A jövő megbízható és hibamentesen működő Internete

Napjainkban az Internet elengedhetetlen tényezője lett a hétköznapjainknak és már-már a társadalom kritikus infrastruktúrájának számít. Ez a tény arra készteti a szolgáltatókat, hogy a hálózatukat megszakítások nélkül tudják üzemeltetni és ezzel teljes mértékben elnyerni a felhasználók bizalmát. Manapság azonban nemcsak a szolgáltatók és a végfelhasználók érintettek ebben a kérdésben, hanem különböző multimédia-szolgáltatók is, hiszen az *IP (Internet Protocol)* elterjedésével, egyre több digitális tartalom „IP felett" jut el a háztartásokba, gondoljunk csak az IP alapú telefóniára, videótáras megoldásokra, valós idejű hírközlésre vagy akár az *IPTV*-re. Szükségszerűen az Internetnek lépést kell tartania ezekkel a valós idejű alkalmazásokkal, amik folyamatos és megbízható kapcsolatot igényelnek. A megbízhatóság azt jelenti, hogy a hálózatban bármelyik időpillanatban a kapcsolat bármely két pont között biztosított, és egy esetleges hiba olyan gyorsan kezelve van, hogy a végfelhasználók ezt semmilyen módon nem érzékelik.

Az Interneten azonban gyakran lépnek fel hibák olyan okokból, mint például a fizikai kábel szakadás, hibás interfészek, stb. Ezeket a hibákat korábban az ún. *Interior Gateway Protocol-ok (IGP)* kezelték[1]. A hiba észlelése után annak ténye az egész hálózatban szétterjesztésre került, majd miután minden csomópont értesült a hibáról, akkor az új topológia alapján újraszámolják a útvonal-választási tábláikat. Ezt szakmai szempontból a hálózat konvergálásának nevezzük és az ideje nagymértékben függ a hálózat méretétől és a csomópontok számítási kapacitásától, ami tipikusan a pár másodperctől percekig, vagy akár órákig is tarthat. Ez az idő egyértelműen meghaladja azt, amit egy valós idejű alkalmazás „kibír".

Ennek érdekében az *Internet Engineering Task Force (IETF)* definiálta az ún. *IP Fast ReRoute (IPFRR)* rendszert, hogy ezt az időt lecsökkentse néhány tíz milliszekundumra. Mindezt úgy éri el, hogy a hibát észlelő csomópontok a hiba tényét nem terjesztik szét, hanem lokálisan a csomagokat előre kiszámított alternatív útvonalakra terelik.

Első megközelítésként az definiálták az ún. *Loop-Free Alternates (LFA)* módszert, ami egyszerű, szabványosított és már régóta elérhető napjaink routereiben. LFA esetén amikor egy csomópont észleli, hogy a szomszédja már nem elérhető, akkor megpróbálja egy olyan másik szomszédjának továbbadni a csomagokat, ami nem fogja neki azt visszaadni és ezzel elkerülve a hurok képződését. Sajnos egy ilyen szomszéd létezése nem minden esetben áll fenn, hiszen ez nagymértékben függ a hálózati topológiától és annak paramétereitől (élköltségek, legrövidebb utak, stb.), így ez a módszer nem tudja garantálni a teljes védelmet tetszőleges hálózatokban. Ezért az elmúlt években rengeteg kezdeményezés született a 100%-os védelem biztosítására, azonban egyik módszer sem használható a jelenleg komplexitásuk, nem szabványos csomagtovábbítási módszerük és addicionális menedzsment költségeik miatt, így a szolgáltatók számára még mindig csak az LFA lehet az egyetlen mentsvár a hálózati hibák ellen.

Nemrég azonban az IETF publikált egy ezidáig még nem szabványosított módszert az LFA által nyújtott védelem növelése érdekében, melynek lényege, hogy a hibák elkerülésére az észlelő csomópont már nem csak a közvetlen szomszédait próbálja meg felhasználni a csomagok elterelésére, hanem távolabbiakat is. Innen jön a neve is a módszernek, ami a *Remote LFA (rLFA)*. Ugyanakkor az LFA-tól „örökölt" topológiafüggő tulajdonsága miatt, a 100%-os rendelkezésre állás biztosítása tetszőleges hálózatokban még mindig nyitott kérdés a kutatók számára.

A hálózati operátorok még mindig hezitálnak a LFA vagy az rLFA „bekapcsolásával" kapcsolatban, hiszen nem egyértelmű az első pillanattól kezdve, hogy ezekkel a módszerekkel ténylegesen mennyit profitálnának a saját hálózatukban, illetve mennyire befolyásolná ez a jelenlegi hálózatuk különböző aspektusait (pl. terheléselosztását).

A kutatásaim során ennek a döntésnek a meghozatalában próbálok segíteni és olyan gráfelméleti eszközöket nyújtok, melyek nagymértékben elősegítik a módszerek és a valós hálózatok védelmi analízisét. Hasonló vizsgálatok már korábban is léteztek a már fent említett, nem szabványosított módszerekhez, de az *LFA-val kapcsolatban* eddig *csak szimulációs* eredmények születtek, és mélyebb matematikai elemzések pedig csak a csomópontok közötti *élek meghibásodását* vették

1 Ilyen például az Open Shortest Path First (OSPF), vagy az IS-IS (Intermediate System-to-Intermediate System)

figyelembe. Ami a *Remote LFA-t* illeti, - tudomásom szerint, - semmilyen információ ezidáig nem volt elérhető arról, hogy különböző hálózatokban a módszer „*hogyan teljesít*”, mik a *korlátai*, vagy éppen hogyan lehetne *javítani* az általa nyújtott védelmen.

