# Hozzárendelt védelmi algoritmusok tervezése optikai hálózatokban

Babarczi Péter

2011. augusztus 1.

# 1. Bevezetés

Megbízható kommunikációs hálózatok tervezése és üzemeltetése a gyorsan változó technológiák miatt egyre nagyobb kihívást jelent a szolgáltatóknak. A nagy felbontású videóműsorok szétosztása miatt rohamosan megugrott sávszélességigény és az átviteli technológia folyamatos változása miatt (pl. hullámhosszosztásos nyalábolás, hullámhossz konverzió megjelenése, dinamikus, többrétegű hálózatok megjelenése) újabb és újabb tervezési eljárások szükségesek. A gerinchálózatokban jelenleg alkalmazott, vagy hamarosan bevezetésre kerülő technológiai megoldások már lehetővé teszik a teljesen optika alapú átviteli utak alkalmazását, kiküszöbölve ezzel a jelek költséges és időigényes optikai-elektromos-optikai (O/E/O) átalakítást.

A hálózattal szemben támasztott legfontosabb követelmények a technológiákkal ellentétben állandónak tekinthetőek. Ezen elvárások az alacsony létesítési (CAPEX) és üzemeltetési költség (OPEX), a forgalmi teljesítőképesség és az egyes szolgáltatások szolgáltatásminősége (QoS). A teljesen optikai alapú átvitel segítségével maximálisan megvalósítható adatsebesség elérte a terabájtos nagyságrendet másodpercenként [24] [8], melynek következtében a szolgáltatás folytonosságában bekövetkező legkisebb kiesés is hatalmas mennyiségű adat elvesztését eredményezi, így a hálózat által biztosított QoS csökken. A bevétel növelése érdekében a szolgáltatók érdeke minél megbízhatóbb hálózatokat tervezni [14], illetve az összeköttetések folytonosságát biztosítani, hiszen egy megbízható szolgáltatásért a felhasználók nagyobb összeget is hajlandóak fizetni. Megbízható hálózatok alkalmasak olyan kritikus valós idejű alkalmazások adatának továbbítására, mint például távoli műtétek végzése, vagy a hálózatban játszható valós idejű játékok, melyek lényegesen magasabb QoS követelményekkel rendelkeznek a hagyományos webes forgalmakhoz képest.

Az egyes alkalmazások lényegesen eltérő QoS követelményei miatt gazdaságtalan valamennyi összeköttetést azonos, magas QoS követelményeknek megfelelően kiépíteni. A hálózati infrastruktúra által biztosított magas rendelkezésre állásra építve a felhasználó igényeihez leginkább illeszkedő szolgáltatás nyújtása a cél. Az összeköttetés minél gazdaságosabb megtervezése érdekében a szolgáltató és a felhasználó a szolgáltatás megkezdése előtt szolgáltatásminőségi szerződést (SLA) kötnek, melyben a szolgáltató kötelezettséget vállal a felhasználó felé arra, hogy egy meghatározott összegért cserébe milyen minimális QoS követelmények mellett továbbítja az adatát

a hálózatában. Ha az SLA-ban vállalt feltételeket a szolgáltató nem teljesíti, súlyos összegeket kell fizetnie a felhasználónak. Ezért komoly üzleti érdek, hogy a szolgáltató az ilyen eseteket elkerülje, melynek fontos lépése a hálózat QoS szempontból történő pontos modellezése, valamint a hálózatban alkalmazott hibamenedzsment technológiák megfelelő kiválasztása.

Az összeköttetések QoS követelményeinek biztosítására alkalmazott hibamenedzsment eljárások optikai hálózatokban alapvetően három fázisra oszthatóak, melyek mindegyikéhez több módszer és megközelítés közül kell kiválasztani a hálózat igényeinek legmegfelelőbb megoldást:

(i) hibák esetén az összeköttetés megszakadásának megelőzése (*védelem*),

(ii) meghibásodások gyors és pontos *detektálása*,

(iii) megszakadt összeköttetések *helyreállítása*.

Annak érdekében, hogy a szolgáltatóknak a szolgáltatásaik eltérő QoS követelményeihez leginkább illeszkedő módszert választhassák, fontos, hogy több hatékony módszer álljon rendelkezésre az optikai hibamenedzsment mindhárom fázisában.

A kutatás célja a felhasználó által igényelt QoS szinthez rugalmasan illeszkedő, megbízható összeköttetések kiépítéséhez és helyreállításának biztosításához szükséges elméleti alapok és gyakorlati módszerek ajánlása, azaz az optikai hibamenedzsment (i) fázisának támogatása. Azaz a célom egy olyan **új matematikai modellt javasolni hozzárendelt védelemre**, amely implementációs kérdések helyett (pl.: diszjunkt útpár keresése az összeköttetés / védendő szegmens forrás és célcsomópontja között) a felhasználó tényleges igényeire koncentrálva határozza meg a hálózatban alkalmazott védelmi struktúrát, ezáltal sokkal nagyobb szabadságot biztosítva a szolgáltatónak az összeköttetés kiépítésekor, mint a korábbi hozzárendelt védelmi eljárások.

