan hatékonysági szempontokat is figyelembe kell venni, amelyek indokolttá tehetik a különböző szegmensalapú védelmi megoldások előnyben vagy hátrányban részesítését egyéb megoldásokkal szemben.

A cikk egyrészt néhány alapvető szegmensalapú védelmi módszert, másrészt pedig ezek GMPLS alapú hálózatokban történő alkalmazásának fontosabb kérdéseit tekinti át.

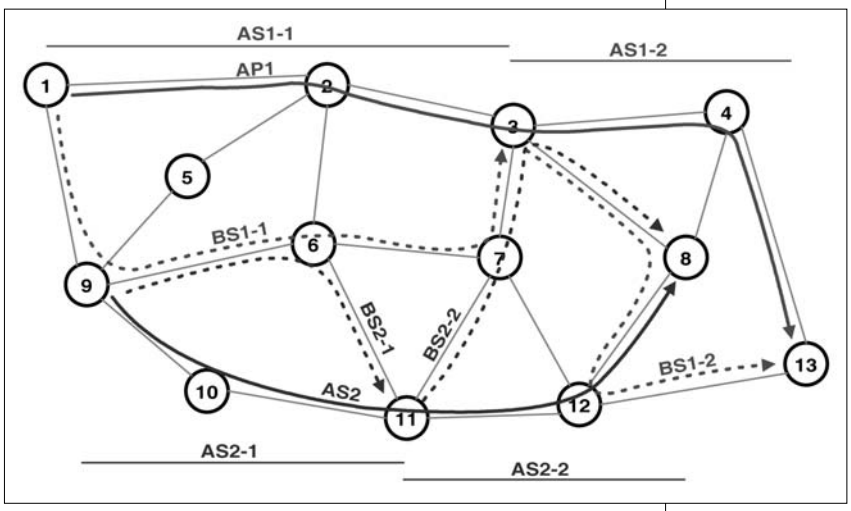
2. Szegmensalapú védelmi módszerek

Az alábbiakban az egyes védelmi módszerek eredeti, irodalomban fellelhető változatait mutatjuk be. A módszereknek az említett védelem-helyreállítás skálán történő elhelyezését és a skála mentén történő lehetséges eltolásának végiggondolását az olvasóra bízzuk.

2.1. Rész-út védelem (Sub-path protection)

A külön védendő szegmensek létrehozásának legkézenfekvőbb megvalósítása az üzemi útvonal partícionálása. Mivel az útvonal részek nem fedik át egymást, a tartalék szegmensek (Backup Segment, BS) a

védett üzemi szegmensek (Active Segment, AS) határainál illeszkednek az aktív útvonalra (Active Path, AP), ahogy az *1. ábrán* látható. Az útvonal tetszőlegesen felbontható, de figyelembe lehet venni bizonyos korlátokat is, például a szegmensek számára vagy a védelmi szegmensek hosszára [7]. Természetesen – hacsak valamilyen egyéb okból nem tiltott – az azonos üzemi útvonalat védő tartalék szegmensek osztozkodhatnak közös erőforrásokon, ahogy az ábra is mutatja.



1. ábra Sub-path protection

A rész-út védelemnek egy speciális esete a terület szerinti szegmens védelem, melynek angol elnevezése szintén *sub-path protection* [8]. Eszerint a nagy kiterjedésű hálózat kisebb területekre van felosztva. Az igények elvezetésekor egyszerre kell az üzemi és a tartalék útvonalat meghatározni. Követelmény, hogy mindkettő ugyanazokon a csomópontokon keresztül lépjen át egyik területről a másikra, illetve mindkettő maradjon az adott területen belül, ha belső kapcsolatot kell létrehozni. Több zónán áthaladó védett kapcsolat elvezetésére mutat példát a *2. ábra*. A védelem felbontása a zónahatárokhoz igazodva történik, így hiba esetén a kapcsolatnak csak az adott területen futó részét kell átkapcsolni a megfelelő tartalék szegmensre.

