BUDAPESTI MŰSZAKI ÉS GAZDASÁGTUDOMÁNYI EGYETEM
VILLAMOSMÉRNÖKI ÉS INFORMATIKAI KAR
INFORMATIKAI TUDOMÁNYOK DOKTORI ISKOLA

ÚJ HÁLÓZATOPTIMALIZÁLÁSI MÓDSZEREK A GYORS IP ALAPÚ HIBAJAVÍTÁSHOZ

Csikor Levente
okleveles mérnök-informatikus

Tézisfüzet

Tudományos témavezető:

Dr. Rétvári Gábor, Ph.D.
Tudományos Főmunkatárs
Budapest Műszaki és Gazdaságtudományi Egyetem
Távközlési és Médiainformatikai Tanszék
Nagysebességű Hálózatok Laboratórium (HSN Lab)
MTA-BME Jövő Internet Kutatócsoport

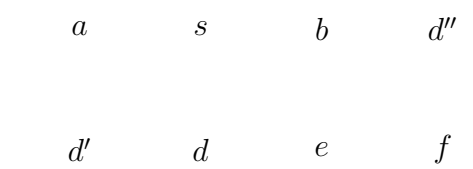
Budapest, Hungary
2015

1. Bevezetés

Napjainkban az Interneten egyre nagyobb teret hódítanak a tradicionális alkalmazások mellett a kereskedelmi távközlési és multimédia szolgáltatások, amik olyan, az eddigiektől merőben különböző és új igényeket támasztó valós idejű alkalmazások megjelenését vonták magukkal, mint például a VoIP, IPTV vagy akár az online játékok. Azonban ez a technológiai konvergencia olyan gyors ütemben zajlik, hogy a jelenlegi Internet eddig nem tudott teljes mértékben lépést tartani vele, és még mindig hiányoznak a kívánt átviteli minőséget garantálni képes komponensek.

Az egyik legfőbb probléma, hogy az Interneten gyakran lépnek fel meghibásodások [18, 10, 28, 32, 22], amiket a jelenleg is használt reaktív technikák [4, 2] csak sok idő után tudnak helyreállítani. Azonban léteznek gyorsabb proaktív védelmi módszerek, melyek egy esetleges hiba után a forgalmat azonnal egy már korábban kiszámított és még rendelkezésre álló elkerülő útvonalakra tudják terelni.

Máig rengeteg javaslat született a probléma megoldására [1, 17, 12, 31, 6, 16], de csak az ún. Loop-Free Alternates (LFA, [3]) módszer az, amely az egyszerűségének köszönhetően nem veszett el a szabványosítás útvesztőjében és elérhető napjaink útvonalválasztóiban. Az LFA esetén amint egy hiba bekövetkezett az elsődleges főútvonalon, a cél pusztán az, hogy legyen egy olyan másik szomszédos csomópont, akinek még van működő útvonala a célcsomópont felé. Sajnos ezen egyszerűségnek van egy hátulütője is, miszerint a módszer nem tudja garantálni a teljes védelmet minden hálózatban, ugyanis egy hiba észlelése után egy ilyen szomszéd csomópont - amely biztosítani tudna egy elkerülő útvonalat, - nem mindig létezik. Példaképpen vegyük szemügyre az 1. ábrát, és tételezzük fel, hogy az s csomópont csomagot szeretne küldeni a d' csomópontnak, de a kapcsolat (továbbiakban *link*) az s és a következő a-val jelölt csomópont (továbbiakban *next-hop*[1]) között meghibásodott. Ebben az esetben az s csomópont nem passzolhatja a csomagot a másik szomszédjának, b-nek, mivel annak a d' felé kiszámított legrövidebb útvonala lehet, hogy pont az s csomóponton halad keresztül, így b a csomagot visszaadva s-nek egy hurkot (*loop*) képezne.



1. ábra. Egy egyszerű hálózati példa, melyben bizonyos meghibásodás sem LFA-val, sem Remote LFA-val nem javítható. A nyilak az legrövidebb útvonalakat mutatják s-ből d'-be, ill. d''-be.

Nemrég, a védelem növelése érdekében megjelent egy általánosított módszer, az ún. Remote Loop-Free Alternates (rLFA, [5]), amely során - az LFA-val ellentétben - nemcsak a közvetlen szomszédok, hanem távolabbi csomópontok is részt vehetnek a hiba elkerülése érdekében. Ez a gyakorlatban úgy valósul meg, hogy a már fentebb említett példánk esetén

[1] A szakirodalom az egy adott útvonalon előforduló következő állomásokat *next-hop* néven említi.

képzeljük el, hogy létezik egy alagút (*tunnel*) az s és az e csomópontok között. Ennek jelentősége abban rejlik, hogy az e csomópont így közvetlen szomszédja lesz s-nek, növelve ezzel annak lokális hibajavítási lehetőségeit. A példahálózatban az e csomópontnak ráadásul a legrövidebb útvonala d' felé nem halad át a meghibásodott (s, a) kapcsolaton, így az e csomópont egy távoli (*remote*) LFA-ja lesz s-nek az (s, a) kapcsolatra és a d' célállomásra nézve.

Ugyan a távolabbi csomópontok használata nagy mértékben javít a legtöbb helyzeten, igénybevételük lehetősége a szimpla LFA-hoz hasonlóan nem mindig garantált. Rengeteg olyan eset van, ahol bizonyos meghibásodások után a hálózat védtelen marad. Vegyük észre, hogy ez a helyzet már a fentebb említett egyszerű hálózat esetén is fenn áll. Tegyük fel, hogy most az s csomópont a d''-nek szeretne csomagot küldeni és véletlenül az (s, b) kapcsolatban meghibásodás lép fel. Ebben az esetben a hiba nem védhető, ugyanis minden lehetséges csomópont - melynek legrövidebb útvonala d'' felé nem megy át a meghibásodott (s, b) kapcsolaton - s-ből csak magán a meghibásodott kapcsolaton keresztül érhető el. Látható tehát, hogy az rLFA ugyan jóval több meghibásodás esetén tud védelmet biztosítani, mint egyszerűbb változata, de használata nem nyújt 100%-os védelmet tetszőleges topológiákban.

2. Kutatási célkitűzések

A disszertáció célja, hogy ezen továbbra is fennálló problémák orvoslására egy átfogó képet és teljesítményelemzést adjon a különböző típusú LFA-kat illetően, és megmutassa, hogy tetszőleges hálózatokban milyen mértékben garantálható a védelem egyszeres link és csomópont meghibásodás esetén. Munkám során tanulmányozom az egyes hálózatok topológiáját, hogy fényt derítsek arra, mi az a gráfelméleti tulajdonság, ami meggátolja vagy éppen lehetővé teszi, hogy az LFA módszer teljes védelmet nyújtson. Továbbá azt is megvizsgálom, hogy egy tetszőleges hálózatban minimális operátori módosításokkal milyen mértékben növelhető az LFA által nyújtott védelem.

A disszertáció első felében különböző hálózatoptimalizálási módszereket vizsgálok meg, melyekkel jelentősen javítható az LFA által biztosított lefedettség. Továbbá tanulmányozom ezen megközelítések bonyolultságát és algoritmusokat javaslok a megoldásuk érdekében. Megmutatom, hogy egyszeres hálózati link hibák esetében az LFA lefedettség akár 100%-osra is növelhető, valamint kitérek a ritkább, de szintén releváns, egyszeres csomópont meghibásodások esetére is.

A disszertáció második felében betekintést nyújtok a kétféle LFA közötti hasonlóságokba és különbségekbe, valamint megmutatom, hogy az egyszerűbb LFA-hoz képest milyen mértékben garantál nagyobb védelmet a nála általánosabb rLFA. Továbbá górcső alá veszem, hogy mik azok a topológiai tulajdonságok, amik jelentősen korlátozzák az rLFA hatékonyságát egy tetszőleges hálózatban. Végül, de nem utolsó sorban szemügyre veszem, hogy függetlenül a meghibásodások típusától, milyen hálózatoptimalizálási módszerek alkalmazásával tehető egy hálózat teljesen védetté.

Úgy gondolom, hogy az eredményeim jelentősen elősegíthetik az LFA módszerek működésének megértését, valamint segíthetnek eddig hezitáló hálózati operátoroknak letenni a voksukat valamely elérhető módszer mellett.

3. Általános feltevések

A disszertációmban olyan módszerek hatékonyságával foglalkozom, melyek célja a hálózati hibák elleni védelem biztosítása egy hálózati doménen belül (*intra-domain*). Ebből adódóan az analizált hálózatokról felteszem, hogy azok autonóm rendszerek, melyekben az összes útvonalválasztónak (*router*) teljes képe van az egész hálózatról. Ez a feltevés magával vonja, hogy a hálózatban egy kapcsolat-állapotú útvonalválasztó algoritmus (*link-state routing*) van hadrendbe állítva, mint például az Open Shortest Path First (OSPF, [24]) vagy az Intermediate System to Intermediate System (IS-IS, [14]). Továbbá azt is feltételezem, hogy a csomópontok az útvonalválasztási döntéseik meghozásában kizárólag a célcsomópont címét veszik figyelembe, és semmilyen egyéb esetleges információ (forrás általi útvonal kijelölés (*source-routing*), addicionális jelzés, stb.) nem kerül számításba. Sőt, minden útvonalválasztó minden egyes célcím esetén kizárólag egy lehetséges útvonalhoz szükséges információt tart számon, azaz ha több legrövidebb útvonal is létezik két pont között (Equal Cost Multiple Paths), akkor azok közül egy van kiválasztva kizárólagosan. Ez leginkább egy technikai feltételezés, hogy a problémát matematikailag könnyebben lehessen kezelni, ugyanakkor ha szükséges könnyedén lehet ezen enyhíteni.

Útvonalválasztási szempontból továbbá felteszem, hogy a hibák elleni védelemnek nem kell az autonóm rendszeren kívülre kiterjedni, mivel azon hibákat a domének közötti (*inter-domain*) útvonalválasztó protokolloknak (pl. Border Gateway Protocol), illetve a másik doménen belüli protokollnak kell megoldania. Mivel a BGP protokoll útvonalválasztása nem pusztán a legrövidebb útvonalak alapján történik, így ebben a disszertációban a domének közötti meghibásodásokkal nem foglalkozom.

