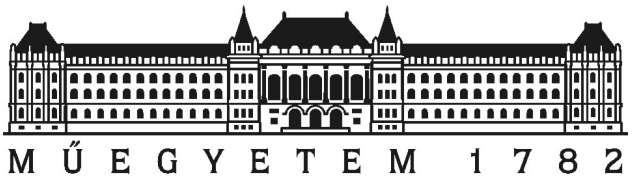


Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Távközlési és Médiainformatikai Tanszék
High-Speed Networks Laboratory (HSN*Lab*)
MTA-BME "Lendület" Jövő Internet kutatócsoport

Megbízható Távközlési Hálózatok

MTA doktori disszertáció tézisei

Tapolcai János, Ph.D.

Budapest
2012

1. Bevezető

Az Internet szolgáltatókon egyre nagyobb a nyomás, hogy hibamentes szolgáltatást nyújtsanak, ne csak a kiemelt ügyfeleik számára, hanem mindenkinek. Ez lassan rákényszeríti a szolgáltatókat, hogy a jelenleginél sokkal megbízhatóbb rendszereket alkalmazzanak. Az áttérésnek zökkenőmentesen, a háttérben kell lezajlania, az Internet Protokollra épülő rengeteg, már működő eszköz módosítása nélkül.

Úgy gondolom, a jövőben megjelennek olyan gerinc- és IP-hálózati megoldások, amelyek sokkal rugalmasabb és magasabb szintű szolgáltatásokat fognak nyújtani. A kutatásom során az Internet megbízható működéséhez kapcsolódó problémákat fogalmazok meg, elemzem és javaslatot teszek a kezelésükre szolgáló eljárásokra.

2. Kutatási előzmények és célkitűzések

Ehhez a technológia forradalomhoz a jelenleginél lényegesen rugalmasabb és megbízhatóbb gerinchálózati szolgáltatásra van szükség. A jövőben a nagysebességű – optikai – kapcsolatokat 100 ms alatt ki kell építeni, vagy le kell bontani. Ezeknek a kapcsolatoknak – a katasztrófákat leszámítva – mindig működniük kell.

A gerinchálózatok a nagy távolságok miatt különösen sebezhetőek, ezért a megbízhatóságuk javítására aktív védelmi módszereket implementálnak. A védelmi módszerek alapötlete, hogy meghibásodás esetén a kieső kapcsolatok adatforgalmát egy másik – ún. védelmi – útra terelik. Ahhoz, hogy a hiba ne okozzon komoly problémákat a felsőbb rétegek szolgáltatásaiban, az átkapcsolásnak legfeljebb néhány 100 ms alatt meg kell történnie.

A leggyakrabban elterjedt megoldás, hogy minden kapcsolathoz több útvonalat rendelnek: egy ún. üzemi utat, amelyen hibamentes esetben küldik az adatforgalmat, valamint védelmi utakat. A legegyszerűbb és egyben legelterjedtebb megoldás az 1+1 hozzárendelt védelem, amikor az adatot párhuzamosan küldik az üzemi és a tőle független védelmi úton. Ekkor az üzemi út meghibásodása esetén elég a végponton a védelmi útra átkapcsolódni. A módszer fő előnye, hogy meghibásodás esetén a kapcsolat néhány 10 ezredmásodpercig szakad csak meg, de hátránya, hogy a hálózat erőforrásigénye legalább duplája a védelem nélküli esetnek. A meghibásodások viszonylag ritka események, dupla erőforrást foglalni minden kapcsolatnak túlzás és drága megoldás.

Kihasználva a tényt, hogy a sok védelmi út közül a hálózatban egyszerre csak néhány fog üzemelni, hiszen a hibák ritkák, és a többszörös

hibák még ritkábbak, a védelmi utak kapacitását meg lehet osztani. A módszert megosztott védelemnek nevezik és sokan tanulmányozták az elmúlt évek során. Igazán akkor működik jól, ha a hálózat linkjei és csomópontjai kellően megbízhatók. Ilyenkor elég egyszeres link- vagy csomópont-meghibásodás ellen védekezni és a megosztott védelem segítségével kb. 25% erőforrás megtakarítást lehet elérni a hozzárendelt védelemhez képest, vagyis a védelmi utak lefoglalt kapacitása lényegében a felére csökken a megosztás következtében. A módszer rosszul működik ritka hálózattopológiákon, vagy, ha többszörös meghibásodás ellen is szeretnénk védeni a hálózatot. Gyakran ilyenkor nincs lehetőség kellően független védelmi utakra, mivel vagy a sok út és hibaállapot miatt jelentős erőforrást kell lefoglalnunk, vagy túl bonyolult a védelmi utak számolása. Erre jó megoldás lenne a helyreállítás.

A helyreállítás alapja, hogy a kapcsolat kiépítésekor nem számol előre védelmi utakat, csak lefoglal egy kevés védelmi kapacitást a linkeken, majd a védelemhez szükséges többi feladatot már csak a meghibásodás után végzi el. Ekkor a meghibásodás után azonosítja a hibás hálózati elemeket, majd az érintett kapcsolatoknak védelmi utakat alakít ki. A helyreállítás több szempontból is sokkal korszerűbb megoldás, mint a hagyományos védelem. Egyfelől lényegesen egyszerűbb kapcsolatokat kialakítani benne, hiszen új kapcsolat létrehozásakor elég az üzemi utat lefoglalni, a védelmi út számolása és foglalása csak a meghibásodás után történik. Ezáltal ez a mechanizmus jobban illeszkedik egy flexibilis gerinchálózat kialakításának igényeihez. Másrészről kevesebb védelmi erőforrást használ, mint bármely előre tervezett védelem: például egyszeres linkhiba esetén 74%-kal kevesebb védelmi erőforrást igényel, mint a hozzárendelt védelem, és kétszeres linkhiba eseténél alig növekszik az erőforrás igénye (ami kb. 84%-kal kevesebb erőforrást jelent hozzárendelt védelemhez képest). Az előnyök ellenére a helyreállítást gerinchálózatokban alig vizsgálták, és nagyon kevés Internet szabvány született a témában. Ennek fő oka, hogy nehéz egy elosztott rendszerben gyorsan hibákat lokalizálni.