2. ábra A sub-path protection egy lehetséges változata

2.2. Védelem több szegmenssel: PROMISE (Protection using multiple segments)

A PROMISE az osztott szegmens védelem egy speciális változata [9]. Az üzemi útvonal (AP) szegmenseit (AS) itt is külön tartalék elvezetések (BS) védik. A javasolt sémában az aktív szegmens halmaznak a következő két feltételt kell teljesítenie:

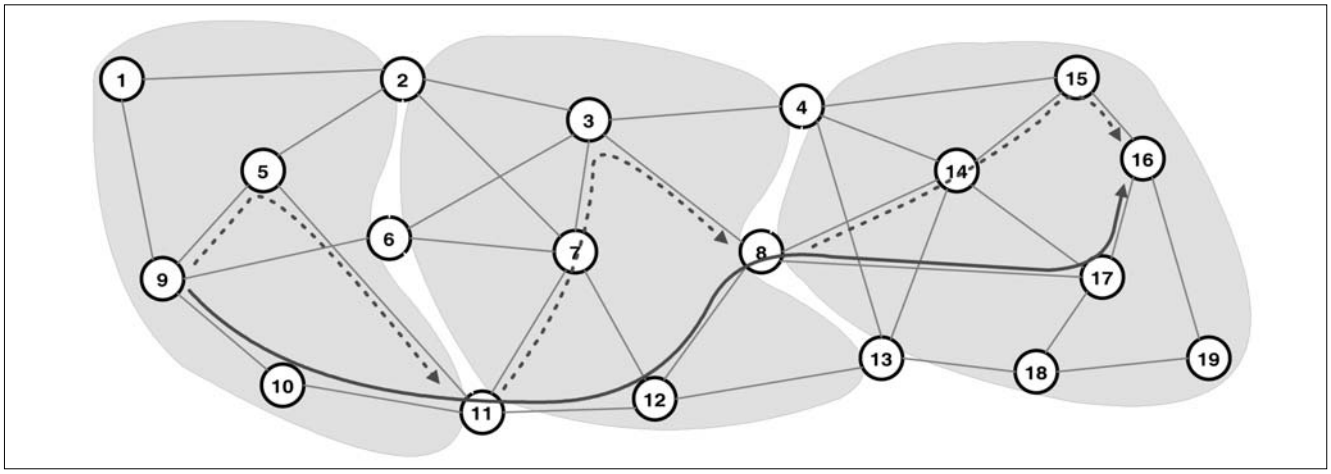
1. Az üzemi útvonal minden linkjét legalább egy szegmensnek tartalmaznia kell, de maximum kettőnek lehet a része.
2. Egy szegmens nem lehet valódi részhalmaza egy másik szegmensnek.

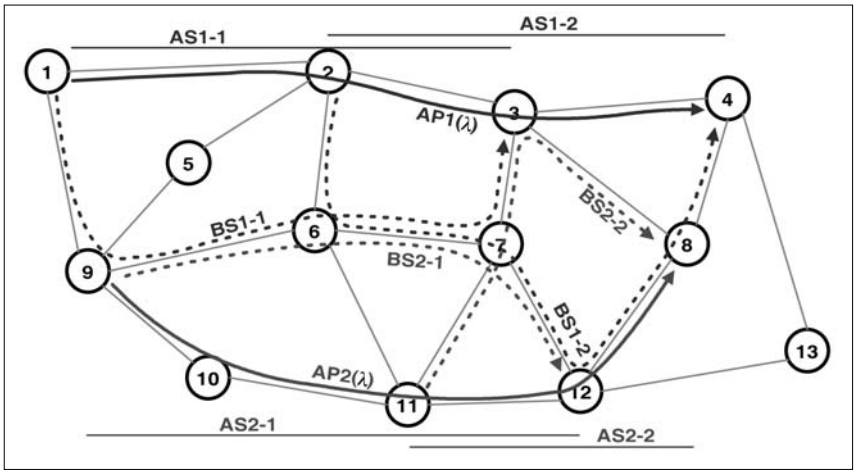
A feltételekből adódik, hogy létrejöhetnek egymást részben átfedő szegmensek, mint ahogy azt a következő oldali *3. ábrán* is látható. Azokat a linkeket, melyek két üzemi szegmenshez tartoznak, definíció szerint a kapcsolat irányához viszonyítva második szegmens tartalék útvonala védi.