# 2. Általános hozzárendelt védelem optikai gerinchálózatokban

Telekommunikációs hálózatokban a kritikus alkalmazások magas QoS követelményeinek biztosításához nem engedhető meg az az egyszerűsítés, hogy a linkek meghibásodása egymástól független esemény [16]. A kutatás során a pontos hibamodell érdekében az összefüggő meghibásodások kezelésére az irodalomban legelterjedtebb modellt, a közös kockázatú csoportokat (shared risk link group, SRLG) alkalmazom [6]. Egy SRLG kifejezi a statisztikai összefüggőséget a benne lévő linkek meghibásodásai között, azaz a benne lévő linkek egy bizonyos esemény hatására (pl.: kábel átvágás, vonali kártya hiba) egyszerre válnak használhatatlanná. Egy SRLG tetszőleges számú linket tartalmazhat, és egy link tetszőleges számú SRLG-ben lehet benne [17].

A leggyakoribb ok, ami miatt két link azonos SRLG-be kerülhet, hogy azonos logikai struktúrában vannak (pl.: két látszólag független fényút azonos fizikai linket használ), vagy a földrajzi közelségük miatt vannak közös veszélynek kitéve (pl.: épületből kimenő linkeket azonos kábelbe szokták fektetni). Mivel a linkek közötti összefüggőségek automatikusan nem nyerhetőek ki teljes biztonsággal a hálózatból [4] és viszonylag statikus információnak számítanak, elegendő őket egy központi adatbázisban tárolni. Megbízható hálózatokban útvonalválasztás, vagy hibalokalizáció tervezése esetén elegendő az adott hibamenedzsment rutinhoz szükséges, adott QoS osztályhoz tartozó $\mathcal{F}$ SRLG lista lekérdezése a központi adatbázisból.

Az irodalomban megbízható hálózatokban leggyakrabban alkalmazott, illetve statisztikailag a leggyakrabban bekövetkező meghibásodásokat tartalmazó $\mathcal{F}$ SRLG listákat tartottam szem előtt [20] a javasolt algoritmusok tervezésénél, melyek:

(1) $\mathcal{F}$ tartalmazza az összes egyszeres linkhibát,

(2) $\mathcal{F}$ tartalmazza az összes egyszeres és kétszeres linkhibát,

(3) $\mathcal{F}$ tartalmazza az összes egyszeres linkhibát és tetszőleges számú többszörös szomszédos linkhibát (magába foglalva akár csomópont hibákat is).

Optikai hálózatokban – a konkrét technológiától eltekintve – virtuális áramkörkapcsolást alkalmaznak, ahol egy-egy SRLG kiesése az áramkör megszakadását eredményezheti, melynek újbóli kiépítése a QoS követelménynek nem megfelelő késleltetést

okozhat. Kritikus, hogy a szolgáltató által a QoS osztályhoz adott valamennyi $f \in F$ hibára fel legyünk készülve, beszéljünk akár az optikai hibamenedzsment (i) vagy (ii) fázisáról.

Egyes alkalmazások (pl.: távoli műtétek végzése) esetén a hiba detektálása / lokalizálása után való új útvonal keresése (helyreállítás) esetleg az SLA alapján nem megengedhető késleltetést okozna. Az olyan alkalmazásoknál, ahol a legkisebb kiesés sem tolerálható, a szolgáltatónak valamilyen védelmi eljárást kell alkalmazni, mely esetén a felhasználó által előfizetett QoS igénynek megfelelően kell az összeköttetést kiépítenie, azaz **az $\mathcal{F}$ listában található hibák esetén a szolgáltatás nem szakadhat meg**. Mindez azt eredményezi, hogy a szolgáltatónak a hálózat hibamentes állapotában használt *üzemi erőforrásokon* (sávszélesség, tároló, processzor idő) túl az összeköttetés által csak hiba esetén használandó *védelmi erőforrásokat* is előre le kell foglalnia.

Annak érdekében, hogy a hálózatban a lehető legtöbb kapcsolatot létesítsük, a védelmi erőforrásokkal a szolgáltatónak a QoS igényeket figyelembe véve a lehető legtakarékosabban kell bánnia. Ennek érdekében egy egységnyi védelmi kapacitást megoszthat olyan felhasználók között, akik üzemi erőforrásai függetlenek egymástól (*megosztott védelem*) [9]. Ebben az esetben hiba esetén a védelmi erőforrást egyszerre legfeljebb egy felhasználó szeretné használni (akinek az üzemi erőforrásai meghibásodtak). A megosztott védelmi megközelítés ugyan gazdaságosan bánik az erőforrásokkal, de a megosztás mértékétől függően az útvonalak meghatározása komplex feladat, mindemellett a gyakorlati alkalmazása is bonyolult. Ezenkívül meghibásodás esetén a hiba tényét vissza kell terjeszteni a hálózatban az összeköttetés forráscsomópontjához, hogy az valamely előre lefoglalt útvonalon folytassa a felhasználó adatának küldését, mely extra késleltetést eredményez az összeköttetés helyreállításáig.