A közelmúltban megjelentek olyan megoldások, amelyek segítségével gyorsan és hatékonyan lehet hibát lokalizálni optikai hálózatokban. A módszer lényege, hogy monitorozó utakat alakítanak ki a hálózatban. Egy ilyen monitorozó út (m-út) nem más, mint egy fényút, amelyen folyamatosan teszt jeleket küldenek. Hiba esetén a nyelő csomópontba nem érkezik meg a teszt jel, melyből a csomópont tudni fogja, hogy az m-út mentén hiba történt. A disszertációban azt vizsgáltam, hogyan lehet ezeket az m-utakat úgy kialakítani, hogy az m-utak státusz in-

formációi alapján egyértelműen lehessen azonosítani a meghibásodott hálózati elemeket, valamint azt is megvizsgáltam, hogy miként érdemes ezt a helyreállítással együtt működtetni.

Számos olyan meghibásodás is bekövetkezhet, amelyet nem lehet az alsó rétegben kivédeni. Ilyen hiba például egy IP útválasztó részleges leállása, amit az alsó réteg nem észlel. Az IP rétegben 100 ezredmásodperc helyreállítási időt még tolerálnak az alkalmazások. A kutatásom során vizsgáltam az IP hálózatok gyors hiba helyreállítás (IPFRR - IP Fast Reroute) módszereit. IPFRR témakörben az elmúlt 10 évben kidolgozott rengeteg módszer közül egyedül az LFA (Loop Free Alternate) implementációja jelent meg kereskedelmi útválasztókban. Az LFA sikere az egyszerűségben rejlik, nem igényel IP szintű hibafelderítést és szétterjesztést, valamint teljes mértékben követi a hagyományos hop-by-hop csomagküldési koncepciót. A módszer lényege, hogy minden bejegyzéshez két – egy fő és egy védelmi – kimenő link-interfészt tárolnak. Alapesetben a csomagot a címének megfelelő fő link-interfészre küldi tovább az útválasztó, kivéve ha fő linkjén hibát észlel, ekkor a csomagot a védelmi kimenő linkre küldi. A disszertációban vizsgáltam, hogyan kell a hálózatot úgy konfigurálni, hogy a védelmi linkre küldés után sose (vagy minél ritkábban) alakulhasson ki hurok. Egy másik IPFRR megvalósítást, a védett útválasztás (Protection Routing, PR) módszerét is vizsgáltam, ami az LFA-nál annyiban általánosabb, hogy a fő és védelmi kimenő link-interfészek kiosztását a hálózatban egy központi egység végzi, vagyis a útvonalak nem feltétlen az adminisztratív költség szerinti legrövidebb utak lesznek. Ehhez OpenFlow útválasztókra van szükségünk a hálózatban.

3. Kutatási módszerek

A modellezésnél és az algoritmusok kidolgozásánál elsősorban a kombinatorikus optimalizálás eredményeit használtam fel. Eredményeim főként gráfelméleten, kombinatorikus csoporttesztelésen és bonyolultságelméleten alapszanak. Célom a problémák egyedi tulajdonságainak és sajátosságainak megértése és ezek alapján célzott heurisztikus módszerek kidolgozása, amelyek a korábbi módszereknél nagyságrendekkel gyorsabbak és jobb megoldást találnak.

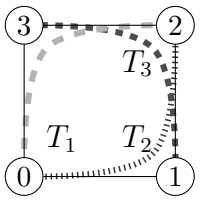
4. Új tudományos eredmények

4.1. Hibalokalizáció optikai hálózatokban

A felügyeleti fényutakkal való hibalokalizáció lényege, hogy erre dedikált fényutakat alakítanak ki a hálózatban. Az értekezésemben a fényút lehet tetszőleges összefüggő részgráfja a hálózatnak ((kétirányú) bidirectional m-trail, bm-út), vagy séta, azaz Euler-tulajdonsággal rendelkező (nem feltétlenül egyszerű) út (monitoring-trail, m-út). Hagyományos – központosított – megoldás esetén a monitorozó utak végén az optikai réteg optikai jelerősség monitorjai (Optical Power Monitor OPM) segítségével folyamatosan monitorozzuk a fényutak állapotát. A monitorozott fényút hibája esetén az OPM megfelelő jelzésüzenetet generál a vezérlősíkon, amiket egy központi hibamenedzser eszköz összegyűjt és ez alapján azonosítja a hibás elemet, majd levezényli a hálózat megfelelő átkonfigurálását. Ezen megoldás esetén a célunk olyan minimális számú m-útból álló rendszer kialakítása egy adott topológián, hogy az m-utak státuszinformációi alapján azonosítani lehessen a meghibásodott hálózati elemeket (ezt Unambiguous Failure Localization (UFL) tulajdonságnak nevezem). A bemeneti topológia gráfot $G = (V, E)$-vel, míg az m-utak számát b-vel jelölöm. A következő információelméleti alsó korlát mindig teljesül: $b \geq \lceil \log_2 |E| + 1 \rceil$. Optimálisnak hívom a megoldást, ha ennyi m-utat használ, és közel optimálisnak, ha ennél néhány m-úttal többet.