A PROMISE a tartalék erőforrások megosztásának két módját is alkalmazza. Az erőforrásokon osztozkodhatnak különböző kapcsolatokhoz tartozó védelmi útvonalak *(intersharing)*, azonban a tartalékok megosztása lehetséges az azonos üzemi útvonalat védő tartalék elvezetések között is *(intrasharing)*. Előbbire példa a 3. ábrán BS1-1 és BS2-1 tartalék útvonalak viszonya, melyek a (9,6), (6,7) szakaszokon osztozhatnak közös erőforrásokon, az utóbbira pedig a BS1-1 és BS1-2 védelmi szegmensek, melyek a (6,7) link egyik hullámhossz csatornáját oszthatják meg.

A PROMISE rugalmassága folytán bizonyos esetekben képes akkor is elvezetni a védett igényt a hálózatban, amikor sem az útvonal-, sem a link védelem nem képes erre [9].

Megjegyezzük továbbá, hogy a PROMISE-hoz teljesítményében és működésében hasonló, másik módszert mutat be [10], amelyet a szerzők osztott szegmens védelemnek (segment shared protection, SSP) neveznek.





3. ábra A PROMISE módszer működése

2.3. A védelmi kör alapú szegmens védelem

A védelmi kör (p-Cycle, pre-configured Cycle) koncepciót Grover és Stamatelakis javasolta [11,12]. A megoldás a szövevény hálózat tartalék kapacitásainak védelmi körökbe szervezésére és előkonfigurálásukra épül: az optikai kapcsolókban már az erőforrások lefoglalásakor létrejönnek a megfelelő tartalék elvezetések, így hiba esetén a gyűrű alapú védelmeket jellemző gyorsasággal épül fel a hálózat.

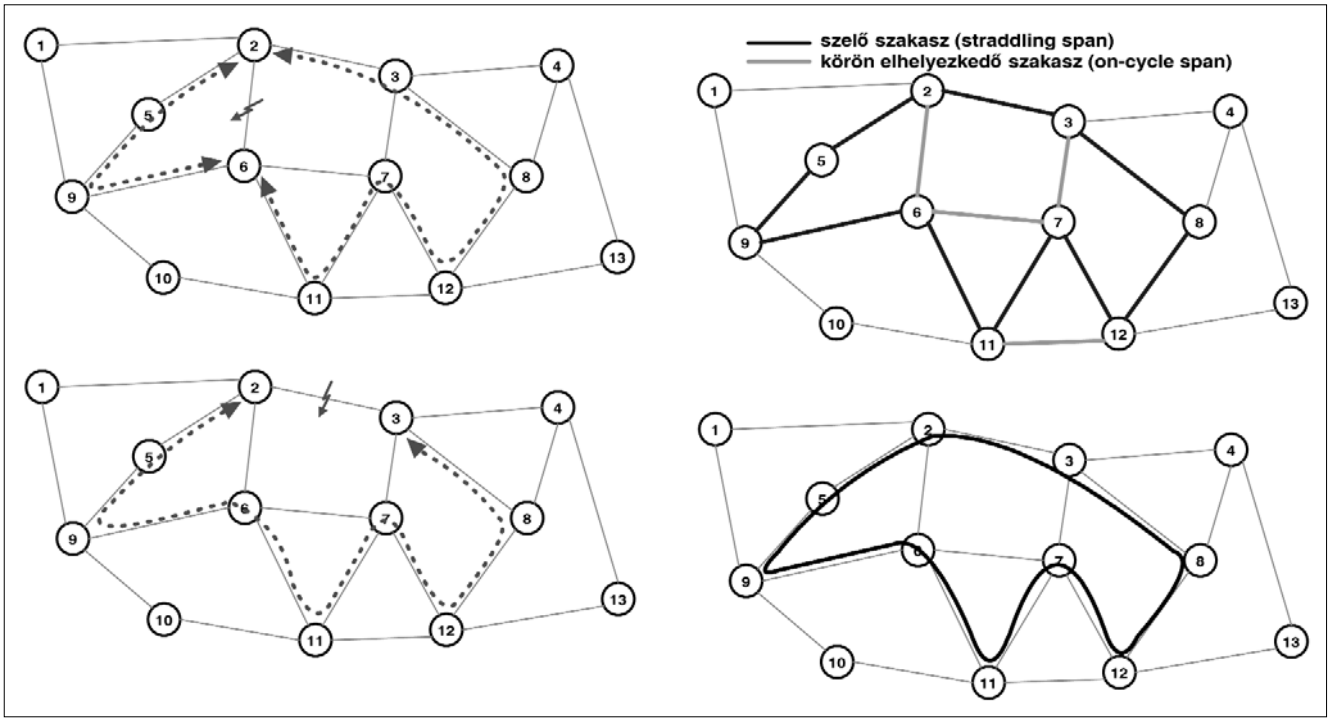
A *4/a.* ábrán egy lehetséges védelmi kör látható, a példában létrehozott védelmi kör által védett szakaszokat pedig a *4/b.* ábra mutatja, típus szerint elkülönítve. A így rendezett tartalék erőforrások a kör minden linkjének meghibásodása ellen képesek védelmet biztosítani a hibás szakaszon áthaladó kapcsolatoknak.