Mivel a legtöbb esetben a meghibásodás tranziens és egy linket vagy csomópontot érint egy időben [21, 13], kizárólag *egyszeres link és csomópont* meghibásodásokkal foglalkozom. Itt megjegyezném, hogy a csomópont hibák esetén különös tekintettel kell eljárni abban az esetben, ha a célcsomópont maga a meghibásodott elem[2](például az 1 .ábrán látható hálózatban (b, d'') forrás-célcsomópont pár esetén) Ilyen esetekben nyilván nincs mód a hiba megkerülésére. A teljes védelem növelése érdekében az ilyen esetekben használatos módszer az, hogy a két csomópontot, mint forrás-cél párt akkor tekintjük védettnek, ha kizárólag a link meghibásodását tudjuk védeni [19]. Mindazonáltal, forgalmi megfontolásokat figyelembe véve (*traffic engineering*) ez nem mindig a legjobb módszer, ugyanis az érintett forgalom nagy eséllyel feltorlódott tartalék linkekre kerülhet növelve ezzel a csomagvesztés valószínűségét. Ebből adódóan nincsen egy mindenki által elfogadott és javallott megközelítés, hogy ilyen esetekben hogyan kell eljárni. A disszertációmban mindkét eshetőséget figyelembe veszem: az LFA-t illető vizsgálat során az ilyen forrás-célcsomópont párok esetén csak a kettejük közötti link védelmét követelem meg, míg Remote LFA-t érintő analízis során az ilyen csomópontok közötti védelmet "nem definiált"-nak tekintem. Megjegyzem, ha bárminemű szignifikáns különbség adódik a két megközelítés között, arra külön felhívom a figyelmet és megvizsgálom.

Továbbá megjegyzendő, hogy többrétegű hálózatok során (*multilayered networks*) több felső rétegbeli (*overlay*) link egy tényleges fizikai linket használ az átvitelre. Nyilván egy

[2]Ezt a problémát a szakirodalom *last-hop* problémaként tartja számon

ilyen fizikai link meghibásodása (pl. a kábel építkezés során történő elszakítása) több virtuális link meghibásodását vonja maga után. Az ilyen jellegű hibák kezelésével a disszertációmban nem foglalkozom.

Gráfelméleti szempontból felteszem továbbá, hogy a hálózat egy egyszerű, irányítatlan, súlyozott gráf, ahol pont-pont linkek kötik össze a csomópontokat és azok kétirányúak, azaz közös kockázatú csoportok (Shared Risk Link Group (SRLG)) valamint kisebb helyi hálózatok (Local Area Network (LAN)) nincsenek a hálózatban. Ami a linkeket illeti, azok élköltségeit szimmetrikusnak feltételezem, azaz ezen adminisztrációs költség mindkét irányba ugyanakkora értéket vesz fel. Mindazonáltal, a Remote LFA vizsgálataim során azzal az egyszerűsítéssel élek, hogy az élköltségek egységek, azaz a utak hosszát két csomópont között az útvonalon lévő csomópontok száma határozza meg. Az ilyen súlyozatlan gráfok sok szempontból bizonyulnak előnyösnek; például manapság még mindig vannak olyan valós hálózatok melyekre ez fennáll, sőt, mint később látni fogjuk ezen feltételezéssel élve az LFA-val kapcsolatos eredmények általánosíthatóak Remote LFA-ra.

Mivel egy tetszőleges link csak akkor védhető elkerülő technikával, ha a hálózatot reprezentáló gráf kétszeresen él-összefüggő, így ezen topológiai tulajdonságot szintén elvártnak tekintem a link hibák esetén. Hasonlóképpen a csomópont meghibásodások esetén feltételezem, hogy a gráf kétszeresen pont-összefüggő. Az összefüggőség azért játszik fontos szerepet, mert ha egy esetleges hiba folytán a hálózat két diszjunkt részre esik szét, akkor nincs az a módszer, ami kiküszöbölné a problémát.

4. Módszertan

Az általános feltevésekkel összhangban egy hálózatot mindig egy *egyszerű, irányítatlan, súlyozott* $G(V, E)$ gráffal modelleztem, ahol a V a csomópontok halmazát, míg az E az azok között futó élek halmazát jelöli. Legyen $n = |V|$ és $m = |E|$, valamint a komplemens élek halmazát jelölje $\overline{E}$. Egy adott élt az (i, j) jelöl, ahol i és j csomópontok V-ből valók. Az élek költségeit egy $c : E \mapsto N$ költségfüggvény reprezentálja. Egy (i, j) él költségének jelölésére $c(i, j)$ szolgál. Ahhoz, hogy leírjuk két tetszőleges (u, v) csomópontpár között a legrövidebb utat, a $\text{dist}(u, v)$ jelölést használom. Mivel az élek kétirányúak és szimmetrikusak, ezért $\text{dist}(u, v) = \text{dist}(v, u)$.

A modellemben mindig gráfelmelétei *alsó és felső korlátokat* kerestem a különböző védelmi mechanizmusok teljesítményét illetően. Ezen tanulmányozásokat mind mesterséges, mind valós hálózati topológiákon végeztem. Az előbbi esetben közismert telekommunikációs (pl. kör, gyűrű) és gráfelméleti (pl. páros gráf, Möbius szalag) topológiákat generáltam. Másrészt, rengeteg valós szolgáltatói hálózati topológia érhető el ingyenesen az interneten. Ilyenek a Rocektfuel [20], SNDLib [29], vagy akár a Topology Zoo [15].

Mindig nagy figyelmet szenteltem arra, hogy a vizsgált hálózatok több tulajdonságban is eltérjenek egymástól (pl. méret, sűrűség, fokszámeloszlás, összefüggőség). Miután felfedeztem, hogy egy tetszőleges hálózatban a hibák elleni védelem rendkívül alacsony is lehet, azt tűztem ki célul, hogy találjak olyan *hálózatoptimalizálási módsze-reket*, melyek segítségével ezt növelhetem. Ezekben az esetekben a célom pusztán a hibák elleni lefedettség növelése volt, így nem vettem figyelembe egyéb szempontokat is, mint pl. a terhelés elosztás, vagy akár az esetleges torlódás, ami a forgalom kerülőútra terelése során léphet fel. Az elméleti

tételeimet, téziseimet matematikailag is bebizonyítottam. Általánosságban kijelenthető, hogy a problémák többsége bonyolultságát tekintve NP-teljes volt, így a megoldásukhoz egzakt algoritmusokat (egészértékű lineáris programokat (ILP)) fogalmaztam meg. A legtöbb esetben, közelítő heurisztikákat dolgoztam ki, hogy elfogadható eredményeket kapjak rövidebb időn belül. Az utóbbi esetben, elsőképp *mohó algoritmusok* kidolgozásával foglalkoztam, majd *szimulált lehűtésen alapuló heurisztikák egy teljes családját* dolgoztam ki *rengeteg állítható paraméterrel*, hogy elősegítsem a lokális optimumok elkerülését, melyek előfordulhatnak a mohó megközelítés esetén. Mindazonáltal, mint látni fogjuk, a mohó algoritmus több esetben is jobb eredményeket produkált mint a szimulált lehűtésen alapuló algoritmusok.

Végül, de nem utolsó sorban, a szimulációs eszköztáramat nagymértékben C++/ LEMON[3] nyelven implementáltam, és az eredményeket különböző BASH[4] szkriptek segítségével állítottam elő. Néhány esetben a hálózatok Geographic Markup Language (GML) leírónyelven voltak elérhetőek, így ezek LEMON segítségével történő analizálásához egy saját alkalmazást fejlesztettem, melyet GML2LGF converter-nek neveztem el [9].

[3]LEMON mozaikszó a Library for Efficient Modeling and Optimization in Networks rövidítése. Ez egy C++ sablon könyvtár, melyben hatékonyan vannak implementálva gráfok kezeléséhez szolgáló adatstruktúrák és algoritmusok különös tekintettel a kombinatorikus optimalizálás lehetőségére (http://lemon.cs.elte.hu/trac/lemon accessed in October 2013).

[4]Bourne Again SHell - klasszikus parancssori interfész a Unix/Linux rendszerekkel való interakcióra.

5. Új eredmények

5.1. Loop-Free Alternates módszer

Ahogy az előző fejezetben röviden bemutatásra került, az LFA módszer alkalmazása során ha egy hálózati meghibásodás bekövetkezik, a szomszédos router megpróbálja egy olyan - még elérhető - szomszédjának küldeni a csomagot, akinek még van működő útvonala a címzetthez.

Ebben a fejezetben egy ilyen szomszéd (LFA) létezéséhez szükséges feltételeket fogalmazom meg formálisan. Vegyük példaképpen az 1. ábrán látható hálózatot és ismét tegyük fel, hogy az s csomópont szeretne csomagot küldeni d-nek, azonban az a next-hop a hozzávezető link meghibásodása miatt nem elérhető. Ebben az esetben s-nek kell egy alternatív szomszédot keresni, aki nem adja vissza a csomagot, azaz egy alternatív next-hopként léphet elő. Szerencsére a b csomópont eleget tesz ennek a feltételnek, így s nyugodt szívvel adhatja neki a d-nek címzett csomagjait. Ebben az esetben az mondjuk, hogy a b csomópont egy kapcsolati meghibásodást védő (továbbiakban *link-protecting*) LFA az (s, d) forrás-célpár számára.

1. Definíció. *Adott egy összefüggő $G(V, E)$ gráf, egy s forrás és egy d cél. Legyen az s forrás d felé vezető alapértelmezett next-hopja e. Ekkor s-nek egy n szomszédja link-protecting LFA a d célállomásra nézve, ha*

(i) $n \neq e$, *and*

(ii) *a hurokmentességi (loop-free) feltétel teljesül:*

$$\mathrm{dist}(n, d) < \mathrm{dist}(n, s) + \mathrm{dist}(s, d) \ . \tag{1}$$

A fenti feltétel könnyen ellenőrizhető, ugyanis ha a távolság az n szomszédtól a d felé szigorúan kisebb, mint a távolság n-től vissza s-ig, majd onnan d-ig, az pont azt jelenti, hogy az n csomópont nem fogja visszapasszolni a csomagot s-nek, hiszen a d cél felé n-nek nem s az alapértelmezett next-hopja.

A kapcsolati meghibásodások elleni védelemhez hasonlóan a csomópont meghibáso-dások ellen védő (továbbiakban *node-protecting*) LFA esetén is megfogalmazhatóak a feltételek.