Kevésbé gazdaságos, de a megosztott védelem hátrányait elkerülő (emiatt a gyakorlatban elterjedt [7]) megközelítés, hogy egy egységnyi védelmi erőforrást kizárólag egy felhasználó használhat, azaz egy-egy hozzárendelést valósít meg az erőforrás és a felhasználó között (*hozzárendelt védelem*). Az egy-egy hozzárendelés miatt a felhasználói adat akár folyamatosan küldhető az üzemi erőforrásokon felül az összes védelmi linken is (hot stand-by). Így, az üzemi utat érintő hiba észlelése esetén elegendő az

1. táblázat. Általános hozzárendelt védelem esetén alkalmazott jelölések

| Jelölés | Leírás |
|---|---|
| $\mathcal{I} = \{G, \mathcal{D}, \mathcal{F}\}$ | az útvonalválasztási feladat egy példánya |
| $G = (V, E)$ | a hálózat irányított vagy irányítatlan gráfmodellje $V$ csomópont és $E$ élhalmaz esetén |
| $c_e$ | az éleken definiált költségfüggvény $e \in E$ |
| $k_e$ | az éleken rendelkezésre álló szabad kapacitás $e \in E$ (BU) |
| $\mathcal{D} = (s, d, b)$ | a dinamikusan érkező igény forrás- és célcsomópontja, valamint sávszélességigénye |
| $\mathcal{F}$ | a szolgáltató által meghatározott közös kockázatú csoportok listája, amely ellen az összeköttetést védeni kell |
| $G_f = (V, E_f)$ | az adott $f \in \mathcal{F}$ csoportban meghibásodott élek törlésével nyert SRLG gráf |
| $\mathcal{X}_\mathcal{I}$ | az $\mathcal{I}$ bemenetet kielégítő $y_\mathcal{I}$ megoldások halmaza |
| $y_\mathcal{I} = \{H, \mathcal{R}\}$ | egy kielégítő megoldás tartalmazza a megfelelő részgráfot $H$ és a csomópontok konfigurációját $\mathcal{R}$ |
| $b_e$ | az $e \in E$ élen foglalt kapacitás a megoldásban (BU) |

útvonalválasztóknak egy másik bejövő interfészre kapcsolni az összeköttetés folytonosságának biztosításához, mely a szigorú (50 ms) optikai időzítési követelményeket teljesíti.

Az olyan megoldásokat, amelyek nem szakadnak meg egyetlen $f \in \mathcal{F}$ hiba esetén sem *ellenálló*, amelyek esetén a helyreállítás lokális döntés alapján eldönthető a vezérlő síkon (Control Plane, CP) küldött konstans jelzés segítségével *robusztus* megoldásnak nevezzük. *Ellenálló és robusztus (E&R)* megoldások esetén elkerülhető az optikai kapcsolók (OXC) újrakonfigurálása, mely nem skálázható megoldást eredményezne, ezen túlmenően a költséges és időigényes volta miatt esetleg nem megengedhető késleltetést eredményezne az optikai helyreállításban.

Az irodalomban található E&R módszerek implementációs kérdésekből indulnak ki, azaz előre megadják, hogy milyen struktúra formájában keressük az útvonalválasztási feladat megoldását. Az $1 + 1$ védelem él- vagy SRLG-független útvonalpár formájában keresi az útvonalválasztási feladat megoldását a forrás- és célcsomópont között [6] [7]. Ekkor egy optikai osztót alkalmaznak a forrásban, míg egy optikai kapcsolót alkalmaznak a célcsomópontban, melynek egyetlen feladata, hogy a hiba

észlelése esetén a másik bejövő interfészre kapcsoljon. Az $1+1$ módszer gyorsasága és egyszerűsége miatt a leginkább elterjedt módszer optikai gerinchálózatokban. Abban az esetben, ha az üzemi útvonalat linkekre, vagy (átlapolódó vagy nem átlapolódó) szegmensekre osztjuk, és a szegmens két végpontja között számolunk egy független útvonalat *hozzárendelt szegmens (vagy link) védelemnek* [7], vagy *részleges útvédelemnek* [21] [23] nevezzük. Ugyan szegmens védelem esetén már magas QoS (áramkörkapcsolt hálózatokban leggyakrabban *rendelkezésre állás*) biztosítható az összeköttetéseknek, de a hozzárendelt védelmi erőforrások gazdaságtalan használata miatt a módszer rossz hálózatkihasználtságot eredményez, mely a gyakorlati alkalmazását nem teszi vonzóvá.

Az előzőekben ismertetett, implementációs kérdésekre koncentráló módszerekkel szemben az általam javasolt matematikai modell általánosan fogalmazza meg a hozzárendelt útvonalválasztási feladatot, és a védelmi struktúra meghatározását az optimalizálási feladatra bízza. Az útvonalválasztás dinamikus változatát vizsgálom, azaz minden összeköttetés igényt a forrás útvonalválasztóhoz való érkezésének $t$ pillanatában elvezetünk.

Jelölje $\mathcal{I} = \{G, \mathcal{D}, \mathcal{F}\}$ az *általános hozzárendelt védelem (GDP)* egy tetszőleges példányát.

- A dinamikus összeköttetés igény érkezésének pillanatában a hálózat aktuális állapotát a $G = (V, E)$ gráf írja le, ahol minden $e \in E$ élen egy nemnegatív költségfüggvény ($c : E \to R^+$) illetve az aktuális szabad kapacitás ($k : E \to R^+$) adott. A linkeken rendelkezésre álló szabad kapacitás a hálózatban $t$ előtt felépített illetve lebontott összeköttetések függvénye.