Az összeköttetések elvezetése a gyűrű alapú védelmekhez hasonlóan a kör érintetlen ívén lehetséges, ahogyan az a *4/c.* ábrán látható. A gyűrű alapú védelmekkel ellentétben a védelmi kör séma olyan linkek hibája ellen is véd, melyek nem részei védelmi körnek, de a végpontjai azon helyezkednek el, ezek az úgynevezett szelő *(straddling)* szakaszok. A *4/d.* ábrán a (2,6) szakasz meghibásodásakor a védelmi kör két tartalék útvonalat is biztosít a megszakadt kapcsolatok átirányítására.

A kör ívén bekövetkező hibák (kerületi hiba, on-cycle failure) esetén egy egységnyi tartalék kapacitás egy egység üzemi kapacitást véd, hiszen ekkor csak egy lehetséges tartalék útvonal van. A szelő szakaszok meghibásodásakor (straddling failure) azonban a védelmi kör egy egységnyi kapacitása két egységnyi üzemi kapacitást véd, hiszen két tartalék útvonal is használható a megszakadt kapcsolatok elvezetésére. Mindkét hibatípus esetén azonban csak a hibás szakasz végpontjainál történik átkapcsolás, aminek következtében a felépülési idő a gyűrű alapú védelmekéhez hasonló [11].

Az bemutatott alapelv linkhibák elleni védelemre lett eredetileg kidolgozva, azaz a fenti leírásban a „szakasz" jelentése ekkor link. Azonban a védendő kapcsolatok folyamalapú szemléletének bevezetésével, tulajdonképpen a „szakaszt" szegmensként értelmezve kiterjeszthető a megoldás szegmensalapú védelemmé is [13].

4. ábra p-Cycle alapfogalmak:
(a) egy lehetséges védelmi kör, (b) a kör által védhető szakaszok fajtái,
(c) a körön levő szakasz hibája elleni védelem, (d) szelő szakasz hibája elleni védelem



A gyűrű topológiájú védelmekkel szemben a védelmi kör séma másik nagy előnye a hatékony erőforrás kihasználás [14]. Amíg az előbbinél az üzemi útvonalakat is a fizikai gyűrűknek megfelelően kell kialakítani, addig az utóbbi esetében a védelmi körök a hálózat kihasználatlan (tartalék) kapacitásaiból szerveződnek, így az üzemi kapcsolatok a legrövidebb vagy más előnyös útvonalon is elvezethetőek.

3. Védelmi módszerek értékelésének szempontjai

A védelmi módszerek bemutatása után először néhány olyan szempontot vizsgálunk meg, amelyek általános alapgondolatokra épülnek, majd fokozatosan eljutunk a GMPLS-környezetből eredő specifikus kérdésekig.

3.1. Hibatűrés

A módszerek tervezésekor a szerzők döntő többsége azzal a feltételezéssel él, hogy a hálózatban egyidőben legfeljebb egy komponens lehet hibás állapotban, azaz gyakorlatilag elhanyagolhatónak tekintik az egyidejű többszörös hibák valószínűségét. Hasonlóképpen gyakran eltekintenek a csomóponti hibáktól, ami szintén racionális megfontolás, tekintettel a nagy megbízhatóságú berendezésekre. Ezek a feltételezések bizonyos esetekben helytállóak lehetnek, bizonyos esetekben pedig nem azok a hálózat méretétől, az alkalmazott technológiától és a teljesítendő megbízhatósági követelményektől függően [15].

