HADMÉRNÖK

XII. Évfolyam 2. szám – 2017. június

# GRÁFELMÉLETI MÓDSZEREK A KRITIKUS INFRASTRUKTÚRA VÉDELEMBEN

## GRAPH THEORIC METHODS IN CRITICAL INFRASTRUCTURE PROTECTION

ZENTAI Dániel

(ORCID: 0000-0002-3321-2013)

zentai.daniel@bgk.uni-obuda.hu

***Absztrakt***

*Telefonhálózatok, úthálózatok, számítógépes hálózatok modellezésének hatékony eszköze a gráfelmélet. Gráfnak nevezzük olyan csomópontok halmazát, melyeket élekkel kötünk össze. Hasonlóan, kritikus infrastruktúrák modellezésének is természetes módja a gráfelméleti eszközök felhasználása, legyen szó információs infrastruktúráról, vagy akár vasúthálózatról. Kritikus infrastruktúrákkal szemben magától értetődő elvárás lehet, hogy egy (vagy esetleg néhány) infrastruktúra elem meghibásodása esetén az infrastruktúra továbbra is összefüggő maradjon, azaz lehetőség szerint ne jöjjenek létre egymástól szeparált infrastruktúra elemek. Ebben a dolgozatban kritikus infrastruktúrák hibatűrését, illetve támadásokkal szembeni ellenállóképességét modellezük gráfelméleti eszközökkel, az infrastruktúrát leíró gráf többszörös összefüggőségét vizsgálva.*

***Kulcsszavak:*** *kritikus infrastruktúra védelem, gráfelmélet, többszörös összefüggőség*

***Abstract***

*Graph theory is an effective tool for modeling telecommunication networks, road networks, or computer networks. A graph is a set of vertices, connected by edges. Graph theory can be used naturally in critical infrastructures too, including e.g. information infrastructures, or railway networks. We can set up a natural requirement regarding to critical infrastructures, namely, even if some failures occur in the infrastructure, and some infrastructure component become unreachable for a while, the infrastructure itself has to remain connected. In this work we model the fault tolerance of critical infrastructures with graph theoric means, and with particular emphasis on the multiple connectivity of the infrastructure graph.*

***Keywords:*** *critical infrastructure protection, graph theory, multiple connectivity*

A kézirat benyújtásának dátuma (Date of the submission): 2017.04.07.
A kézirat elfogadásának dátuma (Date of the acceptance): 2017.06.16.

## BEVEZETÉS

A kritikus infrastruktúrák védelmének kutatása aktuális, és széleskörűen kutatott terület [4]. Ennek ellenére az ehhez kapcsolódó matematikai apparátus még meglehetősen kidolgozatlan. Ebben a dolgozatban kritikus infrastruktúrák védelmének gráfelméleti modellezését tűztük ki célul. A kritikus infrastruktúrák – legyen szó akár információs infrastruktúráról, elektromos hálózatról, vagy úthálózatról – felfoghatók hálózatként, melynek csomópontjai az infrastruktúra elemek, élei pedig az infrastruktúra elemek közötti fizikai, vagy logikai kapcsolatok. Hálózatok vizsgálatához szolgáltat hatékony eszközöket a gráfelmélet. Munkánkban hálózatok megbízhatóságát, hibatűrését vizsgálom gráfelméleti módszerekkel, nevezetesen gráfok többszörös összefüggőségének vizsgálatával.

Az első fejezetben ismertjük a további megértéshez szükséges gráfelméleti alapfogalmakat. Itt csak az elengedhetetlenül szükséges fogalmak kerülnek tisztázásra, mélyebb megalapozáshoz javaslom az érdeklődőknek a [3] könyvet, kritikus infrastruktúrák megismeréséhez pedig a [8] jegyzetet.

A második fejezetben részletesen kitérünk a hálózatok megbízhatóságának egyik legegyszerűbb mérőszámára, a többszörös összefüggőségre, és az ehhez szorosan kapcsolódó hálózati folyamok fogalmára.

A harmadik fejezetben a kritikus infrastruktúrákra vonatkoztatva mutatjuk be a problémát, felvázolva egy algoritmust a kritikus infrastruktúrák gráfelméleti megbízhatóságának vizsgálatára.

## A GRÁFELMÉLETI HÁTTÉR MEGALAPOZÁSA

Ebben a fejezetben ismertetünk bizonyos gráfelméleti alapfogalmakat, melyek szükségesek a továbbiak megértéséhez.

Legyen $V = \{v_1, v_2, \ldots, v_n\}$ véges halmaz, és legyen E a V halmaz bizonyos kételemű részhalmazainak egy halmaza, azaz $E \subseteq \binom{V}{2}$. Az ebből a két halmazból álló $G = (V,E)$ rendezett párt *véges egyszerű gráfnak* nevezzük.

A $V = V(G)$ halmaz elemeit a G gráf *csúcsainak* (más néven pontjainak), az $E = E(G)$ halmaz elemeit pedig a G gráf *éleinek* nevezzük. A $G = (V,E)$ gráfban a $v, w \in V$ csúcsokat *szomszédosnak* nevezzük, ha őket él köti össze, azaz ha $\{v,w\} \in E$. A $G = (V,E)$ gráf *irányított* gráf abban az esetben, ha minden élének van egy iránya is, azaz megkülönböztetjük a $(v,w) \in E$ élt a $(w,v) \in E$ éltől minden v és w csúcspárra. Ebben az esetben $E \subseteq V \times V$. A gráfok szokásos geometriai reprezentációjában az éleket irányítatlan esetben szakaszokkal (1. ábra), vagy görbékkel, irányított esetben pedig nyilakkal (2. ábra) ábrázoljuk.