2. Definíció. *Adott egy s forrás, egy d cél és legyen az s forrás d felé vezető alap-értelmezett next-hopja e. Ekkor s-nek egy n szomszédja node-protecting LFA a d célállomásra nézve, ha az 1. Definíció* (i) *és* (ii) *feltételén felül teljesül, hogy*

$$\mathrm{dist}(n, d) < \mathrm{dist}(n, e) + \mathrm{dist}(e, d) \ . \tag{2}$$

5.2. LFA lefedettség növelése a hálózati linkek költségeinek optimalizálásával

Ahogy azt a bevezetésben láthattuk, vannak olyan esetek, amikor egy link vagy csomópont meghibásodását sem LFA-val, sem rLFA-val nem tudunk védeni topológiai adottságokból kifolyólag. Egyből adódik a kérdés, hogy vajon akkor magának a hálózati topológiának a finomhangolásával van-e mód az LFA által nyújtott védelem növelésére. Erre több megközelítés is lehetséges. Az egyik az ún. *LFA Network Design*, melynek célja, hogy a védeni kívánt hálózatot már az elejétől kezdve úgy tervezzük meg, hogy azon biztosított legyen a 100%-os LFA lefedettség [11]. Egy másik megközelítés az ún. *LFA Graph Extension*, mely során megpróbáljuk a hálózatunkat minimális számú új él hozzáadásával kiterjeszteni úgy, hogy eddig nem védett meghibásodások esetére alternatív tartalék útvonalak "jöjjenek létre" [25, 27]. Lehetőség van arra is, hogy az élköltségek optimalizálásával úgy állítjuk be a legrövidebb utakat, hogy tetszőleges elem meghibásodása során biztosan létezzen legalább egy LFA. Ezt a megközelítést *LFA Cost Optimization*-nek nevezzük [30, 23, 26, 8]. Ugyanakkor jó megközelítés az is, ha az előbb említett két módszert kombináljuk és ezzel egy hibrid megoldást javasolunk, azaz új éleket is hozzáveszünk a hálózathoz és az élek költségeit is optimalizáljuk. Ezzel az ún. *Combined LFA Network Optimization* módszerrel talán kompenzálható az egyik megközelítésből adódó negatív hatás a másik algoritmussal [7].

Az alábbi fejezetben az LFA Cost Optimization problémakört járom végig, ami mint említettem az élköltségek optimalizálásával igyekszik az LFA általi hibalefedettség növelésére.

A probléma körüljárása során az alábbi eredményeket értem el:

1. Tézis. *Formálisan definiáltam az LFA Cost Optimization problémát. Beláttam, hogy a probléma bonyolultságát tekintve NP-teljes mind a link-protecting, mind a node-protecting esetben. A probléma megoldása érdekében javaslatot tettem közelítő algoritmusok egy teljes családjára. Kiterjedt szimulációs vizsgálatok sorozatával arra a következtetésre jutottam, hogy algoritmusaim a legtöbb valós hálózati topológia esetén legalább* 10*%-os javulást produkáltak az LFA által nyújtott lefedettségen.*

5.2.1. A probléma formalizálása

Formálisan, *LFA Cost Optimization problémát link-protecting esetben* az alábbi módon lehet definiálni:

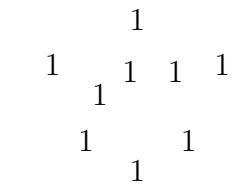
3. Definíció. *LFACostOptLP(G, $\mathcal{S}$): Adott egy $G(V, E)$ gráf és forrás-cél párok egy $\mathcal{S}$ halmaza. Létezik-e egy olyan c élköltség függvény, hogy $\eta_{\mathcal{S}}^{LP}(G, c) = 1$?*

Látható, hogy node-protecting LFA esetén egy LFACostOptNP(G, $\mathcal{S}$) probléma hasonlóképpen definiálható. A továbbiakban, amikor egy adott vizsgálat nem követeli meg a két eset megkülönböztetését, az egyszerűség kedvéért csak LFACostOpt néven fogok a problémára hivatkozni. Sőt, a két probléma kezelése során nem pusztán arra a kérdésre adok választ, hogy létezik-e egy olyan élköltség függvény, mely maximális védelmet nyújt a hálózatban, hanem meg is keresem azt.

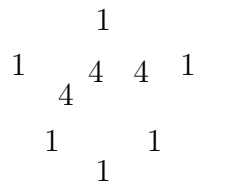
5.2.2. Az élköltségek optimalizálásában rejlő potenciál

A kérdés már az elején felmerül, hogy az élköltségek optimalizálásával vajon mennyire növelhető az LFA által nyújtott védelem. Ugyanis az élköltségek módosítása a legtöbb esetben valószínűleg negatív hatással van a legrövidebb utakra, mivel azokat úgy állították be, hogy a hálózat kihasználtságát maximalizálják. Ahogy azt a következőkben látni fogjuk ezzel a módszerrel akár több, mint 50%-kal is növelhetjük hálózatunk rendelkezésre állását, ami bizonyos esetekben kompenzálhatja a csomagtovábbítási hatékonyságban esetlegesen bekövetkezett "károkat".

1.1. Tézis. *[J2, C1] Tetszőleges k pozitív egész szám esetén létezik egy olyan $4k+2$ csomópontból álló G gráf, melyben két különböző c_1 és c_2 élköltség függvény esetén igaz, hogy $|\eta(G,c_1)-\eta(G,c_2)| \geq \frac{1}{2}$.*



(a) Möbius szalag egység élköltségek esetén



(b) Möbius szalag optimalizált élköltségek esetén

2. ábra. Illusztráció 1.1 tézishez

Példaképpen nézzük meg a 2(a). ábrát, melyen egy ún. Möbius szalag topológia látható egység élköltségekek mellett. Ebben az esetben a link-protecting LFA lefedettség $\eta^{\mathrm{LP}}(G,c) = 0.4$. Ugyanakkor, ha megnézzük a 2(b). ábrán feltüntetett hálózatot, láthatjuk, hogy a különbség csupán annyi, hogy a 3 átlós él költségét 1-ről 4-re változtattuk, ezzel tetszőleges két pont között rövidebb az út ha körbemegyünk a gyűrűn, mintha az átlós élen közlekednénk. Ebben az esetben, mint az könnyen ellenőrizhető, minden forrás-cél pár az egyszeres link meghibásodások esetén védett, azaz $\eta^{\mathrm{LP}}(G,c) = 1$. Sőt, mivel egy esetleges meghibásodás során az LFA-któl a még működő útvonalak pont a legrövidebb utak során nem használt átlós éleken keresztül érhetőek el, csomópont meghibásodások esetén is garantált a teljes védelem, azaz $\eta^{\mathrm{NP}}(G,c) = 1$.

Ez a gráfkonstrukciós eljárás általánosítható tetszőleges $4k+2$ csomópontból álló Möbius szalag topológiára, ahol $k \in \{1,2,3\ldots\}$, és a fenti élköltségek megválasztásával kivétel nélkül mindig elérhető az LFA által nyújtott teljes védelem.

5.2.3. Komplexitás

Tanulmányoztam, hogy link-protecting esetben az LFA Cost Optimization probléma milyen mértékben bonyolult.

1.2. Tézis. *[J2, C1] Bebizonyítottam, hogy az LFACostOptLP(G, $\mathcal{S}$) probléma NP-teljes.*

A bonyolultság közvetlenül abból a tényből fakad, hogy az optimalizálás során megváltoznak a legrövidebb útvonalak, így valószínűsíthető, hogy egy él költségének módosításával ugyan LFA-t tudunk biztosítani egy adott forrás-cél párnak, de egy másik forrás-cél pár esetén viszont megszüntetünk egyet. Sőt, ha egyszerre csak egy célcsomópontot veszünk figyelembe, a probléma komplexitása akkor is NP-teljes. A probléma visszavezethető az ún. Protection Routing problémára (PR, [17]), ahol a feladat az, hogy különböző irányított feszítő DAG-ok (Directed Acyclic Graph, irányított körmentes gráf) segítségével védelmet nyújtsunk az egyszeres csomópont meghibásodások esetén. A probléma bonyolultságáról belátták hogy NP-teljes, én pedig a [C1]-ben megmutattam, hogy az LFACostOptLP(G, $\mathcal{S}$) (Karp)-redukálható a PR problémára felhasználva azt a tényt, hogy egy élköltség függvény egyértelműen meghatároz egy DAG-ot és viszont. Azt a tényt is megfigyeltem, hogy a bizonyítás érvényes marad akkor is, ha a csomópont meghibásodások helyett, "csak" egyszeres link hibákat feltételezünk.

Mivel az említett PR probléma alapvetően csak csomópont meghibásodásokat vesz figyelembe, így az 1.2 tézisben adott állítás a csomópont meghibásodások esetén is érvényes. Ezt az alábbi tézis mondja ki.

1.3. Tézis. *[J2] Megmutattam, hogy az LFA Cost Optimization probléma bonyolultságát tekintve a csomópont meghibásodások esetén is NP-teljes.*

5.2.4. Számszerű kiértékelés

A [J2, C1]-ben egy egzakt algoritmust adtam a probléma megoldására, azonban az a legtöbb esetben nem hozott eredményt véges időn belül. Ezért közelítő algoritmusok kidolgozása mutatkozik az egyetlen járható útnak.

1.4. Tézis. *[J2, C1] Az LFACostOptLP(G, $\mathcal{S}$) probléma orvoslására gyors és hatékony közelítő algoritmusok egy teljes családját dolgoztam ki. Valós és mesterségesen generált topológiákon kiterjedt szimulációs vizsgálatok sorozatával arra a következtetésre jutottam, hogy az LFA általi lefedettség átlagosan legalább* 10*%-kal növelhető valós hálózatok esetén.*

Kidolgoztam heurisztikák egy teljes családját, melyben különböző teljesítményű és a futási idejű algoritmus kapott helyet annak érdekében, hogy egy adott hálózat és az elérni kívánt cél esetén a megfelelő megközelítés könnyen kiválasztható legyen. Kiterjedt szimulációkat végeztem valós hálózatok széles választékán és azt találtam, hogy a számos valós topológián közel teljes LFA lefedettség érhető el az élköltségek optimalizálásával. Továbbá, azt találtam, hogy minél sűrűbb a hálózat, annál nagyobb LFA lefedettség érhető el. Részletesebben, az olyan hálózatok, melyekben az átlagos fokszám nagyobb mint 3, sokkal alkalmasabbak arra, hogy LFA-val relatíve nagy védelmet nyújtsunk, azonban ha az átlagos fokszám kisebb mint 3, akkor az előbbi értelemben vett alkalmasság elenyésző.

Néhány egyszeres link meghibásodásokat figyelembe vevő, valós topológián elért eredményt foglal össze a 1. táblázat, ahol n és m a csomópontok ill. az élek számát jelöli, míg Δ az átlagos fokszámot. Továbbá az $\eta_{LP}(G, c)$ és az $\eta_{LP}(G, c^*)$ reprezentálja a kezdeti ill. az élköltségek optimalizálása során elért link-protecting LFA lefedettséget.