A fent ismertetett módszerek közül a PROMISE és az SSP garantál csak védettséget az üzemi útvonal bármely egyszeres csomóponti vagy linkhibája ellen, a másik két módszer a csomóponti hibák elleni védelmet nem garantálja. Ez utóbbiak működését tekintve azonban látható, hogy ennek ellenére is bizonyos fokú védelmet nyújtanak a csomóponti hibák ellen pusztán a tartalék erőforrások szervezésének módjából eredően.

A többszörös hibákat vizsgálva elmondható általában, hogy minél több „önálló” részre, ha úgy tetszik védelmi domain-re bontjuk a kapcsolat védelmét, a lehetséges többszörös hibák annál nagyobb hányadával szemben lesz ellenálló a kapcsolat, bár hozzá kell tenni, hogy a több részből felépülő védelem több erőforrás felhasználását is jelenti, ami végső soron a kapcsolatot érintő (de nem feltétlenül megszakító) hibák valószínűségét is növeli.

Hasonlóképpen fontos megemlíteni a védelmi erőforrások megosztását, amely szintén befolyásolja a hibatűrést. A védelmi erőforrásokon való osztozás általában alkalmazott feltétele ugyanis csak az egyszeres hibák esetében fellépő versenyhelyzeteket zárja ki, így egy többszörös hibaállapotban előfordulhat, hogy egyszerre két kapcsolatnak is szüksége van a közös védelmi erőforrásra, amely végül az egyik kapcsolat megszakadásához vezet. A szerzőknek nincs tudomása olyan szakaszalapú védelmi módszerről, amely ezeket a hatásokat is figyelembe véve képes valószínűségi alapon garantálni a kapcsolat rendelkezésre állását, bár az útvonalvédelem esetére [16]-ban kidolgozott technika a szegmensalapú védelmek esetére is adaptálható.

3.2. Helyreállítási sebesség

A hálózat valamely elemének meghibásodásakor összeköttetések szakadhatnak meg, így valós idejű kapcsolatok esetében információ veszik el. Minél több időt vesz igénybe a kapcsolat helyreállítása, annál több adat veszik el, így a védelmi séma értékelésénél fontos tényező a hiba bekövetkezése és a forgalom újraindulása között eltelt idő.

Ennek az időnek a fontosabb komponensei a következők [1]. A meghibásodást, amely lehet linkszakadás, vagy akár a bithiba-arány megadott küszöbérték fölé történő növekedése, detektálni kell, amely természetesen valamennyi időbe telik. Megválasztható az úgynevezett korrelációs idő, amelyet azért célszerű várakozásként közbeiktatni, hogy az ugyanahhoz a hibaeseményhez kapcsolódó esetleges további hibadetekciók aggregálva (egy nagyobb logikai entitás meghibásodását jelezve) továbbítódjanak a vezérlési síkra, ezáltal potenciálisan csökkentve a hibakezeléshez szükséges vezérlési overhead-et. A felsőbb rétegek gyakran alkalmaznak úgynevezett hold-off várakozási időket, azaz a hibaesemény észleléséhez képest egy meghatározott ideig még nem kezdik meg a helyreállítást , hogy lehetőséget adjanak az alsóbb rétegeknek a saját védelmi eljárásaik működtetésére. Ez skálázhatósági szempontokból lehet lényeges. Az utolsó komponens a védelem aktiválási ideje, amelyet a bevezetőben említett további négy részre lehet bontani.

A detekciós idő technológiai adottság, amelynek fizikai korlátai vannak. A korrelációs és a hold-off időtartamok hatékony megválasztása lényeges hatékonysági kérdés az üzemeltető számára a vállalható garanciák és a kézbentarthatóság miatt, de alapvetően nem függ az alkalmazott védelmi módszertől. Az aktiválás idejét többféleképpen is lehet csökkenteni. Egyrészt az aktiváláshoz szükséges lépések minél nagyobb részét előre elvégezve, másrészt ha ez nem lehetséges, akkor kis számítási igényű védelmi módszereket alkalmazva, harmadrészt pedig a jelzési forgalmat minél inkább a hiba környezetében levő elemekre korlátozva. Ez utóbbi jelzi a szegmensalapú védelmek egyik előnyös tulajdonságát az útvonal alapúakkal szemben, míg az első szempont a védelem-helyreállítás skálán való eltolással elérhető gyorsulásra utal.