- Az összeköttetés igény $\mathcal{D} = (s, d, b)$ tartalmazza az összeköttetés $s$ forráscsomópontját és $d$ nyelőcsomópontját, az igényelt sávszélességet ($b \in \mathbb{N}$) sávszélesség egységben ($BU$) megadva.

- Végül a bemenet részeként adva van a hálózat operátor által definiált, az SLA-ban megadott QoS szint teljesítéséhez védeni szükséges SRLG-k $\mathcal{F}$ listája, melyet figyelembe kell venni az útvonalválasztási döntés meghozatalakor. Minden SRLG-hez (hibamintához) tartozik egy $\forall f \in \mathcal{F} : G_f = (V, E_f)$ segédgráf, melynek az $E_f$ élhalmazát az $f$ hibamintában megadott meghibásodott élek

törlésével nyerünk $E$-ből. Feltételezzük, hogy valamennyi SRLG az $\mathcal{F}$ listában *védhető*, azaz minden $G_f$ gráf $s-d$ összefüggő.

Jelölje $\mathcal{X}_\mathcal{I}$ az $\mathcal{I}$ példányt kielégítő $y_\mathcal{I} = \{H, \mathcal{R}\}$ megoldások halmazát, mely tartalmaz:

- egy $H = (V, E)$ részgráfot az éleken adott $\forall e \in E : b_e \leq k_e$ kapacitás értékekkel, melyek a megoldásban a folyam értékét jelentik. A megoldás az *összes* $f \in \mathcal{F}$ *hibának ellenáll*, azaz a $H = (V, E)$ gráfban és a $\forall H_f = (V, E_f)$ SRLG gráfban a maximális folyam értéke $s$ és $d$ között legalább $\geq b$.

- Egy kielégítő GDP megoldás másik fele egy robusztus konfiguráció $\mathcal{R}$, amely megadja az optikai csomópontok (OXC) beállításait kapcsolatfelépítéskor (pl.: kapcsoló mátrix, jelek összevonása, esetleg a forgalomszövéshez szükséges információk).

Minden kielégítő $y_\mathcal{I} \in \mathcal{X}_\mathcal{I}$ GDP megoldáshoz egy $f(y_\mathcal{I})$ költséget rendelünk az összeköttetés számára lefoglalt erőforrások függvényében, azaz:

$$f(y_\mathcal{I}) = \sum_{\forall e \in E} c_e \cdot \frac{b_e}{b}, \tag{1}$$

ahol $b_e \leq k_e$ a $H = (V, E)$ megoldásban használt sávszélesség $BU$-ban az $e \in E$ linken. A kielégítő GDP megoldást kereső algoritmusok célja ezen költségfüggvény minimalizálása. Az alkalmazott jelöléseket az 1. táblázat tartalmazza.

A hálózatban rendelkezésre álló optikai eszközök, illetve alkalmazott technológiai megoldásoknak megfelelően két feladatot definiálok. Abban az esetben, ha a GDP megoldást osztatlan folyamok formájában keresünk **IGDP feladatnak**, ha a folyamok osztása és hálózati kódolás alkalmazása is megengedett az egyes linkeken **GDP-NC feladatnak** nevezem. A GDP feladat megoldására javasolt algoritmusokat a 2. táblázatban foglaltam össze.

Korábbi munkám során bebizonyítottam, hogy az IGDP feladat optimális megoldásának megtalálása NP-teljes komplexitású, mind irányított mind irányítatlan gráfmodell esetén [2]. Az eltérő gráfmodelleknek a feladat approximálhatósága szempontjából van egyedül jelentősége, ugyanis csak az irányítatlan esetnek létezik konstans faktorú, nevezetesen közel 2-approximációja [10].

2. táblázat. Ajánlott algoritmusok a különböző GDP feladatokra

| | IGDP | GDP-NC |
|---|---|---|
| optimális megoldás | ILP | LP |
| heurisztika | DH, BEA | - |

Mivel az IGDP feladat NP-teljes komplexitású, ezért a kommunikációs hálózatokban gyakran alkalmazott megközelítésnek megfelelően az optimális IGDP megoldás megtalálására felírtam az egészértékű lineáris programot (ILP). Ajánlottam egy hatékony és gyors, Dijkstra algoritmusán [5] alapuló heurisztikát kielégítő IGDP megoldás találására. Az ILP magas számítási komplexitása miatt szükséges egy gyors heurisztikát megfogalmazni (**Dijkstra Heuristic, DH**), mely gyorsan szolgáltat egy kielégítő IGDP megoldást még akkor is, ha ez nem minimális költségű. Szimulációkkal igazoltam, hogy a legtöbb bemenet esetén a heurisztika által adott megoldás jól közelíti az optimális megoldást. Az algoritmusról analitikusan beláttam, hogy nem approximálja a feladatot egy megfelelően szerkesztett $\mathcal{F}$ SRLG listával egy $G_k = (V, E)$ gráfcsalád tagjain a $\mathcal{D} = (s, d, 1)$ igényre, mely esetén a heurisztika által adott megoldás az optimális megoldás $|\mathcal{F}|$-szorosánál 3-mal több élet használ.