A központosított link-hiba monitorozó rendszerekben a monitorozó eszközök kommunikálnak egymással a meghibásodás utáni kritikus időszakban is. Ez komoly hibaforrás, mert a vezérlő sík működését is érintheti a hiba. A problémára lehetséges megoldás teljesen elosztott hibalokalizáció alkalmazása, ami meghibásodás utáni jelzésüzenetek nélkül képes azonosítani a hálózat minden csomópontjában a hibát. A dedikált fényutakat ilyenkor valamennyi áthaladó csomópontban monitorozzuk OPM segítségével. Ekkor célunk olyan minimális számú élből álló m-út rendszer kialakítása, ahol a hálózat minden csomópontja a rajta keresztül menő m-utak státuszinformációi alapján azonosítani tudja a meghibásodott hálózati elemeket (ezt Networkwide Local-UFL (NL-UFL) tulajdonságnak nevezem). Az m-utak összesített hosszát (élekben számolva) $\|\mathcal{T}\|$-vel jelölöm.

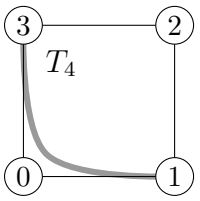
Az 1. ábrán egy egyszeres hibákat egyértelműen lokalizáló m-út megoldás található. A kihúzott felügyeleti fényutak ekvivalens megadása a hibakód tábla ($\underline{\underline{A}}$) az 1(b) ábrán látható. Az $\underline{\underline{A}}$ mátrix tartalmazza a linkekhez hozzárendelt egyedi kódot (pl.: a $(0, \overline{1})$ link esetén 110), mely



(a) UFL

Link	$T_1T_2T_3$
$(0,1)$	0 1 0
$(1,2)$	0 1 1
$(2,3)$	1 0 1
$(3,0)$	1 0 0

(b) $\underline{\underline{A}}$



(c) NL-UFL

Link	$T_1T_2T_4$
$(0,1)$	0 1 1
$(1,2)$	0 1 0
$(2,3)$	1 0 1
$(3,0)$	1 0 0

(d) $\underline{\underline{A}}^0$

1. ábra. Felügyeleti fényutakon alapuló gyors hibalokalizáció. Az (a) ábra mutatja az UFL-hez szükséges monitorozó utakat. Ezt kiegészítve a (c) ábrán látható T_4 m-úttal NL-UFL megoldást kapunk, ahol minden pont a rajta keresztül menő m-utak státuszinformációi alapján azonosítani tudja a meghibásodott hálózati elemeket. A (d) ábra mutatja a 0 pontban látható hibakódtáblát.

megadja, hogy az egyértelmű lokalizáció érdekében hogyan kell a három m-utat (azaz T_1-et, T_2-t és T_3-at) kihúzni a hálózatban. A T_j m-út a mátrix j-edik oszlopának felel meg, azaz minden linken át kell haladnia, melynek a j-edik bitpozíciójában 1 található, és nem haladhat át egyetlen olyan linken sem, melynek a j-edik pozíciója 0. Az m-utak állapotának ismeretében (0- működik, 1- megszakadt) bármely linkhiba egyértelműen lokalizálható. Például kizárólag a T_1 fényút elsötétedése esetén a hálózatmenedzser a $(3,0)$ link hibát azonosítja.

Ahhoz, hogy a 0 pont egyértelműen lokalizálni tudja valamennyi hibát, ismernie kell a T_3 m-út állapotát, ami csak jelzésüzeneteken keresztül lehetséges. Elosztott link-hiba monitorozó megoldást kapunk, ha a 1(c) ábrán látható T_4 m-úttal egészítjük ki a rendszert. Ekkor például a 0 pont az 1(d) ábrán látható hibakód táblája segítségével jelzésüzenetek nélkül tudja azonosítani a hibát.

1. Tézis. *Központosított link-hiba lokalizálás (UFL)*

1.1. Tézis. *Polinomidőben felépíthető* $b = 4 + \lceil \log_2(|E|+1) \rceil$ *közel optimális* ***m-út*** *konstrukciót adtam UFL-hez legalább 6 pontú teljes gráfokra [C1, J1, Disszertáció 3. tétele].*

A bizonyítás azon a felismerésen alapul, hogy bár kisméretű példákon csak kevés, de nagy és erősen összefüggő gráfokon már sok optimális megoldás létezik.

1.2. Tézis. *Polinomidőben felépíthető* $b = \lceil \log_2(|E|+1) \rceil$ *optimális* ***bm-út*** *konstrukciót adtam UFL-hez* $2 \cdot \lceil \log_2(|E|+1) \rceil$ *összefüggő gráfokra [J2, Disszertáció 4. tétele].*

A módszer alkalmazható legalább 18 pontú teljes gráfra. Korábban a legjobb konstrukció $\approx 2\lceil \log_2 |E| \rceil$ bm-utat használt [1].

1.3. Tézis. *Polinomidőben felépíthető $b = 3+\lceil \log_2 (|E|+1) \rceil$ közel optimális bm-utat használó megoldást adtam négyzetrácsra UFL-hez [C2, J2, Disszertáció 5. és 6. tétele].*

Korábban a legjobb konstrukció $\approx 3\lceil \log_2 |E| \rceil$ bm-útat használt [1]. A konstrukció alkalmas a heurisztikus algoritmusok tesztelésére [C2, J2]. A bizonyítás kombinatorikus és algebrai technikákon alapul.

Egy n pontú cirkuláns gráf pontjai legyenek $V = \{v_0, v_1, \ldots, v_{n-1}\}$, ekkor a v_j pont szomszédos $[v_{j+1} \mod n]$ és $[v_{j+2} \mod n]$ pontokkal.

1.4. Tézis. *Polinomidőben felépíthető $b = \lceil \log_2 (|E|+1) \rceil$ optimális bm-utat használó megoldást adtam cirkuláns $C_{1,2}$ gráfokra UFL-hez, amely egyben közel optimális NL-UFL megoldás is [J3, Disszertáció 7. és 11. tételei és 3.3.8 fejezete].*

Felismertem, hogy a gerinchálózati topológiákon jó eséllyel létezik közel optimális m-út megoldás. Ilyen esetben az m-utak a hálózat méretéhez képest viszonylag hosszúak lesznek. Ezt kihasználva egy új heurisztikus módszert javasoltam. A módszer alapötlete, hogy kezdetben véletlen hibakódokat rendel az élekhez, majd a hibakódokat az élek között mohó cserélgetések során m-út megoldássá formálja.