3.3. Erőforrás felhasználás

Természetesen fontos szempont az, hogy az adott módszer mekkora erőforrástöbbletet rendel hozzá a kapcsolathoz a hibák elleni védelem érdekében. Az erőforrások felhasználásának hatékonysága javítható a védelmi erőforrások megosztását lehetővé tevő módszerek alkalmazásával, valamint a védelmi erőforrások kihasználatlansága idejére azokra alacsony prioritású, azaz szükség esetén megszakítható extra forgalom beengedésével. A GMPLS mindkét lehetőséget támogatja [4].

A szegmensalapú módszerek a hatékony erőforrás-kezelés tekintetében az útvonalvédelmeknél gyengébben teljesítenek, de ez felfogható a nagyobb hibatűrésért cserébe fizetendő árként is. Az egyes módszerek által elhasznált címkék száma arányos a kapcsolathoz rendelt védelmi utak számával, ami értelemszerűen szintén nagyobb a szegmensalapú módszerek esetében, mint az útvonalvédelmeknél.

3.4. Skálázhatóság

A felépülési sebesség elemzésénél is esett már szó skálázhatósági szempontokról. Ide tartozik azonban még számos egyéb kérdés. A menedzselhetőség érdekében célszerű a hálózat állapotára vonatkozó bizonyos információkat (például egyes linkjellemzőket vagy egyéb, traffic engineering vonatkozású vezérlési információkat) aggregáltan kezelni. Ez azonban szükségképpen a hálózatról alkotott kép pontatlanabbá válásával is jár, ezért a védelmi sémák garanciáinak tarthatósága érdekében vizsgálni kell a hálózati információveszteség megengedhető mértékét is [1].

A hálózat menedzselhetőségi szempontokból történő vertikális partícionálása is a skálázhatóság kérdésköréhez tartozik. Ez az alapgondolat megjelenik a terület szerinti szegmens védelemben, de a p-Cycle koncepció is kiválóan alkalmas ilyen jellegű működtetésre. Tovább árnyalja a képet a GMPLS címkehierarchiáját esetlegesen kihasználó védelmi megoldások lehetősége, amelyre subnetwork protection-ként is hivatkoznak. Ez a megközelítés lehetővé teszi, hogy az egyes hálózati domainekben az áthaladó kapcsolatok védelméhez csak a domainekhez tartozó csomópontok közreműködése legyen szükséges. A módszer hátránya, hogy az egyes domainek határán levő csomópontok védelmét nem oldja meg, ugyanakkor racionális az a feltételezés, amely szerint ezek valószínűleg a hálózat legmegbízhatóbb csomópontjai közül valók, így vélhetően nem csökkentik jelentős mértékben a kapcsolat rendelkezésre állását.

3.5. Alkalmazás GMPLS környezetben

A GMPLS általánosítja az csomag- valamint cellakapcsolt működésű hálózatokban alkalmazható MPLS alapelvét az adattovábbítást második rétegbeli keret vagy cella fejléce időrés, hullámhossz és térbeli hely (például üvegszál-kapcsolást végző optikai kapcsolóelem) alapján végző hálózati technológiákra. Az egymásba ágyazott LSP-khez hasonlóan a többféle képességekkel rendelkező elemekből felépülő rendszereket továbbítási hierarchiaként is felfoghatjuk: a hierarchia tetején a térkapcsolást végző (Fiber Switch Capable, FSC) eszköz interfészek találhatók, majd a hullámhosszkapcsolást végzők (Lambda Switch Capable, LSC) és az időosztásos multiplexelésre képes (Time-Division Multiplex Capable, TDM) berendezés interfészek következnek, ezután a második rétegbeli kapcsolást végzők (Layer-2 Switch Capable, L2SC) végül pedig a csomagkapcsolt (Packet-Switch Capable, PSC) működésűek [4].

A GMPLS megköveteli, hogy minden LSP hasonló képességekkel rendelkező interfészeken kezdődjön és végződjön, amit a védelmi módszerek alkalmazásánál is figyelembe kell venni.