Az eredményeim azt sugallják, hogy az LFA Cost Optimization nagymértékben segítheti egy hálózatban a magasabb rendelkezésre állás biztosítását, főleg ha más módszer, például új

1. táblázat. Néhány, az LFA Cost Optimization algoritmussal, valós hálózatokon elért eredmény.

Topology	n	m	Δ	$\eta_{LP}(G,c)$	$\eta_{LP}(G,c^*)$	$\eta_{NP}(G,c)$	$\eta_{NP}(G,c^*)$
AS1221	7	9	2.57	0.809	0.833	0.452	0.523
AS1239	30	69	4.60	0.873	0.963	0.757	0.937
AS1755	18	33	3.66	0.872	0.993	0.764	0.941
AS3257	27	64	4.74	0.923	1	0.726	0.938
AS3967	21	36	3.42	0.785	0.953	0.642	0.897
AS6461	17	37	4.35	0.933	1	0.738	0.886
Abilene	12	15	2.5	0.56	0.674	0.515	0.606
AT&T	22	38	3.45	0.822	0.987	0.58	0.82
Deltacom	113	161	2.85	0.577	0.662	0.488	0.581
Geant	37	55	2.97	0.69	0.76	0.41	0.622
Germany	17	25	2.94	0.695	0.911	0.562	0.727
InternetMCI	19	33	3.47	0.904	0.932	0.704	0.809
Italy	33	56	3.39	0.784	0.944	0.57	0.803

élek hozzáadása nem lehetséges. Ezenfelül arra is fény derült, hogy a közelítő algoritmusok futási ideje nagymértékben függ a topológiától, azon belül is a csomópontok és élek számától. Néhány esetben az 500 általam futtatott szimuláció pár perc alatt véget ért, míg bizonyos esetekben ez több órát is igénybe vett. Mindazonáltal fontos megjegyezni, hogy a futási idő ebben az esetben nem játszik fontos szerepet, mivel a tervezett LFA Cost Optimization algoritmust csak egyszer kell lefuttatni még mielőtt a hálózatunkat hadrendbe állítjuk.

1.5. Tézis. *[J2] Kiterjesztettem az algoritmikus keretrendszert a csomópont meghibásodások esetére is, és szimulációkkal beláttam, hogy az egyszeres csomópont meghibásodások elleni LFA által nyújtott védelem* 10-20*%-kal megnövelhető.*

Kiterjedt szimulációk segítségével arra a következtetésre jutottam, hogy a csomópont meghibásodások esetére kiterjesztett algoritmusok az LFA lefedettséget $10-20\%$-kal megnövelik. Így az átlagos 60%-os kezdeti lefedettség egészen $75-80\%$-ra növelhető. Hasonlóképpen a link meghibásodások esetéhez néhány, valós topológián elért eredményt foglal össze az 1. táblázat, ahol $\eta_{NP}(G,c)$ jelöli a kezdeti csomópont meghibásodások elleni LFA lefedettséget, míg az $\eta_{NP}(G,c^*)$ mutatja az LFA Cost Optimization után realizáltakat.

5.3. Kombinált optimalizálási módszer az LFA lefedettség növelése érdekében

Eddig az LFA Graph Extension és a fentebb tárgyalt LFA Cost Optimization probléma külön-külön került górcső alá. Azonban adódik a kérdés, hogy bizonyos esetekben nem érné-e meg kombinálni a két módszert, ha az elérni kívánt LFA védettségi szint pusztán az egyik módszerre támaszkodva nem kivitelezhető. Ugyanakkor, egy új fizikai link hozzáadása a hálózathoz - ami által már a kívánt lefedettség el is érhető lenne - nagyon költséges is lehet. Másrészről, ha a lefedettség növelése mellett egyéb forgalmi igényeket, követelményeket is figyelembe kell venni, akkor egy link élköltségének átállításából adódó változások a legrövidebb utakban nem kívánt eredményekhez vezethetnek. Sőt, egy új él hozzáadásából adódó

esetleges változások kompenzálhatóak az élköltségek optimalizálásával. Ezekben az esetekben segítségünkre lehet egy az előző két módszert hatékonyan ötvöző optimalizálási algoritmus. Ezt az módszert Combined LFA Network Optimization-nek neveztem el és ennek elemzése során az alábbi eredményeket értem el.

2. Tézis. *Formálisan definiáltam a Combined LFA Network Optimization problémát. Bebizonyítottam, hogy a probléma bonyolultságát tekintve NP-teljes mind a link-protecting, mind a node-protecting esetben, valamint megmutattam, hogy az LFA Graph Extension és LFA Cost Optimization módszereket milyen módon érdemes kombinálni. Kiterjedt szimulációs vizsgálatok sorozatával arra a következtetésre jutottam, hogy új élek hozzáadása a hálózathoz és az élköltségek együttes optimalizálása hatékony módszer a LFA lefedettség növelése érdekében.*

5.3.1. A probléma formalizálása

A *Combined LFA Network Optimization probléma* az alábbi módon formalizálható:

4. Definíció. *LFACombinedOptLP(G, $\mathcal{S}$, k): Adott egy egyszerű, irányítatlan, súlyozott $G(V, E)$ gráf, forrás-cél párok egy $\mathcal{S}$ halmaza, valamint egy pozitív k egész szám. Létezik-e a komplementer éleknek egy $F \subseteq \overline{E}$ halmaza, ahol $|F| \leq k$ és egy megfelelően választott c élköltség függvény úgy, hogy $\eta_{\mathcal{S}}^{LP}(G(V, E \cup F), c) = 1$?*

A különbség az egyszerűbb LFA Graph Extension problémához képest, hogy ebben az esetben megengedjük az élköltségek és ezzel együtt a legrövidebb útvonalak megváltozását is.

5.3.2. Komplexitás

2.1. Tézis. *[J1] Bebizonyítottam, hogy a Combined LFA Network Optimization probléma bonyolultságát tekintve NP-teljes.*

Az eddig tárgyalt problémák közül, természetéből adódóan a Combined LFA Network Optimization probléma a legbonyolultabb, mivel mindkét részproblémája önmagában is NP-teljes. Ebből adódik, hogy ezen kombinált probléma szintén NP-teljes.

Így optimális megoldások keresése helyett, az részproblémákra adott heurisztikákon alapuló közelítő algoritmusra tettem ajánlatot. Az ajánlott algoritmus működését tekintve minden lépésben végrehajt egy LFA Graph Extension fázist, majd ezt egy LFA Cost Optimization fázis követ. Az első fázisban egy új élet adunk hozzá a hálózathoz, majd a második fázisban már a kiterjesztett hálózaton optimalizáljuk az élköltségeket a legmagasabb LFA lefedettség elérése érdekében. Ez a két fázis ismétlődik egészen addig, amíg a teljes LFA lefedettség nem lesz biztosított.

2.2. Tézis. *[J1] Megmutattam, hogy a kombinált algoritmus nagymértékben csökkenti (átlagosan több mint 50%-kal) a teljes LFA lefedettséghez szükséges addicionális élek számát.*

Eddig a kombinált algoritmus eredményezte a legjobb eredményeket, mely azt jelenti, hogy nagyszámú valós topológián teljes LFA általi védelem érhető el pusztán néhány új él hozzáadásával.

5.4. Remote LFA által nyújtott hibavédelem elemzése

A Remote LFA (rLFA) egy olyan kiterjesztése a szimpla LFA-nak, mely segítségével nagyobb védelem érhető el. Ahogy azt az 1. ábrán láthattuk, ha egy link LFA által nem védhető, akkor a hibát észlelő szomszédos csomópont alagutak segítségével távoli (nem szomszédos) LFA csomópontokat hív segítségül. Fontos megjegyezni, hogy ezen alagutakat csak az elkerülő forgalom használja és alap esetben a normál forgalom útvonalait nem befolyásolja. E cél érdekében többféle alagutazási technikát is használhatunk, de egy MPLS/LDP-vel (Multiprotocol Label Switching-Label Distribution Protocol, többprotokollos címke kapcsolás - címke terjesztő protokoll) támogatott hálózat esetén egy egyszerű "label stack" (címke halom) is használható egy ilyen alagút biztosításához.

Ugyanakkor azt is megfigyelhettük, hogy ugyan az rLFA használata valóban nagyobb védelmet nyújt egyszerűbb megfelelőjéhez (LFA) képest, vannak bizonyos helyzetek, melyek még általa sem védhetőek.

A következőkben megmutatom, hogy egy adott forrás-cél pár mikor védhető Remote LFA által. Link-protecting esetben az útvonalválasztók egy olyan halmaza, melyek a forrástól elérhetőek anélkül, hogy a meghibásodott elemen áthaladjanak, a forrás a hibás link-re vett $P-space$-ének nevezzük (továbbiakban $\mathcal{P}_{\mathrm{LP}}$, ahol $_{\mathrm{LP}}$ a link-protecting esetre utal). Azon útvonalválasztók halmaza, melyeknek a célhoz vezető útvonalaik nem mennek át a hibás elemen a cél hibás link-re vonatkozó $Q-space$-ének nevezzük (továbbiakban $\mathcal{Q}_{\mathrm{LP}}$). Mivel egy forrás csak akkor használ elkerülőútvonalat, ha egy meghibásodást észlelt, így az ilyen értelemben vett alagút végpontjának következő hop-ja (next-hopja) a forrás normál továbbító mechanizmusának nem lehet része. Enne okán az ún. "extended P-space" terminológia is definiálásra került (továbbiakban $\mathcal{P}^{\mathrm{e}}_{\mathrm{LP}}$), mely a forrás szomszédaihoz tartozó P-space halmazok uniója. A forráshoz tartozó $\mathcal{P}_{\mathrm{LP}}$ (vagy $\mathcal{P}^{\mathrm{e}}_{\mathrm{LP}}$), illetve a célhoz tartozó $\mathcal{Q}_{\mathrm{LP}}$ metszete az ún. $\mathrm{PQ}_{\mathrm{LP}}$-pontok halmaza egy adott linkre nézve. Azon pontok, melyek ebbe a halmazba esnek a potenciális Remote LFA jelöltek. Ha a metszet vizsgálata során az extended P-space-t is figyelembe vesszük, akkor a metszetben lévő csomópontokat extended Remote LFA-knak tekintjük.

Node-protecting esetben a fentebb említett terminológiák hasonlóképpen definiálhatóak ($\mathcal{P}_{\mathrm{NP}}$, $\mathcal{P}^{\mathrm{e}}_{\mathrm{NP}}$ $\mathcal{Q}_{\mathrm{NP}}$, $\mathrm{PQ}_{\mathrm{NP}}$-pontok).