A DH algoritmus jelentősége gyorsaságán túl abban rejlik, hogy több heurisztikus eljárásban használható építőelemként. A heurisztikára építve egy kvázi-optimális megoldást szolgáltató meta-heurisztika került kidolgozásra [15]. A bakteriális evolúciós algoritmuson (**Bacterial Evolutionary Algorithm, BEA**) alapuló módszer nagy gráfok, illetve sok SRLG-t tartalmazó $\mathcal{F}$ listák esetén hatékonynak bizonyult.

Megvizsgáltam a GDP feladat legáltalánosabb változatát (GDP-NC), azaz bonyolultabb hálózati eszközök alkalmazásával mennyivel csökkenthető a GDP feladat 1. egyenletben megfogalmazott költsége. Ez annak az esetnek felel meg, amikor az egyes OXC-kben a bejövő optikai jeleken algebrai operációkat végező eszközöket tételezünk fel [12].

A GDP-NC feladatról analitikusan megmutattam, hogy hálózati kódolás alkalmazásával polinom időben megoldható. Példát adtam annak a demonstrálására, hogy az LP relaxált ellenálló, de hálózati kódolás alkalmazása nélkül nem robusztus megoldást szolgáltat. Az IGDP feladatra felírt ILP feladat LP relaxáltja szolgáltat ugyan

egy ellenálló optimális részgráfot, de robusztus megoldást csak abban az esetben kaphatunk, ha valamilyen kódolást végeznünk a csomópontokon. A korábban multicast feladat megoldására adott kódolási eljárások bemenetet úgy módosítottam, hogy azok az LP által adott ellenálló $H = (V, E)$ gráf egy robusztus kódolását szolgáltassák. A javasolt módszerek

- a speciális kódstruktúrának köszönhetően mindig garantálják a robusztus kód létezését,
- míg random kódok alkalmazásával nagy valószínűséggel megfelelő kódokat kapunk, mely az alkalmazás szempontjából megengedhető bizonytalanságot visz be a rendszerbe.

# 3. Szimulációs eredmények

A javasolt polinomiális futási idejű (GDP-NC) és bakteriális módszer erőforrás használatát, futási idejét és blokkolási valószínűségét szimulációk segítségével megvizsgáltam. A hálózatok élei egységnyi költségűek 32 hullámhosszal. A bejövő forgalmak egységnyi sávszélességet foglalnak, és Poisson folyamat szerint érkeznek exponenciális eloszlású időközökkel, átlagosan 5 időegységenként. Az adatokat 10, különböző 200 igény elvezetésének átlagaként nyertük, valamint feltüntettük a 95%-os konfidencia intervallumot.

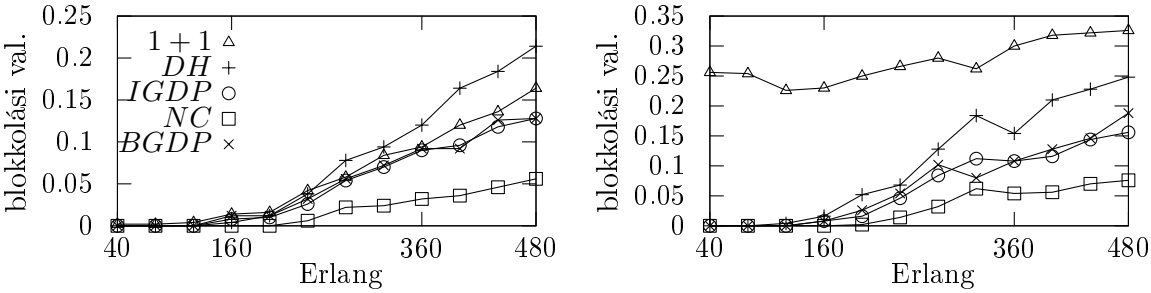
Mivel az optikai szálakat gyakran fektetik közös kábelbe, ezáltal gyakran egyszerre hibásodnak meg, ezért a szimulációkban elsősorban szomszédos linkhibákat vizsgálunk [13] [3] ((3) típusú lista). Ezen belül a $p\%$ paramétertől függően megkülönböztetjük, hogy a lista az egyszeres hibákon felül hány százalék szomszédos dupla hibát tartalmaz. Egyszeres hiba esetén $p = 0$, míg az alacsony, közepes és magas lista esetén $p$ rendre $10, 50$ és $90$. Az $\mathcal{F}$ lisában található SRLG számra a 3. táblázatban látható példa.

Az ábrákon $BEA$ a javasolt bakteriális módszert jelöli, $NC$ a javasolt polinom idejű, hálózati kódolást igénylő megoldást, míg $DH$ és $ILP$ a [19] és [2] cikkekben javasolt heurisztikus és optimális módszerre vonatkozik.

Az $1 + 1$ módszert Suurballe algoritmusának [18] segítségével implementáltuk.

3. táblázat. Az SRLGs szám az $\mathcal{F}$ listában a COST266 Core hálózatban [11]

| SRGL lista | Egyszeres | Alacsony | Közepes | Magas | Sűrű |
|---|---|---|---|---|---|
| SRLG szám | 23 | 27 | 43 | 60 | 276 |




(a) Egyszeres link hibák (1)

(b) 10% dupla hiba (3)

1. ábra. Blokkolási valószínűség (1) és (3) típusú SRLG listák mellett a 37 csomópontos COST266 hálózatban [11].