1.5. Tézis. *Az RCA-RCS nevű heurisztikus módszert javasoltam m-utak kialakítására UFL-hez. A gyakorlatban 1000-10000-szer gyorsabbnak bizonyult a korábbi módszereknél [C1, J1]. (Részletek a Disszertáció 2.2.8 fejezetében találhatók.)*

Azóta több hasonló módszert is publikáltak, de ezek lényegesen hosszabb idő alatt tudnak esetenként jobb megoldást számolni (lásd Disszertáció 2.9 ábrája). A módszer gyorsaságának köszönhetően több mint 5000 hálózati topológián végeztem vizsgálatokat. (Lásd még a disszertáció 2.15 és 2.16 ábráit.)

1.6. Tézis. *A CGT-GCS nevű heurisztikus módszert javasoltam többszörös link-hiba monitorozásra, amely kombinatorikus csoporttesztelésnél alkalmazott kódokat rendel a gráf éleihez. Bizonyítottam, hogy az aktuálisan legjobb kódcsere megkereshető $O(|E|^2 \log |E|)$ lépésben [J4, Disszertáció 2.3.2 fejezete].*

A problémára más, hasonló hatékonyságú módszerek továbbra sem ismertek.

2. Tézis. *Elosztott link-hiba lokalizáció (NL-UFL) és helyreállítás*

2.1. Tézis. *Alsó korlátokat adtam tetszőleges gráfokra NL-UFL eléréshez az m-utak éleinek számára. Ritka gráfok esetére*

$$\|\mathcal{T}\| \geq \xi |V| \log_2 (|E| + 1),$$

ahol ξ a gráftól függő paraméter [J3]. (Részletek a Disszertáció 9 tételében találhatók.) Sűrű gráfok esetére [J3, Disszertáció 12. tétele]

$$\|\mathcal{T}\| \geq 2|E| \left(1 - \frac{1}{|V|}\right).$$

A vizsgált 50 csomópontos, hatnál kisebb átlagos fokszámú véletlen gráfokban $0,85 < \xi < 0,95$ volt. A következő tézisben élesítettem a korláton ritka gráfokra közel $\xi \approx 1,0$-ra [C3, Disszertáció 11. tétele]. A tételt általánosabb esetre kombinatorikus csoporttesztelési feladatra mondom ki. Az általános csoporttesztelési feladatban a tesztek költsége függjön a tesztek méretétől. Jelölje m az elemek számát és $\omega(t)$ a t méretű teszt költségét, ahol ω teljesítse a következő három feltételt: $\omega(1) = 1$, $\omega(t+1) \geq \omega(t)$ és $\frac{\omega(t)}{t} \geq \frac{\omega(t+1)}{t+1}$ ha $1 \leq t < m$.

2.2. Tézis. *Legyen $T_1, \ldots, T_b$ csoporttesztek halmaza amellyel m elemből egyszeres hibát tudunk azonosítani. Bizonyítottam, hogy a tesztek összköltsége*

$$\sum_{i=1}^{b} \omega(|T_i|) \geq \min_{1 \leq x \leq \frac{m}{2}} \omega(x) \left(\log_2 x + \frac{m}{x} - 1\right).$$

[C3, Disszertáció 10. tétele]

2.3. Tézis. *Polinomidőben felépíthető optimális és közel optimális NL-UFL konstrukciókat adtam vonal, teljes és csillag gráf esetére [J3, Disszertáció 13.,14. és 15. tétele].*

Az 1.4 és 2.3 tézisek konstrukciói alapján feszítőfa formájú bm-út megoldásokat célszerű választani.

2.4. Tézis. *Az RSTA-GLS keresztelt heurisztikus módszert javasoltam, amely feszítő fa formájú bm-utakat keres. A gyakorlatban 2-3-szor jobb megoldást képes elérni a többi ismert módszernél [J3, Disszertáció 3.4-es fejezete].*

Közel 1000 véletlen, síkba rajzolható gráfon végzett vizsgálatomban a megoldások a legjobb alsó korláttól átlagosan $\approx 9.70\%$-ra voltak.

Vizsgáltam továbbá, hogy hogyan integrálhatók az elosztott hibalokalizációs módszerek megosztott védelemmel vagy helyreállítással. Az integrálhatóság alapkérdése, hogy az m-utak a hálózat hibamenetes működésekor a védelmi kapacitást milyen mértékben használhatják. A védelmi kapacitás a forgalom méretétől függ, míg a monitorozó kapacitás a topológiától. Jelölje θ a forgalom mértékét, ami a forgalmi igények száma az összes létező pontpárhoz képest.

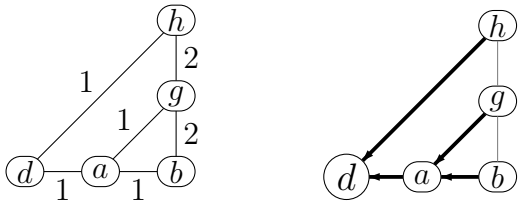
2.5. Tézis. *Bizonyítottam, hogy tetszőlegesen kicsi θ estén létezik olyan hálózat forgalommal, ahol az m-utak átlagos erőforrásigénye kisebb a védelmi kapacitásnál [C3, Disszertáció 16. tétele].*

Szimulációkkal rámutattam, hogy a gyakorlatban a védelmi kapacitás tipikusan elegendő az m-utak számára.