Mindezek fényében a munkám elején a „szimpla” LFA által nyújtott védelem matematikai analízisének kiterjesztésére fókuszáltam, mely a csomópontok meghibásodását is figyelembe veszi. Ebben az esetben beláttam, hogy a hálózatok pusztán gráfelméleti tulajdonságai alapján (csomópontok és élek száma, átlagos fokszám, stb.) hogyan változik az LFA lefedettség, mik az alsó és felső korlátok. Hasonló elemzéseket végeztem Remote LFA esetén is, továbbá megállapítottam, hogy mik a szükséges és elégséges feltételek a védelem biztosítása érdekében. Ugyanakkor megvizsgáltam, hogy melyek azok a „rossz” hálózatok, ahol az módszer nem tud megfelelő védelmet nyújtani. Megmutattam, hogy bár az LFA-nál mindig jobb védelmet tud nyújtani, léteznek olyan topológiák, ahol ez az érték megközelíti a nullát. Mindemellett rávilágítottam azokra az összefüggésekre, amelyek megmutatják milyen következtetéseket lehet levonni az egyik módszerrel kapcsolatban, ha van információnk a másikról.

A kezdeti LFA használatok a valós hálózatokban rámutattak arra, hogy a legtöbb esetben sajnos nem tudja garantálni a kívánt védelmet. Az eddigi ismeretek alapján egyértelmű, hogy egy esetleges javulás érdekében a módszerhez nem érdemes nyúlni, hiszen onnantól kezdve az a többi alkalmazhatatlan megközelítés sorsára jut. Így az egyetlen járható út az, ha magához a hálózati topológiához nyúlunk hozzá és próbáljuk meg úgy „csavargatni”, hogy növeljük az LFA-k által nyújtott védelmet. Ezt az utat követtem én is, és különböző hálózat-optimalizálási módszereket tanulmányoztam és dolgoztam ki ennek érdekében. Az egyik ilyen módszer, ha a hálózatunkat már eleve az esetleges hibák elleni védelemre tervezzük meg. A másik az ún. *LFA Graph Extension*, amely a meglévő hálózatot megpróbálja a lehető legkevesebb új éllel kiegészíteni úgy, hogy az LFA lefedettség a lehető legnagyobb mértékben növekedjen. A módszer megalkotói megmutatták, hogy tipikusan **2-3** új él hozzáadásával 100%-os védelem érhető el.

Én először egy harmadik -féle módszert dolgoztam ki, mely az élköltségeket optimalizálja, megváltoztatva ezzel a legrövidebb utakat a hálózatban és így LFA-kat biztosítva olyan esetekben, ahol eddig nem volt. A problémáról (*LFA Cost Optimization*) beláttam, hogy bonyolultságát tekintve *NP-teljes*, így megfogalmaztam egy *lineáris programot (ILP)*, valamint kidolgoztam több *közelítő algoritmust és egy keretrendszert*, melyben rengeteg paraméter függvényében válik ilyen értelemben optimalizálhatóvá a vizsgált hálózat. Megmutattam, hogy ezzel a módszerrel közel **100%**-osra növelhető a védelem bizonyos hálózatokban. Mivel az előző két módszernek lehetnek megvalósítási szempontból korlátai, így egy negyedik megközelítésben összevetettem a kettőt és egy *kombinált módszert* dolgoztam ki, mellyel csökkenthető a fentebb említett szükséges új élek száma.

Mivel a Remote LFA módszer is már a szabványosítás útján jár, ezért a védelmi szempontból történő teljesítőképességét megvizsgáltam több valós hálózati topológiában is, melyek az Internetről szabadon hozzáférhetőek. Az LFA-hoz hasonlóan, ebben az esetben is javaslatot tettem a védelem növelése érdekében egy hálózat-optimalizálási módszerre. Első megközelítésben adaptáltam a fent említett LFA Graph Extension módszert és átdolgoztam. A problémáról (rLFA Graph Extension) szintén kiderült, hogy bonyolult és mivel a módszer maga is több eshetőséget vizsgál, mint a szimpla LFA, így valószínűleg ez is NP-teljes. Ezért ebben az esetben is *közelítő heurisztikát* dolgoztam ki, mely segítségével megmutattam, hogy már néhány él hozzáadásával is elérhető a kívánt **100%**-os védelem. Mindemellett, természetesen ennek a módszernek a kidolgozása során is ügyeltem azokra az esetekre is, ahol maga a csomópont is meghibásodhat. Mivel a csomópont hibák magukkal vonják több él együttes „kiesését” is a hálózatból, így ebben az esetben átlagosan csak **1-2** éllel kell több a teljes védelem elérése érdekében.

Összefoglalás

Munkám során a konzulensemen, Dr. Rétvári Gáboron (BME) kívül, együtt dolgoztam több ipari kutatóval is, többek között Dr. Császár Andrással és Dr. Enyedi Gáborral (Ericsson). A közös munkánk eredménye egy olyan alkalmazás, mely az említett módszereinket elérhetővé teszi hálózati operátorok számára. Továbbá, jelenleg is kapcsolatban vagyunk a Remote LFA-t szabványosító szervezet tagjaival, akikkel megvitatjuk kérdéseinket és segítjük a munkájukat a mi eredményeinkkel.