Megjegyzendő, hogy az $1 + 1$ nem ellenálló az $\mathcal{F}$ listában szereplő összes hibával szemben többszörös hibák esetén, ezért csak referenciaként vehető figyelembe.

## 3.1. Polinomiális futási idejű GDP-NC módszer analízise

A GDP-NC az általánosabb eszközöknek köszönhetően mind az erőforrás használatban, mind a futási időben javított az ILP teljesítményén. A legjelentősebb előrelépés azonban a blokkolási valószínűség esetén mutatkozik a korábbi módszerekhez képest, ugyanis dinamikus forgalmak esetén is jelentősen több felhasználó engedhető be a rendszerbe hálózati kódolás alkalmazásával. A szimulációs eredmények összefoglalása az 1. ábrán látható. Megállapítható, hogy az implementációs kérdésekre koncentráló $1 + 1$ védelem (1) típusú listáknál még jól teljesít, azonban (3) típusú $\mathcal{F}$ SRLG lista esetén már jelentős blokkolás történik. Addig az optimális GDP algoritmusok minden típusú bemeneti SRLG listára meggyőző teljesítményt nyújtanak.

A szimulációkban a költségfüggvényt együtt optimalizáltam az üzemi és védelmi élekre. Megjegyzendő, hogy a feladat változtatása nélkül egy megfelelő inputtal előre

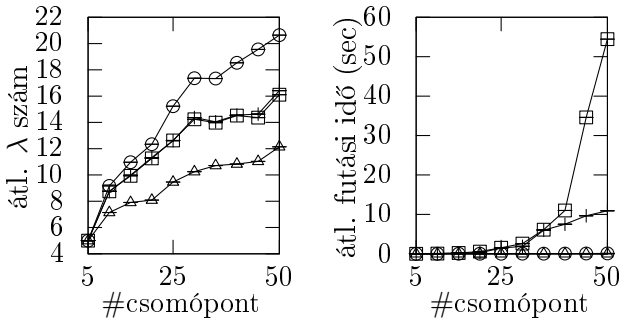
számolt üzemi útvonal esetén is képes optimális védelmi struktúrát szolgáltatni. Azáltal, hogy a GDP általános matematikai modellje az optimalizációra bízza a csomóponti szerepek kialakítását az implementációs kérdésekre koncentráló korábbi módszerekkel szemben, a legtöbb módszer esetén előforduló *csapda szituáció elkerülhető* [22]. Könnyen végiggondolható, hogy ha létezik megoldása a GDP feladatnak egy $\mathcal{W}_1$ üzemi útvonal esetén, akkor bármely másik $\mathcal{W}_2$ üzemi úttal is létezik, azaz a legrövidebb útvonal választása üzemi útként nem befolyásolja a védelmi struktúra létezését, és ezáltal az összeköttetés kiépítését.

## 3.2. A meta-heurisztikus bakteriális módszer analízise

A fejezetben különböző átlagos fokszámmal (2,3 és 4,5 között) rendelkező random hálózatokon végeztünk szimulációkat a javasolt bakteriális $BEA$ algoritmus teljesítményének vizsgálatára, melyeket az `lgfgen` LEMON [1] gráfgenerátorral készítettünk.

Miután az eltérő sűrűség hatását megvizsgáltuk, a COST266 core európai hálózaton végzünk szimulációkat [11]. A hálózatnak 16 csomópontja és 23 éle van, míg az átlagos fokszám $2,88$ (min. 2, max. 5).

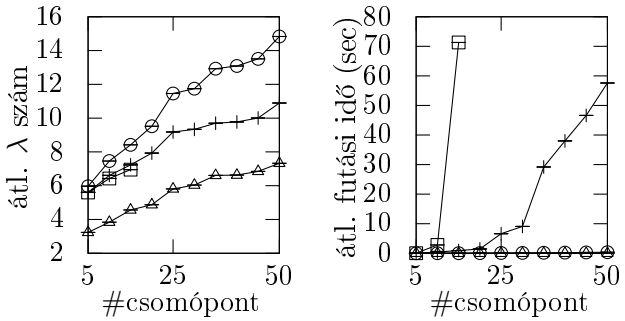
Előzetes szimulációk segítségével megállapítottuk a bakteriális módszer szükséges paramétereit, azaz a baktériumszámot, a klónok számát, a mutációs rész nagyságát és a generációk, valamint a géntranszferek számát. Ennek megfelelően a hálózatok döntő többsége esetén 3-ra állítottuk a paramétereket.




(a) átlagos $\lambda$ szám (b) átlagos futási idő (sec)

2. ábra. A 200 igény által átlagosan használt hullámhossz szám a COST266 core hálózatban **magas SRLG szint mellett ritka hálózatokban**, ahol az $1+1$, $DH$, $ILP$ és $BEA$ módszert rendre $\triangle$, $\circ$, $\square$ és $+$ jelöli.