A következőkben új eszközöket adok az rLFA által nyújtott lefedettség ($\mu_{\mathrm{LP}}(G)$ és $\mu_{\mathrm{NP}}(G)$) gráfelméleti vizsgálatához, valamint rámutatok egy érdekes kapcsolatra az szimpla LFA és az rLFA között.

3. Tézis. *Analitikusan és numerikusan is elemeztem a Remote LFA által nyújtott védelmet mind link-protecting, mind node-protecting esetben. Egy csomópontpár védettségének definiálásához alternatív szükséges és elégséges feltételeket adtam meg, melyek tetszőleges hálózat esetén fennállnak. Mély kapcsolatot fedeztem fel a szimpla LFA és a Remote LFA között, valamint beláttam, hogy egység élköltségek és extended rLFA esetén tetszőleges hálózatban garantált a teljes védelem az egyszeres link hibák ellen. Ugyanakkor szintén beláttam, hogy ez az eset nem áll fenn ha csomópont meghibásodásokat is védeni szeretnénk.*

5.4.1. Link-protecting eset

Elsőként a P-space és Q-space jelöléseket fogalmaztam meg távolságokban kifejezve hasonlóan ahhoz, ahogy az a szimpla LFA esetén is definiálva volt [3]-ban (lásd 1. és 2. egyenletet). Ez az alábbi alternatív szükséges és elégséges feltételekhez vezet link-protecting rLFA esetén:

3.1. Tézis. *[C2, J3] Adott s forrásra, d célra és e next-hop-ra egy $n \neq s, d$ csomópont link-protecting Remote LFA az $s-d$ párra nézve ($n \in \mathrm{rLFA_{LP}}(s,d)$-vel jelölve) akkor és csak akkor, ha*

$$\mathrm{dist}(s,n) < \mathrm{dist}(s,e) + \mathrm{dist}(e,n) \tag{3}$$

$$\mathrm{dist}(n,d) < \mathrm{dist}(n,s) + \mathrm{dist}(s,d)\ . \tag{4}$$

Könnyen észrevehető, hogy (3) valójában azt állítja, hogy egy s forrás és e next-hop esetén egy ($n \in V$) csomópont $\mathcal{P}_{\mathrm{LP}}(s,e)$-ben van. A (4) pedig azt jelenti, hogy az s forrás és a d cél esetén egy $n \in V$ csomópont $\mathcal{Q}_{\mathrm{LP}}(s,d)$-ben van, így az elkerülő út nem mehet át a hibás linken. Továbbá ezen feltétel pontosan megegyezik a link-protecting LFA hurokmentességi feltételével is.

Másodszor az „extended P-space" jelölést fogalmaztam meg távolságokban kifejezve. Hasonlóan az előbbiekhez, ebben az esetben a következő alternatív szükséges és elégséges feltételhez jutunk link-protecting extended rLFA esetén:

3.2. Tézis. *[C2, J3] Adott s forrásra, d célra és e next-hop-ra egy $n \neq s, d$ csomópont extended link-protecting Remote LFA az $s-d$ párra nézve akkor és csak akkor, ha*

$$\exists v \in \mathit{neigh}(s) : \mathrm{dist}(v,n) < \mathrm{dist}(v,s) + \mathrm{dist}(s,e) + \mathrm{dist}(e,n) \tag{5}$$

$$\mathrm{dist}(n,d) < \mathrm{dist}(n,s) + \mathrm{dist}(s,d)\ . \tag{6}$$

A következőkben rámutatok, hogy mi a kapcsolat a szimpla LFA és a Remote LFA között, azaz megmutatom milyen következmények vonhatóak le, ha valamelyikük létezik.

3.3. Tézis. *[C2, J3] Bebizonyítottam az alábbi ekvivalencia feltételeket a szimpla LFA és az rLFA között mind link-protecting, mind node-protecting esetre:*

- *Egy tetszőleges $u \in \mathrm{rLFA}(s,d)$ csomópont, melyre $u \in \mathrm{neigh}(s) \Rightarrow u \in \mathrm{LFA}(s,d)$, ahol $\mathrm{neigh}(s)$ jelöli azon pontok halmazát, melyek s közvetlen szomszédai.*
- *Egy tetszőleges $u \in \mathrm{rLFA}(s,d)$ csomópont, melyre $u \in \mathrm{neigh}(s) \Leftrightarrow u \in \mathrm{LFA}(s,d)$ feltéve, hogy az élköltségek egységek.*

5.4.2. Node-protecting eset

Hasonlóan a link-protecting esethez, a P-space és Q-space jelöléseket node-protecting esetben is megfogalmaztam távolságokban kifejezve. Ez az alábbi alternatív szükséges és elégséges feltételekhez vezet node-protecting rLFA esetén:

3.4. Tézis. *[J3] Adott s forrásra, d célra és e next-hop-ra egy $n \neq s, d$ csomópont node-protecting Remote LFA az $s-d$ párra nézve ($n \in \mathrm{rLFA}_{\mathrm{LP}}(s,d)$-vel jelölve) akkor és csak akkor, ha*

$$\mathrm{dist}(s,n) < \mathrm{dist}(s,e) + \mathrm{dist}(e,n) \tag{7}$$
$$\mathrm{dist}(n,d) < \mathrm{dist}(n,e) + \mathrm{dist}(e,d) \ . \tag{8}$$

Hasonlóképpen a link-protecting esethez, az (7) valójában azt állítja, hogy egy s forrás és e next-hop esetén egy ($n \in V$) csomópont $\mathcal{P}_{\mathrm{NP}}(s,e)$-ben van. Sőt, az is könnyen észrevehető, hogy a $\mathcal{P}_{\mathrm{NP}}$ feltétel nem változott a link-protecting esetben definiált $\mathcal{P}_{\mathrm{LP}}$-hez képest. Továbbá, a (8) feltétel tulajdonképpen a szimpla node-protecting LFA hurokmentességi feltétele.

Az „extended P-space" jelölést node-protecting esetben szintén megfogalmaztam távolságokban mérve, mely az alábbi alternatív szükséges és elégséges feltételekhez vezet node-protecting extended rLFA esetén:

3.5. Tézis. *[J3] Adott s forrásra, d célra és e next-hop-ra egy $n \neq s, d$ csomópont extended node-protecting Remote LFA az $s-d$ párra nézve akkor és csak akkor, ha*

$$\exists v \in \mathrm{neigh}(s) : \mathrm{dist}(v,n) < \mathrm{dist}(v,e) + \mathrm{dist}(e,n) \tag{9}$$
$$\mathrm{dist}(n,d) < \mathrm{dist}(n,e) + \mathrm{dist}(e,d) \ . \tag{10}$$

Fontos kiemelni, hogy a távolságokban megfogalmazott feltételek a 3.1, 3.2, 3.4, valamint a 3.5 tézisekben igazak tetszőleges élköltségekkel rendelkező hálózatok esetén is.

A következő két tézisben összevetem az rLFA és az extended rLFA által elérhető hibavédelmi lefedettséget.

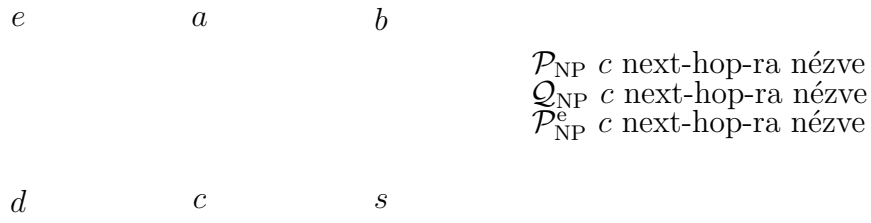
3.6. Tézis. *[C2, J3] Megmutattam, hogy az extended Remote LFA esetén minden egység élköltségű hálózatban biztosított a teljes védelem.*

Egy tetszőleges kétszeresen él-összefüggő, egység élköltségű hálózatban $\mu_{\mathrm{LP}} = 1$ akkor és csak akkor, ha minden $(u,v) \in E$ esetén u-nak van $\mathrm{rLFA}_{\mathrm{LP}}$-je v-hez és viszont. Az összefüggőségből adódóan azt tudjuk, hogy (u,v) egy átlómentes körben van, aminek a hossza legyen k. Ebben az esetben, ha k páratlan, akkor $\mathrm{PQ}_{\mathrm{LP}}$-space halmaz nem üres. Ugyanakkor, ha k páros az azt jelenti, hogy legrosszabb esetben is az extended P-space miatt mindig létezik olyan csomópont mely védelmet nyújthat.

A következőkben megmutatom, hogy a 3.6. tézis nem teljesül ha csomópont meghibásodások esete is fennáll.

3.7. Tézis. *[J3] Megmutattam, hogy általánosságban az extended Remote LFA nem nyújt teljes védelmet a csomópont meghibásodások ellen még kizárólag egység élköltségekkel rendelkező hálózatokban sem.*

Példaképpen vessünk pillantást a 5.4.2. ábrára, ahol a c next-hop meghibásodott miközben s csomagot szeretett volna küldeni d-nek, melyek közötti legrövidebb út a vastag nyíllal van jelölve. A potenciális javítóutak végpontjai a $\mathrm{PQ}_{\mathrm{NP}}$-pontok halmazában van, ami ebben az esetben üres. Sajnos ugyanez az eset áll fenn akkor is, ha $\mathcal{P}^{\mathrm{e}}_{\mathrm{NP}}$ is használható lenne. Ez azt jelenti, hogy vannak olyan hálózatok, amik 100%-osan nem védhetően egyszeres csomópont meghibásodások ellen sem sima, sem extended rLFA esetén sem.



3. ábra. Extended P-space sem tud teljes védelmet nyújtani egyszeres csomópont meghibásodások ellen

5.5. Remote LFA alsó korlátai és hálózat optimalizálási módszerek

Az alábbi alfejezetben visszatérek az egyszerű Remote LFA estére és azt feltételezem, hogy az extended Remote LFA opció nem áll rendelkezésre a hibák javítása érdekében.

Az első célom, hogy gráfelméleti szempontból jellemezzem a Remote LFA lefedettséget. Részletesebben az a célom, hogy azonosítsam egység élköltségű hálózatokban elérhető legalacsonyabb rLFA lefedettséget mind link-protecting, mind node-protecting esetben. Analízisem során adok néhány jól használható módszert, mellyel $\mu(G)$ könnyedén számolható nevezetes gráftopológiák egy széleskörű családjában.