4.2. Gyors IP hiba-helyreállítás

A módszer két megvalósítását vizsgáltam, az LFA-t és a PR-t. Az 2(a) ábrán egy példahálózat található. Ha b-ből d-be szeretnénk csomagokat továbbítani, akkor az elsődleges továbbítási pont (PNH) az a csomópont lesz. Ha megszakad az összeköttetés a b és a pontok között, akkor b-nek keresnie kell egy olyan alternatív szomszédot, amely képes eljuttatni a d-nek címzett csomagokat egy olyan útvonalon keresztül, amely a (b, a) linket nem tartalmazza. Ellenkező esetben csomagtovábbítási végtelen-hurok alakulna ki. Ha példánkban az (a, e) link meghibásodása esetén a csomópont g szomszéd felé irányítja a d-be menő forgalmat, akkor biztosak lehetünk benne, hogy nem alakul ki hurok.

Egy d-be címzett csomag valamennyi lehetséges útvonala a topológia gráf egy részgráfja, amit $R_d = (V, E_d)$ jelöljük. R_d irányított körmentes gráf (DAG) lesz aminek egy nyelője van: a d pont. LFA esetén további megkötés, hogy az élekhez költséget rendeltek, és R_d a d pontba vezető legrövidebb utak DAG-ja. Egy tetszőleges s pontot védettnek tekintünk d felé, ha minden $(s, n) \in R_d$ élre létezik egy olyan $(s, k) \neq (s, n)$ él úgy, hogy R_d-ben k-ból nem vezet út s-be. Az (s, n) élet Primary Next Hop-nak, míg (s, k)-t Secondary Next Hop-nak (SNH) hívjuk. Jelölje $\eta(G)$



(a) LFA esetén az élköltségek (b) R_d routing

2. ábra. Gyors IP hiba-helyreállítás. A (b) ábra a d-be címzett csomag valamennyi lehetséges útvonalát mutatja, d-be a kivételével minden pont védett.

a topológiában az LFA védettség mértékét, ami a következő:

$$\eta(G) = \frac{\text{védett } (s,d) \text{ pontpárok száma}}{\text{összes } (s,d) \text{ pontpár}}.$$

Ha $\eta(G) = 1$ akkor a hálózatot teljesen védettnek hívjuk.

3. Tézis. *IP helyreállítás vizsgálata*

3.1. Tézis. *A védettség mértékere a következő korlátokat adtam* $|V| \geq 2$ *esetére:*

$$\eta(G) \leq \frac{|V|}{|V|-1}(\Delta - 2) + \frac{2}{|V|-1} \ ,$$

ahol Δ *az átlagos csomópont fokszámot jelöli, és*

$$\eta(G) \geq \frac{|V|}{|V|-1}\frac{\frac{\Delta}{2}-1}{\Delta_{\max}-1} + \frac{1}{(|V|-1)(\Delta_{\max}-1)} \ ,$$

ahol $\Delta_{\max}$ *a maximális csomópont fokszámot jelöli [C4, J5, Disszertáció 17. és 18. tétele].*

A két tétel ritka gráfokra ad jó korlátokat. Vizsgáltam, hogy hogyan lehet az LFA módszer hatékonyságát növelni, ha lehetőségünk van új linkek hozzáadására. A következő két algoritmikus problémát elemeztem.

Adott $G(V,E)$ irányítatlan gráf egységnyi élköltségekkel és adott k egész szám esetén létezik-e $F \subseteq \overline{E}$ komplemens élhalmaz úgy, hogy $|F| \leq k$ és $\eta(G(V, E \cup F)) = 1$, azaz a gráfhoz F-et egységnyi élköltséggel hozzáadva teljes védettséget kapunk.

Adott $G(V,E)$ súlyozott irányítatlan gráf és adott k egész szám esetén létezik-e $F \subseteq \overline{E}$ komplemens élhalmaz és megfelelő élköltségek úgy, hogy $|F| \leq k$, $\eta(G(V, E \cup F)) = 1$, és a legrövidebb utak a $G(V,E)$ és a $G(V, E \cup F)$ gráfban egybeesnek.

3.2. Tézis. *Megmutattam, hogy az Loop Free Alternate (LFA) topológia bővítés probléma NP-nehéz, egységnyi és általános költségfüggvény esetére is [C5, Disszertáció 19. és 20. tétele].*

A bizonyítások a minimális halmazfedési feladatra vezetik vissza a problémákat. Olyan transzformációkat tartalmaznak, amik visszafelé is igazak. Így a minimális halmazfedésnél alkalmazott heurisztikák az LFA topológia bővítés problémára is alkalmazhatók, sőt a gyakorlatban is hatékonyan működnek [C5, J6].

Protection Routing esetén az élköltségek nem játszanak szerepet az R_d meghatározásában. Kwong, et al. [2] sejtéseket fogalmazott meg arra vonatkozóan, hogy milyen gráf topológiákon létezik teljes védettség. Az utolsó altézis erre add részben választ. Két feszítőfa pontfüggetlen, ha tetszőleges két pont között a két fában vezető út pontfüggetlen [3].

3.3. Tézis. *A G gráf teljesen védhető Protection Routing módszerrel, ha található benne két pontfüggetlen feszítőfa [J7, Disszertáció 23. tétele].*

5. Eredményeim hasznosíthatósága és hatása

A kutatásom során a következő két kérdéskör megválaszolásával foglalkozom:

(1) Hogyan lehet optikai gerinchálózatokban gyorsan azonosítani a meghibásodott elemeket monitorozó utak segítségével? Hogyan lehet egy monitorozó rendszert hatékonyan üzemeltetni kiszolgálva a helyreállítás igényeit? A témában született cikkeim a legkiválóbb folyóiratokban és konferenciákon jelentek meg (IEEE INFOCOM [C1, C2], IEEE Trans. on Networking [J1, J8, J3], és IEEE/OSA Journal of Lightwave Technology [J4], IEEE RNDM'11 keynote előadás), és egy részük tananyagként is szerepelt külföldi egyetem PhD kurzusán.