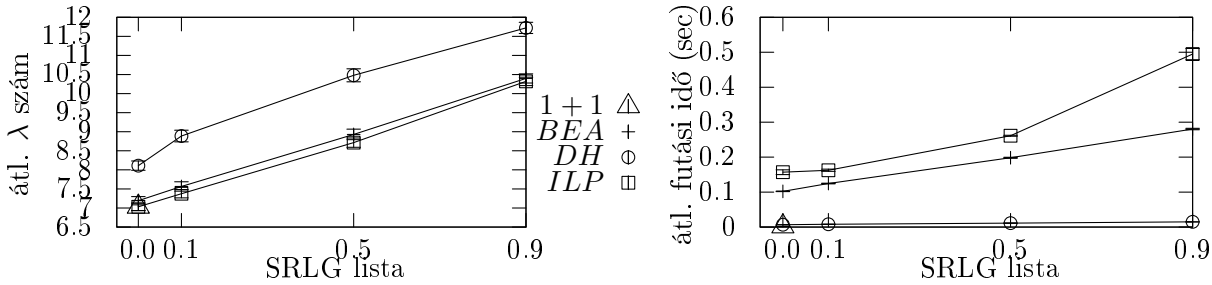
Ritka hálózatok esetén minden módszer erőforrás használata növekszik, ahogy a hálózat mérete nő (2. ábra). A BEA által adott kvázi-optimális megoldás megközelíti az ILP által adott optimális megoldást, míg futási időben jelentősen túlszárnyalja (54 s helyett akár 10 s). Sűrű hálózatok esetén a BEA teljesítménye hasonló, míg a futási időben még jelentősebb a meta-heursztikus módszer előnye az ILP-vel szemben (3. ábra).




(a) átlagos $\lambda$ szám (b) átlagos futási idő (sec)

3. ábra. A 200 igény által átlagosan használt hullámhossz szám a COST266 core hálózatban **magas SRLG szint mellett sűrű hálózatokban**, ahol az $1+1$, $DH$, $ILP$ és $BEA$ módszert rendre $\triangle$, $\circ$, $\square$ és $+$ jelöli.

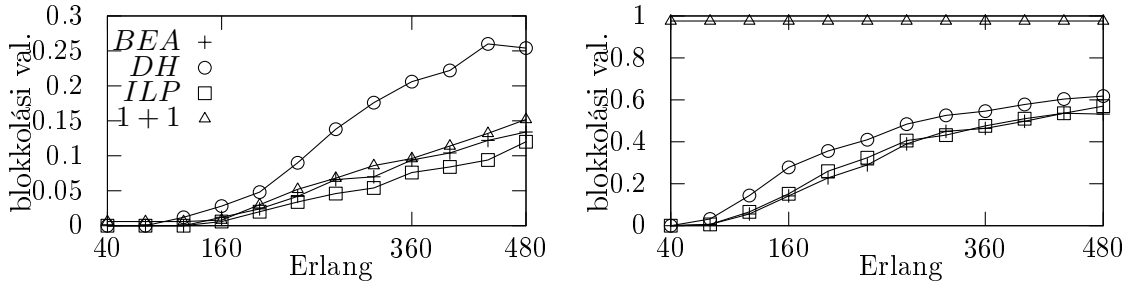
A topológia analízis után a továbbiakban a COST266 core hálózaton folytatjuk a módszerek teljesítményének elemzését eltérő SRLG listák esetén (4. ábra), melyen hasonló tendencia figyelhető meg, mint a korábbi szimulációk során. Az elblokkolt összeköttetések számát az 5. ábra szemlélteti (1) és (3) típusú SRLG lista esetén. Magas SRLG lista esetén a GDP módszer általánosságának köszönhető legfőbb előnye jól kivehető. Míg egyszeres hibák esetén a heurisztikus DH módszer blokkolja a legtöbb összeköttetés igényt, addig magas SRLG szám mellett az $1+1$ módszer az igények jelentős része esetén nem képes az összes hibát védeni, mivel nem létezik SRLG független útvonal a gráfban, így a módszer blokkolása jelentősen megnő.




(a) átlagos $\lambda$ szám

(b) átlagos futási idő (sec)

4. ábra. A 200 igény által átlagosan használt hullámhossz szám a COST266 core hálózatban. (Megj.: $1+1$ csak egyszeres hibák ellen véd garantáltan).




(a) Egyszeres hibák

(b) Magas SRLG szint

5. ábra. Blokkolási valószínűség COST266 core hálózaton.

# 4. Összefoglalás

A 2. fejezetben bemutatott matematika modell szakít az implementációs kérdésekre koncentráló korábbi hozzárendelt védelmi megközelítésekkel. Olyan flexibilis módszert biztosít a szolgáltatók számára, mely a felhasználó QoS igényeinek legmegfelelőbb védelmi struktúra kialakítását teszi lehetővé, ezáltal nagyban csökkentve a lefoglalt erőforrásokat. A javasolt algoritmusok bármely dinamikusan kapcsolt optikai hálózatban alkalmazhatóak az összeköttetések védelmének biztosítására. A szolgáltatónak csak ki kell választatnia a hálózatban telepített eszközök képességeihez leginkább illeszkedő megközelítést.

Jelen kutatás célja meta-heurisztikus (BEA), valamint polinom idejű (NC) módszerek kidolgozása volt a GDP feladatra a korábban létező optimális (ILP) és heurisztikus (DH) módszereken felül. A 3. fejezetben szimulációs eredményekkel igazoltuk az új módszerek által elért teljesítménynövekedést.

# Hivatkozások


[1] Lemon: A c++ library for efficient modeling and optimization in networks. Technical report, http://lemon.cs.elte.hu.