Ahogy azt látni fogjuk, létezik néhány olyan hálózat, amelyben a Remote LFA lefedettség akár nagyon alacsony is lehet. Ebből adódóan a második célom, hogy kialakítsak egy speciális *hálózat optimalizálási* algoritmust, melynek lényege, hogy a hálózatban jól megválasztott addicionális élek hozzáadásával teljes rLFA védettséget biztosítsunk.

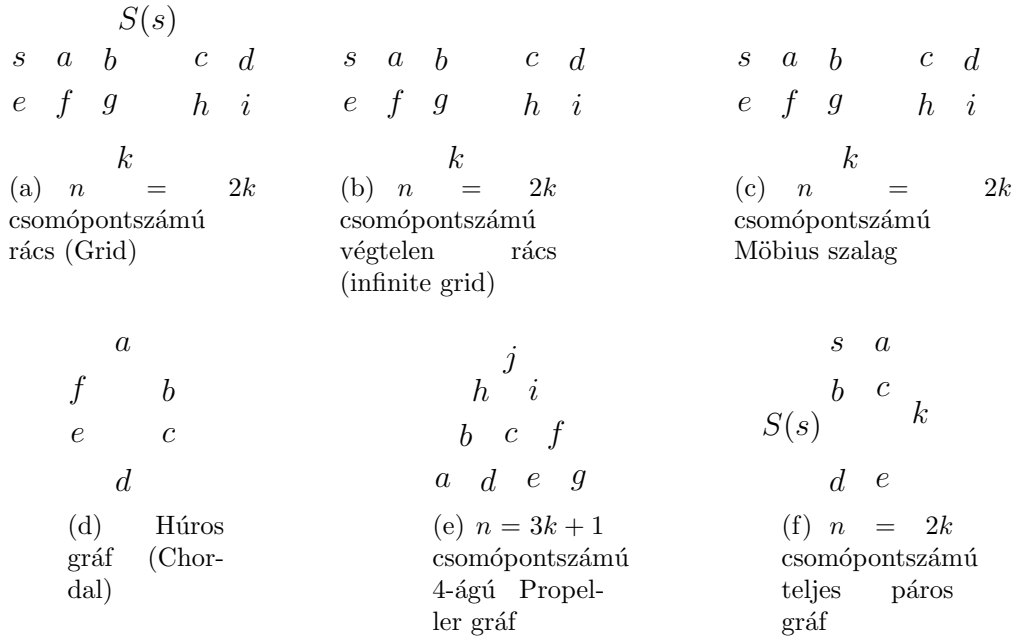
Alsó korlátok keresése a számítástudományban egy örökké visszatérő séma. A mi esetünkben ez egy olyan gráftopológiailag legrosszabb adottságokkal rendelkező hálózat keresését jelenti (*worst-case scenario*), mely rendelkezik olyan kórós tulajdonságokkal, melyeket egy hálózatoptimalizálási fázis során mindenképp célszerű elkerülni. Ennek fényében kiterjesztettem az LFA lefedettséggel kapcsolatos korábbi analíziseket [C2] az rLFA esetére is. Tehát olyan G gráfokat kerestem, melyekre $\mu_{\mathrm{LP}}(G)$ vagy $\mu_{\mathrm{NP}}(G)$ minimális.

4. Tézis. *Úgy találtam, hogy bizonyos egység élköltségekkel rendelkező hálózatokban a Remote LFA módszer a forrás-cél párok csupán* 33*%-ának tud védelmet biztosítani egyszeres link hibák esetén, míg ez az érték egyszeres csomópont meghibásodásokat is figyelembe véve akár* 0*%-ra is csökkenhet. Ajánlatot tettem egy heurisztikus algoritmusra, mely jól közelíti az rLFA Graph Extension probléma megoldását mind egyszeres link hibák, mind egyszeres csomópont hibák ellen. Kiterjedt szimulációs vizsgálatok sorozatával arra a következtetésre jutottam, hogy egyszeres link hibák ellen átlagosan* 3.06 *új él szükséges a teljes rLFA lefedettség elérése végett. Ez az érték egyszeres csomópont meghibásodások esetén* 4.05*, míg extended rLFA esetén* 3.3*.*

5.5.1. Link-protecting eset

Először megmutatom, hogy kétszeresen élösszefüggő hálózatokban milyen alacsony is lehet az rLFA lefedettség, majd folytatom vizsgálataimat kétszeresen pontösszefüggő hálózatokon.

4.1. Tézis. *[C2, J3] Megmutattam, hogy bármely $k \geq 1$ számhoz létezik egy olyan kétszeresen élösszefüggő, $n = 3k + 1$ csomópontszámú G gráf, amire $\mu(G) = \frac{1}{3}$.*



(a) $n = 2k$ csomópontszámú rács (Grid)

(b) $n = 2k$ csomópontszámú végtelen rács (infinite grid)

(c) $n = 2k$ csomópontszámú Möbius szalag

(d) Húros gráf (Chordal)

(e) $n = 3k + 1$ csomópontszámú 4-ágú Propeller gráf

(f) $n = 2k$ csomópontszámú teljes páros gráf

4. ábra. Illusztrációs topológiák

Bizonyításképpen megmutatom, hogy az ún. „4-ágú propeller gráf" (P_k, lásd 4(e). ábra) eléri ezt a korlátot. Tekintsünk úgy a propeller gráfra, hogy k darab lapátja van. Vegyük észre, hogy a lapátok végén lévő csomópontoknak minden célhoz van rLFA-juk, kivéve a szomszédaikhoz, mivel velük egy páros hosszú körön vannak. A lapátok oldalain elhelyezkedő pontok, mint források, csak a szomszédos link hibák ellen tudnak védelmet nyújtani a szembelévő pontokra mint célállomásokra nézve. Végül a középső csomópontnak csak a lapátok végén elhelyezkedő célállomásokra nézve van rLFA-ja. Így $\mu(G) = \frac{1}{3}$.

A következőkben a kétszeresen pontösszefüggő hálózatokban elérhető alsó korlátokat vetem górcső alá. Az alábbi tézis foglalja össze az ezzel kapcsolatos eredményeket:

4.2. Tézis. *[C2, J3] Úgy találtam, hogy bármely $k > 2$ számra létezik egy olyan kétszeresen pontösszefüggő, $n = 2k$ csomópontszámú G gráf, amire $\mu_{\mathrm{LP}}(G) = \frac{k-1}{2k-1} < 0.5$.*

Bizonyításként megmutatom, hogy a rács topológia (G_k (lásd 4(a). ábra)) és a teljes páros gráf ($K_{k,k}$, lásd 4(f). ábra) eléri ezt a korlátot. A rács topológia esetén minden forrás-cél pár, ahol a cél közvetlen szomszédja a forrásnak, vagy a cél ugyanazon az oldalon van mint a forrás (az ábrán $S(s)$-sel jelölve), nem védhető. Könnyen észrevehető, hogy minden csomópont egy 4 hosszú körön helyezkedik el, amiben a szomszédok mint célcsomópontok nem védhetőek és minden ugyanazon oldalon lévő ponthoz viszont egy ilyen szomszédon át vezet az út. Így ezen csomópontok sem védhetőek. $K_{k,k}$ esete nagyon hasonló, hiszen minden célállomás, ami ugyanazon az oldalon van, mint a forrás, az védett. Ugyanakkor a teljes páros gráf tulajdonságaiból adódóan a forrás és vele minden szomszédos csomópont egy páros körön van, így azok szintén nem védhetőek.

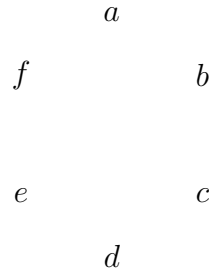
5.5.2. Node-protecting eset

Az alábbi alfejezetben megmutatom, hogy a link-protecting esettel ellentétben, - ahol $\mu_{\mathrm{LP}}(G)$ alulról egy konstans által volt korlátozva, - a node-protecting esetben $\mu_{\mathrm{NP}}(G)$ tetszőlegesen kicsi is lehet akár egy nem túl komplex hálózatban is. Ahogy az a 3. fejezetben említésre került, a Remote LFA elemzésem során a két tetszőleges szomszédos pont között a csomópontok meghibásodása elleni védelmet „nem definiáltnak" tekintem. Így csak azokat a gráfokat veszem számításba, ahol legalább egy nem szomszédos csomópont pár létezik, azaz olyan gráfokat, amelyek nem teljesek. Még ezekben a gráfokban is a kérdés csak akkor érdekes, ha maga az egyszeres csomópont meghibásodás elleni védelem legalább elméletileg lehetséges, azaz a hálózat legalább kétszeresen pontösszefüggő.

Az alábbi tézisben foglalom össze az eredményeket:

4.3. Tézis. *[J3] Úgy találtam, hogy tetszőleges $n \geq 4$ számra létezik egy olyan kétszeresen pontösszefüggő, n csomópontszámú G gráf, amire $\mu_{\mathrm{NP}}(G) = \frac{2(n-3)}{n^2-5n+6} \leq \frac{4}{n}$.*

Ahogy az előzőekben is, bizonyításképpen egy bizonyos n csomópontszámú gráfot mutatok, mely eléri ezt a korlátot. Erre az n csomópontszámú gráfra továbbiakban $\mathcal{L}_n$-ként hivatkozom. Egy példa látható az $\mathcal{L}_n$ gráfra $n = 6$ esetén az 5. ábrán. A gráf legfőbb tulaj-



5. ábra. $\mathrm{rLFA_{NP}}$ szempontból a legrosszabb topológiai adottságokkal rendelkező, $n = 6$ csomópontszámú gráf

donsága, hogy van egy csomópont felül, melynek fokszáma $n-1$; két csomópont, melynek fokszáma 2; valamint a maradék $n-3$ csomópont, melynek fokszáma 3. Ebből adódóan, a nem szomszédos csomópontpárok száma $n^2 - 5n + 6$. Továbbá látható, hogy csak azon csomópontpárok védhetőek, melyek egy 4 hosszú körön egymással szemben helyezkednek el. Az ilyen csomópontpárok száma kétszer annyi, mint a 4 hosszú körök száma (azaz $n-3$), és így védett csomópontpárok számok $2(n-3)$. Így $\mu_{\mathrm{NP}}(\mathcal{L}_n) = \frac{2(n-3)}{n^2-5n+6}$. Vegyük észre, hogy ez a korlát tart a nullához, ami azt jelenti, hogy nagyon nagy $\mathcal{L}_n$ gráfokban az rLFA által lefedett csomópontok aránya elenyésző.

Numerikus elemzéssel arra a következtetésre jutottam, hogy az általam talált alsó korlátok valóban alsó korlátok, legalábbis $n < 10$ esetén, és az a sejtésem, hogy ezek az általános alsó korlátjai az rLFA által nyújtott védelemnek.