A különböző képességű rendszerekben a rendelkezésre álló címkekészlet mérete jelentősen eltérő lehet. Egyrészt az egyes üvegszálakon párhuzamosan futó, ezért a GMPLS-ben alapértelmezés szerint külön linkként megjelenő hullámhosszak száma nagyon nagy lehet, amelyek összefogására a GMPLS bevezeti a link bundling fogalmát. Ezzel kapcsolatban azonban a korábban már említett megengedhető információveszteség vizsgálatának kérdése merül fel [1]. Másrészt a TDM, LSC és FSC interfészeken rendelkezésre álló címkekészlet jelentősen kisebb lehet, mert az itt alkalmazható címkék fizikai tartalommal bírnak, ellentétben a más interfészeken alkalmazott logikai címkékkel szemben. Ez az alkalmazni kívánt módszer címkeigénye szempontjából fontos.

A használható címketartományra is elképzelhetők korlátozások. A gyakorlatban a forrás felőli csomópont a soron következő csomópontnak javasolhat használatra egy bizonyos címkét, amelyet az nem köteles elfogadni, ám ez esetben számolnia kell azzal, hogy a címke megváltoztatása a szükséges konfigurációs lépések elvégzése miatt nagyobb időveszteséggel jár. Ez különösen olyan optikai kapcsolóelemek esetében lehet lényeges, ahol a címkeváltás akár mikrotükrök mozgatását is jelentheti, amely a jelterjedési időkhöz képest jelentős időtöbblet. Ennek ugyancsak jelentősége lehet a védelmi módszerek szempontjából a különböző minőségi garanciák vállalásánál.

A GMPLS a skálázhatóság érdekében bevezeti a *forwarding adjacency* fogalmát is, amely kiaknázza a címkehierarchiában rejlő lehetőségeket. A megoldás lényege röviden, hogy több LSP-t aggregálnak egyetlen LSP-be, és az útvonal közbülső csomópontjainak elegendő csupán ezt a külső LSP-t látniuk, a belsőkhöz kapcsolódóan így nem kell továbbítási bejegyzéseket fenntartaniuk. Ez lényegében a skálázhatóságnál említett vertikális partícionálást is támogatja, ami rögtön nyilvánvalóvá válik, ha megemlítjük, hogy például elegendő a külső LSP-t védeni, a belsők egyenként történő megvédése helyett. Magától értetődően fontos, hogy ezt a működést összhangban tartsuk az alkalmazott védelmi módszer használatával.

Ugyanakkor a GMPLS az MPLS-sel ellentétben megengedi a kétirányú kapcsolatok kezelését is, amely a jelzésforgalom csökkentése mellett jelentősen egyszerűsítheti és hatékonyabbá teheti a védelmi módszerek alkalmazását is.

A hálózat állapotának a csomópontokhoz való eljuttatására és traffic engineering jellegű információk továbbítására a GMPLS is a már eddigiekben alkalmazott routing protokollokat (OSPF, IS-IS), pontosabban azok megfelelő kiterjesztéseit használja. [17] bemutat egy lehetséges csomóponti funkcionális blokkvázlatot, amelyből kiderül, hogy egy esetleges védelmi módszernek az ezek segítségével felépített és karbantartott

link állapot adatbázis alapján kell a GMPLS vezérlést végző entitás kezdeményezésére meghatároznia a megfelelő elvezetéseket.

Ennek mikéntjére vonatkozóan éppen a védelmi/helyreállítási módszerek széles körének alkalmazhatósága miatt a GMPLS ajánlások nem tartalmaznak megkötéseket. Mindazonáltal a különböző gyártótól származó berendezések együttműködésének természetes igénye szükségszerűvé teszi, hogy az alkalmazott védelmi módszer részletkérdéseitől függetlenül az üzemivédelmi erőforrásválasztáshoz szükséges információcsere standard módon történjen. Ebben az irányban azonban az ajánlások még nem érték el a végleges állapotot, de a folyamatos munkának köszönhetően a közeljövőben további kérdések tisztázása várható.

5. Összegzés

A cikk két fontos területet kísérelt meg vázlatosan bemutatni: a hibatűrő hálózati kapcsolatok szegmensalapú védelmi módszerekkel történő biztosítását, valamint az ennek egyik lehetséges alkalmazási területeként felmerülő GMPLS hálózati környezet ehhez kapcsolódó vonatkozásait.