[2] P. Babarczi, J. Tapolcai, and P.H. Ho. Availability-constrained Dedicated Segment Protection in circuit switched mesh networks. In *Ultra Modern Telecommunications and Workshops, 2009. ICUMT '09. International Conference on*, pages 1–6, 2009.

[3] H. Choi, S. Subramaniam, and H.A. Choi. Loopback recovery from neighboring double-link failures in WDM mesh networks. *Information Sciences*, 149(1-3):197–209, 2003.

[4] G. Das, D. Papadimitriou, W. Tavernier, D. Colle, T. Dhaene, M. Pickavet, and P. Demeester. Link State Protocol data mining for shared risk link group detection. In *Computer Communications and Networks (ICCCN), 2010 Proceedings of 19th International Conference on*, pages 1–8. IEEE, 2010.

[5] EW Dijkstra. A note on two problems in connexion with graphs. *Numerische mathematik*, 1(1):269–271, 1959.

[6] Georgios Ellinas, Eric Bouillet, Ramu Ramamurthy, Jean-Francois Labourdette, Sid Chaudhuri, and Krishna Bala. Routing and restoration architectures in mesh optical networks. *Optical Networks Magazine*, pages 91–106, January/February 2003.

[7] A. Fumagalli and L. Valcarenghi. IP restoration vs. WDM protection: is there an optimal choice? *Network, IEEE*, 14(6):34–41, 2000.

[8] Konstantinos N. Georgakilas, Kostas Katrinis, Anna Tzanakaki, and Ole B. Madsen. Impact of Dual-Link Failures on Impairment-Aware Routed Networks. In *Transparent Optical Networks, 2010. Proceedings of 2010 12th International Conference on*. IEEE, 2010.

[9] Pin-Han Ho, J. Tapolcai, and T. Cinkler. Segment shared protection in mesh communication networks with bandwidth guaranteed tunnels. *IEEE/ACM Transactions on Networking*, 12(6):1105–1118, December 2004.

[10] J. Konemann, S. Leonardi, G. Schafer, and S. van Zwam. From primal-dual to cost shares and back: a stronger LP relaxation for the Steiner forest problem. *Automata, languages and programming*, pages 930–942, 2005.

[11] S.D. Maesschalck, D. Colle, I. Lievens, M. Pickavet, P. Demeester, C. Mauz, M. Jaeger, R. Inkret, B. Mikac, and J. Derkacz. Pan-European optical transport networks: an availability-based comparison. *Photonic Network Communications*, 5(3):203–225, 2003.

[12] E.D. Manley, J.S. Deogun, L. Xu, and D.R. Alexander. Network Coding for WDM All-Optical Multicast. *CSE Technical reports*, page 10, 2009.

[13] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.N. Chuah, and C. Diot. Characterization of failures in an IP backbone. In *Proc. IEEE Infocom*, volume 4, pages 2307–2317. Citeseer, 2004.

[14] H.T. Mouftah and P.H. Ho. *Optical networks: architecture and survivability.* Kluwer Academic Publishers, 2003.

[15] P. Soproni, P. Babarczi, J. Tapolcai, T. Cinkler, and P.-H. Ho. A Meta-Heuristic Approach for Non-Bifurcated Dedicated Protection in WDM Optical Networks. In *Design of Reliable Communication Networks, (DRCN)*, 2011.

[16] J. Spragins. Dependent Failures in Data Communication Systems. *IEEE Transactions on Communications, [legacy, pre-1988]*, 25(12):1494–1499, 1977.

[17] J. Strand, AL Chiu, and R. Tkach. Issues for routing in the optical layer. *IEEE Communications Magazine*, 39(2):81–87, 2001.

[18] J. W. Suurballe and R. E. Tarjan. A quick method for finding shortest pairs of disjoint paths. *Networks*, 14(2):325–336, 1984.

[19] J. Tapolcai, P. Babarczi, and P.H. Ho. Dedicated Protection Scheme with Availability Guarantee. In *The 13th International Telecommunications Network Strategy and Planning Symposium, 2008. Networks 2008.*, pages 1–11, 2008.

[20] S. Verbrugge, D. Colle, P. Demeester, R. Huelsermann, and M. Jaeger. General availability model for multilayer transport networks. In *Proceedings. 5th International Workshop on Design of Reliable Communication Networks, 2005.(DRCN 2005).*, page 8, 2005.

[21] H. Wang, E. Modiano, and M. Médard. Partial path protection for WDM networks: End-to-end recovery using local failure information. In *Computers and Communications, 2002. Proceedings. ISCC 2002. Seventh International Symposium on*, pages 719–725. IEEE, 2002.

[22] D. Xu, Y. Xiong, C. Qiao, and G. Li. Trap avoidance and protection schemes in networks with shared risk link groups. *Journal of Lightwave Technology*, 21(11):2683, 2003.

[23] G. Xue, W. Zhang, T. Wang, and K. Thulasiraman. On the partial path protection scheme for WDM optical networks and polynomial time computability of primary and secondary paths. *MANAGEMENT*, 3(4):625–643, 2007.

[24] Y. Yano, T. Ono, K. Fukuchi, T. Ito, H. Yamazaki, M. Yamaguchi, and K. Emura. 2.6 Terabit/s WDM transmission experiment using optical duobinary coding. In *Optical Communication, 1996. ECOC'96. 22nd European Conference on*, volume 5, 1996.