5.6. A Remote LFA Graph Extension probléma

Korábbi fejezetekben láthattuk, hogy léteznek nem túl bonyolult hálózatok, melyekben az rLFA által nyújtott védelem minimális. Egyből adódik a kérdés, hogy vajon milyen minimális topológiai módosítás során lehetne az rLFA védelmet 100%-ra feltornászni mind link-protecting, mind node-protecting esetben. Ez a kérdés több aspektusból is fontos szerepet játszik. Egyrészt ez válasz adna arra, hogy a kevésbé védett hálózatok milyen messze vannak a teljes védelemtől, másrészt a hálózati operátorok számára biztosítana egyfajta módszert hálózatuk védelmének megerősítésére.

5.6.1. A probléma formalizálása

A már ismert LFA Graph Extension problémát adaptáltam az általam vizsgált *rLFA Graph Extension* problémára, melynek célja a hálózat minimális számú, jól megválasz-tott élekkel való kiegészítése.

5. Definíció. *$rLFAGraphExtensionLP(G)$: Adott egy $G(V,E)$ gráf, találjuk meg a G gráf $\overline{E}$ komplemens élei halmazának a legkisebb F részhalmazát, melyre $\mu_{\mathrm{LP}}(G(V,E\cup F)=1$.*

A node-protection esetén a definíció hasonlóképpen fogalmazható meg:

6. Definíció. *$rLFAGraphExtensionNP(G)$: Adott egy $G(V,E)$ gráf, találjuk meg a G gráf $\overline{E}$ komplemens élei halmazának a legkisebb F részhalmazát, melyre $\mu_{\mathrm{NP}}(G(V,E\cup F)=1$.*

5.6.2. Számszerű kiértékelés

Mivel az összes korábban tárgyalt LFA hálózat optimalizálási probléma NP-teljesnek bizonyult, - azaz nem volt olyan optimális algoritmus, mely elfogadható időn belül megoldotta volna a problémát, - közvetlenül közelítő algoritmusok kidolgozásával foglalkoztam. Mohó és szimulált lehűtésen alapuló heurisztikák egy teljes családját definiáltam az $rLFAGraphExtensionLP(G)$ és az $rLFAGraphExtensionNP(G)$ probléma megoldására. Az eredmények minden esetben azt mutatták, hogy a mohó módszer idézi elő a legjobb megoldást. Továbbá, mivel az extended P-space nem garantált teljes védelmet egyszeres csomópont meghibásodások ellen, az algoritmusok kiértékelése során ezt az opciót is figyelembe vettem. Az alábbi tézis számszerűsíti az elért eredményeket:

4.4. Tézis. *[C2, J3] Az $rLFAGraphExtension(G)$ probléma megoldására gyors és hatékony heurisztikák egy teljes családját dolgoztam ki. Kiterjedt szimulációs vizsgálatok sorozatával arra a következtetésre jutottam, hogy a vizsgált egység élköltségű hálózatok nagy részében pusztán* 2*, átlagosan pedig* 3.6 *addicionális él hozzáadásával teljes* $\mathrm{rLFA_{LP}}$ *lefedettség érhető el. Egyszeres csomópont meghibásodások esetén átlagosan* 4.05 *új él szükséges, mely szám* 3.3*-ra redukálódik, ha extended rLFA-t használunk.*

Rövid összefoglaló eredmények láthatóak a 2. táblázatban. Link-protecting esetben az η_{LP} jelöli a kezdeti LFA lefedettséget, míg $Gr_{\eta_{\mathrm{LP}}}$ mutatja a teljes LFA lefedettséghez szükséges minimális számú addicionális élek számát, melyet az LFA Graph Extension algoritmus eredményezett. $Gr_{\mu_{\mathrm{LP}}}$ jelöli a kezdeti rLFA lefedettséget, valamint az előzőekhez

2. táblázat. Néhány, a Remote LFA Graph Extension algoritmussal elért eredmény link-protecting esetben

Topology	η_{LP}	$Gr_{\eta_{\mathrm{LP}}}$	μ_{LP}	$Gr_{\mu_{\mathrm{LP}}}$	η_{NP}	$Gr_{\eta_{\mathrm{NP}}}$	μ_{NP}	$Gr_{\mu_{\mathrm{NP}}}$	μ^{e}_{NP}	$Gr^{e}_{\mu_{\mathrm{NP}}}$
AS1221	0.833	1	0.833	1	0.083	3	0.083	1	0.083	1
AS1239	0.898	6	1	0	0.658	16	0.843	1	0.928	1
AS1755	0.889	4	1	0	0.704	7	0.912	1	1	0
AS3257	0.946	3	0.954	1	0.521	20	0.702	5	0.866	3
AS3967	0.864	7	0.969	1	0.715	10	0.896	2	0.994	1
AS6461	0.919	2	1	0	0.505	8	0.596	3	0.747	2
Abilene	0.56	6	0.833	1	0.608	3	0.725	2	0.872	1
AT&T	0.823	6	0.888	2	0.565	12	0.684	4	0.849	2
Deltacom	0.542	79	0.885	4	0.436	113	0.818	9	0.868	9
Geant	0.646	20	0.827	4	0.411	30	0.676	5	0.74	5
Germany	0.695	1	0.882	1	0.599	8	0.77	2	0.955	2
InternetMCI	0.877	3	0.888	2	0.558	9	0.837	3	0.916	1
Italy	0.784	12	0.951	2	0.574	24	0.839	3	0.926	2

hasonlóan $Gr_{\mu_{\mathrm{LP}}}$ mutatja az rLFA Graph Extension által elért eredményeket. Egyszeres csomópont meghibásodások esetén η_{NP} és μ_{NP} indikálja a kezdeti LFA és rLFA lefedettségeket, valamint a $Gr_{\eta_{\mathrm{NP}}}$ és $Gr_{\mu_{\mathrm{NP}}}$ mutatja a szükséges élek számát az LFA Graph Extension, valamint rLFA Graph Extension algoritmust futtatva. Hasonlóképpen, az utolsó két oszlop pedig a node-protecting esetet mutatja extended rLFA használata során.

Az első észrevétel, hogy bizonyos hálózatok Graph Extension algoritmus nélkül is teljes rLFA védettséget élveznek. Másodszor, rLFA módszert használva jóval kevesebb addicionális él szükséges a teljes link-protecting védelem elérése érdekében, mintha csak szimpla LFA-t használnánk. Hasonlóképpen igaz ez az állítás egyszeres csomópont meghibásodások esetén is. Az eredmények azt igazolják, hogy a vizsgált hálózatok nagy részében pusztán 2 új él hozzáadás elegendő a 100 %-os link-protecting rLFA lefedettséghez. Az összes hálózatra nézve ez az érték átlagosan 3.6, míg egyszerű LFA esetén átlagosan 14.5 új él volt szükséges. Egyszeres csomópont meghibásodások esetén, ha extended rLFA-t feltételezünk, átlagosan pusztán 3.3 új él szükséges a teljes rLFA lefedettség eléréséhez. Fontos megjegyezni, hogy ez a szám jóval nagyobb (4.05), ha az egyszerű rLFA opció érhető csak el.

6. Alkalmazhatóság

Úgy gondolom eredményeim nemcsak akadémiai szinten állják meg a helyüket, hanem az ipar számára is relevánsak. Továbbá úgy hiszem, hogy eredményeim jelentősen elősegíthetik az LFA módszerek működésének megértését, valamint segíthetnek eddig hezitáló hálózati operátoroknak letenni a voksukat valamely elérhető módszer mellett. Az LFA alapú optimalizációs kutatásaim során ipari szempontból az Ericsson TrafficLab Magyarország céggel dolgoztam együtt, mely kooperáció során az optimalizációs algoritmusaim egy grafikus interfésszel is rendelkező hálózat elemző alkalmazáshoz is implementálásra kerültek. Így a hálózati operátorok könnyedén analizálhatják és optimalizálhatják saját topológiájukat.

Másrészt, ami a Remote LFA-val kapcsolatos kutatásaimat illeti, kapcsolatban vagyok IETF szabványosítási szervezettel, hogy az eddig Draft-ként lézető rLFA módszer RFC szabvány lehessen. A P-, Q- és extended P-space során bemutatott, távolságokban mért alternatív definícióim ((3), (4) és (5)) megkönnyítik annak eldöntését, hogy egy csomópont

rLFA-e vagy sem[5], mivel az alapvető hurokmentességi feltételek a szimpla LFA [3] esetén is távolságokban vannak kifejezve. Továbbá úgy gondolom, hogy - elsőként az irodalomban - a Remote LFA-val kapcsolatos elemzéseim és a módszer előnyeinek és lehetséges hálózati optimalizálási módszerek megmutatásával talán egy nagyobb „lökés" adható a szolgáltatóknak abba az irányba, hogy az Internetet megszakítás nélkül üzemeltessék és valóban elnyerjék a potenciális felhasználók korlátlan bizalmát.

Köszönetnyilvánítás

Mindenek előtt köszönettel tartozom tudományos témavezetőmnek, Rétvári Gábornak mindazon idejéért és energiájáért, melyet konzultálásomba fektetett. Bátorítása, tanácsadása és támogatása nélkül lehetetlen lett volna a tématerület kutatójává válni. Rámutatott olyan fontos dolgokra, hogy hogyan gondolkodjunk, fejlesszünk és prezentáljuk kutatási eredményeinket. Mindenképp kiemelném, hogy publikációim előkészületeihez tett hasznos tanácsai, megjegyzései nélkül képtelen lettem volna bármilyen tekintélyes és értékes cikk megírására. Mindig irányt mutatott, mikor elveszettnek éreztem magam.

Hálás köszönet illeti Heszberger Zalánt, aki M.Sc-s éveimben volt a konzulensem és egyengette utamat a doktorandusszá válás során. Doktoranduszi éveim alatt mindig segített, mikor céljaim elérésének tekintetében meginogtam.

Szeretnék köszönetet mondani kollégáimnak és szobatársaimnak, Fehér Zoltánnak, Lajtha Balázsnak, Kőrösi Attilának, Csernai Mártonnak, Babarczi Péternek, Németh Feliciánnak, Sonkoly Balázsnak, Gulyás Andrásnak és mindazoknak kiknek neve nem férne fel erre az oldalra a segítségeikért és a kiváló közösségi programokért, melyeket együtt töltöttünk.