Látható, hogy egyrészt a GMPLS ajánlások jelenlegi készültségi állapota és a még kidolgozás alatt álló, hozzájuk kapcsolódó javaslatok nagy száma miatt egyelőre vannak nyitott kérdések, amelyek megválaszolása elengedhetetlen ahhoz, hogy ténylegesen működtetni lehessen szegmensalapú védelmi módszereket GMPLS környezetben. A módszerek teljesítőképességére vonatkozó kutatási eredmények körültekintő alkalmazással párosulva azonban egy sok szempontból előnyös technológiai megoldást ígérnek.

Irodalom

[1] D. Griffith, R. Rouil, S. Klink, K. Sriram, An Analysis of Path Recovery Schemes in GMPLS Networks with Various Levels of Pre-Provisioning, SPIE OptiComm 2003

[2] D. A. Schupke, R. G. Prinz, Capacity Efficiency and Restorability of Path Protection and Rerouting in WDM Networks Subject to Dual Failures, Photonic Network Communications, Vol. 8, Issue 2., pp.191–207., 2004. szeptember

[3] J. Doucette, M. Clouqueur, W. D. Grover, On the Availability and Capacity Requirements of Shared Backup Path-Protected Mesh Networks, Optical Networks Magazine, Vol. 4, Nr.6., pp.29–44, 2003 november

[4] E. Mannie (Ed.), Generalized Multi-Protocol Label Switching (GMPLS) Architecture, RFC3945, 2004. október

[5] L. Berger, Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description, RFC3471, 2003. január

[6] L. Berger et al., GMPLS Based Segment Recovery, draft-ietf-ccamp-gmpls-segment-recovery-01.txt, 2004. október

[7] V. Anand, S. Chauhan, C. Qiao, Sub-path Protection: A New Framework for Optocal Layer Survivability and its Quantitative Evaluation, Department of Computer Science and Engineering State University of New York at Buffalo, Technical Report, 2002. január

[8] C. Ou, H. Zang, B. Mukherjee, Sub-Path Protection for Scalability and Fast Recovery in WDM Mesh Networks, Optical Fiber Communications Conference (OFC) Technical Digest, 2002, pp.495–496.

[9] Dahai Xu, Yizhi Xiong, Chumning Qiao, Novel Algorithms for Shared Segment Protection, IEEE Journal on Selected Areas in Communications, Vol. 21, Nr.8, pp.1320–1331., 2003. október

[10] P.-H. Ho, J. Tapolcai, T. Cinkler, Segment Shared Protection in Mesh Communications Networks With Bandwidth Guaranteed Tunnels, IEEE/ACM Transactions on Networking, Vol. 12, Nr.6, pp.1105–1118., 2004. december

[11] W. D. Grover, D. Stamatelakis, Cycle-Oriented Distributed Preconfiguration: Ring-like Speed with Mesh-like Capacity for Self-planning Network Restoration, IEEE Intern. Conf. on Communications (ICC) 1998

[12] W. D. Grover, D. Stamatelakis, Bridging the ring-mesh dichotomy with p-cycles, Design of Reliable Communications Networks Conference (DRCN) 2000

[13] G. Shen, W. D. Grover, Extending the p-Cycle Concept to Path Segment Protection for Span and Node Failure Recovery, IEEE Journal on Selected Areas in Communications, Vol. 21, Nr.8, pp.1306–1319., 2003. október

[14] D. A. Schupke, C. G. Gruber, A. Autenrieth, Optimal Configuration of p-Cycles in WDM networks, IEEE Intern. Conf. on Communications (ICC) 2002

[15] Zs. Pándi, A. Fumagalli, M. Tacca, L. Wosinska, Impact of OXC Failures on Network Reliability, SPIE Photonics Europe Conference 2004

[16] Zs. Pándi, M. Tacca, A. Fumagalli, A Threshold Based On-line RWA Algorithm with End-to-End Reliability Guarantees, Optical Network Design and Modelling (ONDM) 2005 Conference

[17] H. Liu, D. Pendarakis, N. Komaee, D. Saha, GMPLS-Based Control Plane for Optical Networks: Early Implementation Experience, SPIE ITCom 2002 Conference