(2) Hogyan lehet az LFA IPFRR módszer hatékonyságát növelni, ha lehetőségünk van új linkek hozzáadására? A témán a magyarországi Ericsson kutatócsoporttal közösen dolgoztunk, amiből egy hálózattervező szoftver is készült. A témában született két IEEE INFOCOM'11 [C5, C6] cikkre két Internet szabvány is hivatkozik (IETF draft [4, 5]). A IEEE DRCN'11 [C4] megjelent munkánkat a konferencia legjobb cikkének választották.

A témákban végzett munkámnak köszönhetően 2012-ben az MTA Lendület kiválósági program keretében kutatócsoportot alapíthattam.

A tézisek témájában megjelent közlemények

Folyóirat cikkek

[J1] J. Tapolcai, P.-H. Ho, B. Wu, and L. Rónyai, „A novel approach for failure localization in all-optical mesh networks," IEEE/ACM Transactions on Networking, vol. 19, pp. 275–285, 2011.

[J2] J. Tapolcai, L. Rónyai, and P.-H. Ho, „Link fault localization using bi-directional m-trails in all-optical mesh networks," IEEE Transactions on Communications, 2012.

[J3] J. Tapolcai, P.-H. Ho, L. Rónyai, and B. Wu, „Network-wide local unambiguous failure localization (NWL-UFL) via monitoring trails," IEEE/ACM Transactions on Networking, 2012.

[J4] J. Tapolcai, P.-H. Ho, L. Rónyai, P. Babarczi, and B. Wu, „Failure localization for shared risk link groups in all-optical mesh networks using monitoring trails," IEEE/OSA Journal of Lightwave Technology, vol. 29, no. 10, pp. 1597–1606, 2011.

[J5] L.Csikor, G. Rétvári, and J. Tapolcai, „Optimizing IGP link costs for improving IP-level resilience with loop-free alternates," Computer Communications Journal, 2012.

[J6] M. Nagy, J. Tapolcai, and G. Retvari, „Optimization methods for improving ip-level fast protection for local shared risk groups with loop-free alternates," Telecommunication Systems, 2012.

[J7] J. Tapolcai, „Sufficient conditions for protection routing in ip networks," Springer Optimization Letters, 2012.

[J8] P. Babarczi, J. Tapolcai, and P.-H. Ho, „Adjacent link failure localization with monitoring trails in all-optical mesh networks," IEEE/ACM Transactions on Networking, vol. 19, no. 3, pp. 907 – 920, June 2011.

[J9] P.-H. Ho, J. Tapolcai, and H. Mouftah, „On achieving optimal survivable routing for shared protection in survivable next-generation internet," IEEE Transactions on Reliability, vol. 53, no. 2, pp. 216–225, 2004.

[J10] P.-H. Ho, J. Tapolcai, and T. Cinkler, „Segment shared protection in mesh communication networks with bandwidth guaranteed tunnels," IEEE/ACM Transactions on Networking, vol. 12, no. 6, pp. 1105–1118, December 2004.

[J11] J. Tapolcai and P.-H. Ho, „Dynamic survivable routing for shared segment protection," Journal of Communication and Networks (JCN), vol. 9, no. 2, pp. 198–209, 2007.

[J12] P.-H. Ho, J. Tapolcai, and A. Haque, „Spare capacity reprovisioning for shared backup path protection in dynamic generalized multi-protocol label switched networks," IEEE Transactions on Reliability, vol. 57, no. 4, pp. 551–563, Dec. 2008.

[J13] J. Segovia, E. Calle, P. Vila, J. Marzo, and J. Tapolcai, „Topology-focused availability analysis of basic protection schemes in optical transport networks," Journal of Optical Networking, vol. 7, no. 4, pp. 351–364, 2008.

[J14] J. Tapolcai, P.-H. Ho, D. Verchere, T. Cinkler, and A. Haque, „A new shared segment protection method for survivable networks with guaranteed recovery time," IEEE Transactions on Reliability, vol. 57, no. 2, pp. 272–282, 2008.

[J15] P. Cholda, J. Tapolcai, T. Cinkler, K. Wajda, and A. Jajszczyk, „Quality of resilience QoR as a network reliability characterization tool," IEEE Network Magazine, vol. 23, no. 2, pp. 11–19, March/April 2009.

[J16] Q. Guo, P.-H. Ho, H. Yu, J. Tapolcai, and H. Mouftah, „Spare capacity reprovisioning for high availability shared backup path protection connections," Computer Communications, vol. 33, no. 5, pp. 603–611, March 2010.

[J17] B. Lin, P.-H. Ho, L. Xie, X. Shen, and J. Tapolcai, „Optimal relay station placement in broadband wireless access networks," IEEE Transactions on Mobile Computing, vol. 9, no. 2, pp. 259–269, February 2010.

[J18] J. Tapolcai, P.-H. Ho, and H. Yu, „Switching/merging node placement in survivable optical networks with ssp," Computer Communications, vol. 33, pp. 381–389, 2010.

[J19] B. Wu, P.-H. Ho, K. Yeung, J. Tapolcai, and H. Mouftah, „CFP: Cooperative fast protection," IEEE/OSA Journal of Lightwave Technology, vol. 28, no. 7, pp. 1102 –1113, apr. 2010.

[J20] B. Lin, J. Tapolcai, and P.-H. Ho, „Dimensioning and site-planning of integrated pon and wireless cooperative networks for fixed mobile convergence," IEEE Transactions on Vehicular Technology, vol. 60, no. 9, pp. 4528 – 4538, Nov. 2011.

[J21] J. Tapolcai, S.-J. Yang, and P.-H. Ho, „A general availability – aware survivable routing architecture on gmpls-based recovery," Journal of Internet Technology, vol. 12, no. 3, pp. 1–8, 2011.

[J22] B. Wu, P.-H. Ho, K. Yeung, J. Tapolcai, and H. Mouftah, „Optical layer monitoring schemes for fast link failure localization in all-optical networks," IEEE Comm. Surveys & Tutorials, vol. 13, no. 1, pp. 114–125, First Quater 2011.