Kutatási munkám a Budapesti Műszaki és Gazdaságtudományi Egyetem, Távközlési és Médiainformatikai Tanszékén, azon belül is az MTA-BME Lendület kutatócsoportban és a Nagysebességű Hálózatok Laboratóriumban (HSNLab) végeztem, így köszönettel tartozom Tapolcai Jánosnak, Szabó Róbertnek, Vidács Attilának, Molnár Sándornak a támogatásért, valamint Győri Erzsébetnek a segítségeiért.

Végül, de nem utolsó sorban, hálás köszönet illeti szüleimet, akik lehetővé tették, hogy egyetemi hallgató koromban kizárólag a tanulmányaimra tudjak koncentrálni. Továbbá meg szeretném köszönni testvéremnek és családomnak a szeretetüket és türelmüket. Egy ilyen nagyszerű családi légkör nélkül sosem teljesülhettek volna be az álmaim.

[5] `http://tools.ietf.org/html/draft-ietf-rtgwg-remote-lfa-06#page-25`

Publikációk

Folyóiratcikkek

[J1] **L. Csikor**, M. Nagy, and G. Rétvári, "Network Optimization Techniques for Improving Fast IP-level Resilience with Loop-Free Alternates," Infocommunications Journal, vol. 3, iss. 4, pp. 2-10, 2011. $(6/2 = 3)$

[J2] **L. Csikor**, G. Rétvári, and J. Tapolcai, "Optimizing IGP Link Costs for Improving IP-level Resilience with Loop-Free Alternates," Computer Communications Journal, Special Issue on Reliable Network-based Services, vol. 36, iss. 6, pp. 645-655, 2013. $(6/2 = 3)$

[J3] **L. Csikor** and G. Rétvári, "On Providing Fast Protection with Remote Loop-Free Alternates," Telecommunication Systems Journal, vol. 60, iss. 4, pp. 485-502, 2015. $(6/1 = 6)$

Konferenciacikkek

[C1] 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, pp. 62-69, 2011. (winner of Best Paper Award) $(3/4 = 0.75)$

[C2] **L. Csikor** and G. Rétvári, "IP Fast Reroute with Remote Loop-Free Alternates: the Unit Link Cost Case," in Proc. RNDM, pp. 16-22, 2012. $(3/1 = 3)$

Könyvfejezetek

[B1] **L. Csikor**, G. Rétvári and J. Tapolcai. „High Availability in the Future Internet", Future Internet Assembly 2013: Validated Results and New Horizons, Lecture Notes in Computer Science, *The Future Internet*, vol. 7859, pp. 64-76, 2013. $(6/2 = 3)$

Egyéb, szorosan nem kapcsolódó publikációk

[OC2] **L. Csikor** and Z. Fehér. „Exploring Hidden Relations in Moving Human Groups". In *Proc., POSTER 2010*, Prague, Czech Republic, 6. May 2010. $(3/2 = 1.5)$

[OC1] **L. Csikor** and Z. Fehér. „Information Spreading in Self Oragnizing Mobile Networks". In *Proc., MACRo Conference 2010*, Tirgu Mures, Romania, 14-15. May 2010. $(3/2 = 1.5)$

[OJ1] P. Babarczi, F. Tanai, **L. Csikor**, J. Tapolcai and Z. Heszberger. „Útvonalválasztás késleltetés-toleráns hálózatokban". *Híradástechnika*, vol. 66, no. 1, pp. 23-31, 2011. $(1/5 = 0.2)$

[OC3] F. Németh, B. Sonkoly, A. Gulyás, **L. Csikor**, J. Tapolcai, P. Babarczi and G. Rétvári. „Improving resiliency and throughput of transport networks with OpenFlow and Multipath TCP: Demonstration of results over the Géant OpenFlow testbed". *Open Networking Summit*, Flyer and Demo, Santa Clara, USA, Apr. 2013.

[OC4] F. Németh, B. Sonkoly, **L. Csikor**, and A. Gulyás, "A Large-Scale Multipath Playground for Experimenters and Early Adopters," in ACM SIGCOMM (DEMO), Hong Kong, China, pp. 482-483, 2013.

[OC5] B. Sonkoly, F. Németh, **L. Csikor**, L. Gulyás, and A. Gulyás, "SDN based testbeds for evaluating and promoting multipath TCP," in Proc. IEEE International Conference on Communications (ICC), pp. 3044-3050, June 2014. (3/5 = 0.6)

[OC6] A. Csoma, B. Sonkoly, **L. Csikor**, F. Németh, A. Gulyás, W. Tavernier and S. Sahhaf „ESCAPE: Extensible Service ChAin Prototyping Environment using Mininet, Click, NETCONF and POX". In *Proc., ACM SIGCOMM 2014*, Demo, Chicago, Aug. 2014.

[OC7] A. Csoma, B. Sonkoly, **L. Csikor**, F. Németh, A. Gulyás, D. Jocha, J. Elek, W. Tavernier and S. Sahhaf „Multi-layered Service Orchestration in a Multi-Domain Network Environment". In *Proc., EWSDN 2014*, Demo, Budapest, Sep. 2014.

Hivatkozások

[1] A. Atlas. U-turn alternates for IP/LDP fast-reroute. Internet-Draft, draft-atlas-ip-local-protect-uturn-03, February 2006.

[2] C. Alaettinoglu, V. Jacobson, and H. Yu. Towards milli-second IGP convergence. Internet-Draft, draft-alaettinoglu-isis-convergence-00.txt, IETF, (downloaded: Oct 2013), 2000.

[3] A. Atlas and A. Zinin. Basic specification for IP fast reroute: Loop-Free Alternates. RFC 5286, 2008.

[4] A. Basu and J. G. Riecke. Stability issues in ospf routing. In *ACM SIGCOMM*, pages 225–236, San Diego, CA, USA, August 2001.

[5] S. Bryant, C. Filfils, S. Previdi, M. Shand, and N. So. Remote LFA FRR. Internet-Draft, Dec. 2012.

[6] S. Bryant, M. Shand, and S. Previdi. IP fast reroute using Not-via addresses. Internet-Draft, March 2010.

[7] L. Csikor, M. Nagy, and G. Rétvári. Network optimization techniques for improving fast IP-level resilience with Loop-Free Alternates. *Infocommunications Journal*, 3(4):2–10, 2011.

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

[9] Levente Csikor. GML 2 LGF converter. http://csikor.tmit.bme.hu/GML2LGF.

[10] N. Feamster and H. Balakrishnan. Detecting bgp configuration faults with static analysis. In *NSDI*, pages 43–56, 2005.

[11] C. Filsfils, P. Francois, M. Shand, B. Decraene, J. Uttaro, N. Leymann, and M. Horneffer. Loop-free alternate (LFA) applicability in service provider (SP) networks. RFC 6571, June 2012.

[12] P. Francois, M. Shand, and O. Bonaventure. Disruption-free topology reconfiguration in ospf networks. In *IEEE INFOCOM*, Anchorage, USA, May 2007. INFOCOM 2007 Best Paper Award.

[13] G. Iannaccone, C.-N. Chuah, R. Mortier, S. Bhattacharyya, and C. Diot. Analysis of link failures in an IP backbone. In *ACM SIGCOMM Internet Measurement Workshop*, pages 237–242, 2002.

[14] ISO. Intermediate ststem-to-intermediate system (is-is) routing protocol. ISO/IEC 10589, 2002.

[15] Simon Knight, Hung X. Nguyen, Nick Falkner, Rhys Bowden, and Matthew Roughan. The internet topology zoo. *Selected Areas in Communications, IEEE Journal on*, 29(9):1765–1775, 2011.

[16] A. Kvalbein, A. F. Hansen, T. Čičic, S. Gjessing, and O. Lysne. Fast IP network recovery using multiple routing configurations. In *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, pages 1–11, 2006.

[17] K.-W. Kwong, L. Gao, R. Guerin, and Z.-L. Zhang. On the feasibility and efficacy of protection routing in IP networks. In *INFOCOM, long version is available in Tech. Rep. 2009*, University of Pennsylvania, 2010.

[18] C. Labovitz, A. Ahuja, and F. Jahanian. Experimental study of Internet stability and backbone failures. In *FTCS*, pages 278–285, 1999.

[19] S. Litkowski, B. Decraene, C. Filsfils, and K. Raza. Operational management of loop free alternates. Internet-Draft, draft-litkowski-rtgwg-lfa-manageability-01, February 18, 2013.

[20] R. Mahajan, N. Spring, D. Wetherall, and T. Anderson. Inferring link weights using end-to-end measurements. In *ACM IMC*, pages 231–236, 2002.

[21] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, Y. Ganjali, and C. Diot. Characterization of failures in an operational IP backbone network. *IEEE/ACM Transactions on Networking*, 16(4):749–762, 2008.

[22] A. Markopoulou, G. Iannacone, S. Bhattacharyya, C.-N. Chuah, and C. Diot. Characterization of failures in an IP backbone. In *Proc. IEEE Infocom*, Mar. 2004.

[23] M. Menth, M. Hartmann, and D. Hock. Routing optimization with IP Fast Reroute. Internet-Draft, July 2010.

[24] J. Moy. OSPF version 2. RFC 2328, Apr. 1998.

[25] M. Nagy, J. Tapolcai, and G. Rétvári. Optimization methods for improving IP-level fast protection for local shared risk groups with loop-free alternates. *Springer Telecommunication Systems Journal*, 2012.

[26] G. Rétvári, L. Csikor, J. Tapolcai, G. Enyedi, and A. Császár. Optimizing IGP link costs for improving IP-level resilience. In *Proc. of DRCN*, pages 62–69, Oct. 2011.

[27] G. Rétvári, J. Tapolcai, G. Enyedi, and A. Császár. IP Fast ReRoute: Loop Free Alternates revisited. In *INFOCOM*, pages 2948–2956, 2011.

[28] A. Shaikh, C. Isett, A. Greenberg, M. Roughan, and J. Gottlieb. A case study of OSPF behavior in a large enterprise network. In *IMC*, pages 217–230, 2002.

[29] SNDLib. Survivable fixed telecommunication network design library. http://sndlib.zib.de, downloaded: Apr. 2012.

[30] H. T. Viet, P. Francois, Y. Deville, and O. Bonaventure. Implementation of a traffic engineering technique that preserves IP Fast Reroute in COMET. In *Rencontres Francophones sur les Aspects Algorithmiques des Telecommunications, Algotel*, 2009.

[31] J. Wang and S. Nelakuditi. IP fast reroute with failure inferencing. In *ACM SIGCOMM Workshop on Internet Network Management – The Five-Nines Workshop*, 2007.

[32] D. Watson, F. Jahanian, and C. Labovitz. Experiences with monitoring OSPF on a regional service provider network. In *ICDCS*, pages 204–212, 2003.