[J23] C. Zhang, P.-H. Ho, and J. Tapolcai, „On batch verification with group testing for vehicular communications," Wireless Networks, vol. 17, no. 8, pp. 1851–1865, 2011.

[J24] ——, „Survey on out-of-band failure localization in all-optical mesh networks," Telecommunication Systems, vol. 1, 2012.

[J25] ——, „Shared risk link group failure restoration with in-band approximate failure localization," Optical Switching and Networking, 2012.

Könyv és könyvfejezetek

[B1] J. Marzo, T. Stidsen, S. Ruepp, E. Calle, J. Tapolcai, and J. Segovia, Graphs and Algorithms in Communication Networks. Springer, 2009, ch. Network Survivability: End-to-End Recovery Using Local Failure Information, pp. 137–161.

[B2] J. Tapolcai, Routing algorithms in survivable telecommunication networks. LAP Lambert Academic Publishing AG & Co KG, 2010, iSBN 978-3-8383-9297-4.

[B3] P. Babarczi and J. Tapolcai, Resilient Optical Network Design: Advances in Fault-Tolerant Methodologies. Pennsylvania: IGI Global, 2011, ch. Protection Survivability Architectures: Principles and Challenging Issues.

Konferencia cikkek

[C1] J. Tapolcai, B. Wu, and P.-H. Ho, „On monitoring and failure localization in mesh all-optical networks," in Proc. IEEE INFOCOM, Rio de Janero, Brasil, 2009, pp. 1008–1016.

[C2] J. Tapolcai, L. Rónyai, and P.-H. Ho, „Optimal solutions for single fault localization in two dimensional lattice networks," in Proc. IEEE INFOCOM Mini-Symposium, San Diego, CA, USA, 2010.

[C3] J. Tapolcai, P.-H. Ho, P. Babarczi, and L. Rónyai, „On achieving All-Optical failure restoration via monitoring trails," in Proc. IEEE INFOCOM Mini-Symposium, Turin, Italy, USA, Apr. 2013.

[C4] G. Rétvári, L. Csikor, J. Tapolcai, G. Enyedi, and A. Császár, „Optimizing IGP link costs for improving ip-level resilience," in Proc. International Workshop on Design Of Reliable Communication Networks (DRCN), Krakow, Poland, 2011, pp. 62–69.

[C5] G. Rétvári, J. Tapolcai, G. Enyedi, and A. Császár, „IP fast ReRoute: loop free alternates revisited," in Proc. IEEE INFOCOM, Shanghai, P.R. China, 4 2011.

[C6] J. Tapolcai and G. Rétvári, „Router virtualization for improving IP-level resilience," in Proc. IEEE INFOCOM, Turin, Italy, USA, Apr. 2013.

[C7] P. Chołda, K. Wajda, A. Jajszczyk, J. Tapolcai, T. Cinkler, S. Bodamer, D. Colle, and G. Ferraris, „Considerations about service differentiation using a combined qos/qor approach," in Proc. International Workshop on Design Of Reliable Communication Networks (DRCN), 2005.

[C8] J. Tapolcai, P. Fodor, G. Rétvári, M. Maliosz, and T. Cinkler, „Class-based minimum interference routing for traffic engineering

in optical networks," in Proc. Next Generation Internet Networks (EURO-NGI), Rome, Italy, Apr. 2005, pp. 31–38.

[C9] J. Tapolcai, P.-H. Ho, D. Verchere, and T. Cinkler, „A novel shared segment protection method for guaranteed recovery time," in Proc. Broadband Optical Networking Symposium (BroadNets), 2005, pp. 127–136.

[C10] J. Tapolcai, P. Chołda, T. Cinkler, K. Wajda, A. Jajszczyk, A. Autenrieth, S. Bodamer, D. Colle, G. Ferraris, H. Lonsethagen, I.-E. Svinnset, and D. Verchere, „Quality of resilience (QoR): Nobel approach to the multi-service resilience characterization," in Proc. GOSP co-located with BroadNets, 2005, pp. 405–414.

[C11] P.-H. Ho, J. Tapolcai, A. Haque, S. Shen, T. Cinkler, and M. Desroches, „A novel dynamic availability-aware survivable routing architecture with partial restorability," in Proc. Biennial Symposium on Communications, Kingston, Kanada, 2006, pp. 360 – 363.

[C12] J. Tapolcai, P.-H. Ho, and T. Cinkler, „A distributed control framework for shared protection based on tropical semi-rings," in MPLS/GMPLS Workshop, Girona, Spain, 2006.

[C13] J. Tapolcai, D. Máthé, A. Zahemszky, A. Autenrieth, P. Chołda, T. Cinkler, D. Colle, and K. Wajda, „Quantification of resilience for voice-over-ip applications," in Proc. International Symposium on Broadband Access Technologies in Metropolitan Area Networks (ISBAT), Niagara Falls, Canada, 2006.

[C14] J. Tapolcai, P. Chołda, T. Cinkler, K. Wajda, A. Jajszczyk, and D. Verchere, „Quantification of resilience and quality of service," in Proc. IEEE International Conference on Communications (ICC), Istanbul, Turkey, Jun. 2006, pp. 477–482.

[C15] P. Babarczi and J. Tapolcai, „End-to-end service availability guarantee with generalized dedicated protection," in Proc. Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP), Graz, Austria, 2008.

[C16] J. Tapolcai, P. Babarczi, and P.-H. Ho, „Dedicated protection scheme with availability guarantee," in Proc. International

Telecommunication Network Planning Symposium (NETWORKS), Budapest, Hungary, 2008.

[C17] A. Zahemszky, J. Tapolcai, A. Császár, and A. Mihály, „Novel availability metrics for network topologies," in Proc. International Telecommunication Network Planning Symposium (NETWORKS), Budapest, Hungary, 2008, pp. 1–13.

[C18] P. Babarczi, J. Tapolcai, and P.-H. Ho, „Availability-constrained dedicated segment protection in circuit switched mesh networks," in Proc. of the Workshop on Reliable Networks Design and Modeling (RNDM), Saint Petersburg, Russia, Oct. 2009, pp. 1–6.

[C19] B. Wu, P.-H. Ho, K. Yeung, J. Tapolcai, and H. Mouftah, „CFP: Cooperative fast protection," in Proc. IEEE INFOCOM Mini-Symposium, Rio de Janero, Brasil, 2009, pp. 2606–2610.

[C20] P. Babarczi, J. Tapolcai, P.-H. Ho, and B. Wu, „Srlg failure localization in transparent optical mesh networks with monitoring trees and trails," in International Conference on Transparent Optical Networks (ICTON), jun. 2010, pp. 1 –4.

[C21] B. Wu, P.-H. Ho, J. Tapolcai, and X. Jiang, „A novel framework of fast and unambiguous link failure localization via monitoring trails," in Proc. IEEE INFOCOM, Work in Progress Track, 2010.

[C22] B. Wu, P.-H. Ho, J. Tapolcai, and P. Babarczi, „Optimal allocation of monitoring trails for fast SRLG failure localization in All-Optical networks," in Proc. IEEE Global Telecommunications Conference (GLOBECOM), Miami, Florida, USA, 12 2010.

[C23] M. Ali, P.-H. Ho, B. Wu, J. Tapolcai, and B. Shihada, „Monitoring burst (m-burst) - a novel framework of failure localization in all-optical mesh networks," in Proc. International Workshop on Design Of Reliable Communication Networks (DRCN), Krakow, Poland, 2011, pp. 9–16.

[C24] P. Babarczi, J. Tapolcai, and P.-H. Ho, „SRLG failure localization with monitoring trails in all-optical mesh networks," in Proc. International Workshop on Design Of Reliable Communication Networks (DRCN), Krakow, Poland, 2011, pp. 188–195.

[C25] E. Moghaddam, J. Tapolcai, D. Mazroa, and . Hosszu, „Physical impairment of monitoring trails in all optical transparent networks," in Int. Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011.

[C26] W. He, B. Wu, P.-H. Ho, and J. Tapolcai, „Monitoring trail allocation for fast link failure localization without electronic alarm dissemination," in Proc. International Conference on Optical Network Design and Modeling (ONDM), Bologna, Italy, 2 2011.

[C27] Z. Heszberger, J. Tapolcai, A. Gulyás, J. Biro, A. Zahemszky, and P.-H. Ho, „Adaptive bloom filters for multicast addressing," in IEEE Infocom Workshop, High-Speed Networks (HSN), Shanghai, P.R. China, 4 2011, pp. 174–179.

[C28] 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 Proc. International Workshop on Design Of Reliable Communication Networks (DRCN), Krakow, Poland, 2011, pp. 110–117.

[C29] P. Babarczi, J. Tapolcai, P.-H. Ho, and M. Médard, „Optimal dedicated protection approach to shared risk link group failures using network coding," in Proc. IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, 2012.

[C30] H. Overby, G. Biczók, P. Babarczi, and J. Tapolcai, „Cost comparison of 1+1 path protection schemes: A case for coding," in Proc. IEEE International Conference on Communications (ICC), Ottawa, ON, Canada, 2012.

[C31] G. Rétvári, Z. Csernátony, A. Körösi, J. Tapolcai, A. Császár, G. Enyedi, and G. Pongrácz, „Compressing ip forwarding tables for fun and profit," in ACM HotNets, 2012.

[C32] J. Tapolcai, A. Gulyás, Z. Heszberger, J. Biro, P. Babarczi, and D. Trossen, „Stateless multi-stage dissemination of information: Source routing revisited," in IEE Globecom - Next Generation Networking and Internet Symposium, 2012.

[C33] J. Tapolcai, „Failure presumed protection (FPP): Optical recovery with approximate failure localization," in Broadband Communications, Networks, and Systems, ser. Lecture Notes of the Institute for

Computer Sciences, Social Informatics and Telecommunications Engineering. Springer Berlin Heidelberg, 2012, vol. 66, pp. 361–368.

Magyar nyelvű folyóirat cikkek

[F1] J. Szigeti, J. Tapolcai, G. Rétvári, L. Láposi, and T. Cinkler, „Útvonalkijelõlés és forgalomelvezetés több tartományú kapcsolt optikai hálózatokban - routing and traffic by-pass in multidomain optical switched networks," pp. 42–49, 2004, communications - Híradástechnika.

[F2] G. Németh, G. Makrai, and J. Tapolcai, „Multi-homing in IP networks based on geographical clusters," pp. 9–13, 2009, communications - Híradástechnika.

További hivatkozások

[1] N. Harvey, M. Patrascu, Y. Wen, S. Yekhanin, and V. Chan, „Non-Adaptive Fault Diagnosis for All-Optical Networks via Combinatorial Group Testing on Graphs," in IEEE INFOCOM, 2007, pp. 697–705.

[2] K.-W. Kwong, L. Gao, R. Guerin, and Z.-L. Zhang, „On the feasibility and efficacy of protection routing in IP networks," in IEEE INFOCOM, 2010.

[3] T. Hasunuma, „Completely independent spanning trees in the underlying graph of a line digraph," Discrete Mathematics, vol. 234, no. 1-3, pp. 149–157, 2001.

[4] A. Atlas, R. Kebler, M. Konstantynowicz, G. Enyedi, A. Csaszar, R. White, and M. Shand, An Architecture for IP/LDP Fast-Reroute Using Maximally Redundant Trees, Internet-Draft, Standards Track status Std., 2011.

[5] Csaszar, G. Enyedi, J. Tantsura, S. Kini, J. Sucec, and S. Das, IP Fast Re-Route with Fast Notification, Internet-Draft, Standards Track status Std., 2011.