A $G = (V,E)$ gráf $v \in V$ csúcsának *fokszáma* a v szomszédjainak számával egyenlő. A v csúcs fokszámát d(v) jelöli. Irányított gráf esetében megkülönböztetjük a v csúcs *befokát* és *kifokát*. A v csúcs befoka azon éleknek a száma, melyeknek végpontja v, a v csúcs kifoka pedig azon élek száma, melyeknek a kezdőpontja v.

A *séta* a gráfban csúcsok és élek váltakozó $v_0e_1v_{1\ldots}e_kv_k$ sorozata, ahol mindegyik $e_i = \{v_{i-1},v_i\}$ él a sorozatban őt megelőző és őt követő csúcsokat köti össze. A *vonal* olyan séta, amelyben egy él legfeljebb egyszer szerepelhet, az *út* pedig olyan vonal, amelyben minden csúcs is maximum egyszer szerepel. A séta, vonal vagy út hosszának az ezek során érintett élek számát nevezzük.

A $G = (V,E)$ gráfot *összefüggőnek* nevezzük, ha bármely $u \in V$ pontjából bármely $v \in V$ pontjába vezet u kezdőpontú és v végpontú út. Legyen $G = (V,E)$ nem feltétlenül összefüggő gráf. G ponthalmazának egy $C \subseteq V(G)$ részhalmazát akkor nevezzük összefüggőségi *komponensnek*, ha teljesül rá, hogy bármely $u \in C$ pontból bármely $v \in C$ pontba vezet út, de semelyik C-beli pontból nem vezet út a $V \setminus C$ halmaz semelyik pontjába sem. A G gráf

összefüggőségi komponenseinek számát c(G) jelöli. Egy G gráf tehát pontosan akkor összefüggő, ha c(G) = 1.

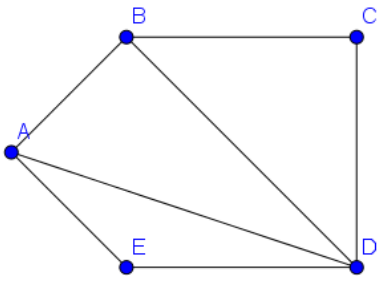
## HÁLÓZATOK MEGBÍZHATÓSÁGA

A továbbiakban végig feltesszük, hogy a kritikus infrastruktúránkat modellező G = (V,E) gráf összefüggő. Ezen egyszerű feltevést az indokolja, hogy ha esetleg nem összefüggő gráfot vizsgálunk, akkor elegendő az alábbiakban tárgyalt gráfparamétereket komponensenként vizsgálni. Kritikus infrastruktúrák, és általában véve hálózatok megbízhatóságának egy természetes mérőszáma az infrastruktúrát modellező gráf többszörös összefüggősége.

*Definíció*: Azt mondjuk, hogy a G = (V,E) gráf *k-szorosan él-összefüggő*, vagy röviden k-él-összefüggő, ha G-nek legalább k+1 pontja van (azaz $|V(G)| \geq k+1$), és bárhogyan hagyunk el G-ből legfeljebb k darab élt, a kapott G' gráf összefüggő marad. A legnagyobb olyan k értéket, ami a fenti feltételeket teljesíti, a gráf él-összefüggőségi számának nevezzük, és $\lambda(G)$-vel jelöljük.

*Definíció*: Azt mondjuk, hogy a G = (V,E) *k-szorosan összefüggő*, vagy röviden k-összefüggő, ha G-nek legalább k+1 pontja van (azaz $|V(G)| \geq k+1$), és bárhogyan hagyunk el G-ből legfeljebb k darab csúcsot, a kapott G' gráf összefüggő marad. A legnagyobb olyan k értéket, ami a fenti feltételeket teljesíti, a gráf összefüggőségi számának nevezzük, és $\kappa(G)$-vel jelöljük.

A fenti két definíció közül mi a k-összefüggőséget fogjuk vizsgálni. Feltételezzük ugyanis, hogy a támadó nem az infrastruktúrában lévő összeköttetéseket támadja, hanem egy, vagy több csomópont kiiktatására, elérhetetlenné tételére törekszik. Ebben az esetben úgy kell az infrastruktúrát kialakítani, hogy az azt modellező G = (V,E) gráfra $\kappa(G) \geq t$ teljesüljön, ahol t a támadó feltételezett támadási kapacitása, azaz t az a maximális érték, ahány infrastruktúra elemet képes a támadó kiiktatni feltételezésünk szerint. Az alábbi ábrán látható gráf 2-összefüggő, hiszen bármely csúcs törlésével összefüggő marad, de nem 3-összefüggő, hiszen például az A és D csúcsok törlésével két komponens keletkezik.




**1. ábra** Példa 2-összefüggő gráfra

A gyakorlatban a definíció alapján nem tudjuk hatékonyan kiszámolni egy gráf összefüggőségi, illetve él-összefüggőségi számát. Ugyanis egy n csúcsú gráfban összesen $\binom{n}{k}$ féle lehetőségünk van k csúcsot kitörölni, így $\binom{n}{k}$ esetben kellene ellenőriznünk, hogy a kapott G' gráf összefüggő marad-e, ennyi lehetőséget megvizsgálni pedig csak egészen kis k értékek esetén tudnánk akár a leggyorsabb számítógépek segítségével is. (Él-összefüggőség vizsgálatakor ez az érték $\binom{|E|}{k}$.) Ezért a gyakorlatban az összefüggőségi definíciók alábbi ekvivalens alakjait ellenőrizzük. A következő két tétel Menger tételének közvetlen következményei. Menger tételeit itt most nem közöljük, ugyanis a megértéshez ezek nem szükségesek. Az érdeklődő olvasó megtalálja Menger tételeit [2]-ben.

*Állítás*: Az alábbi két állítás ekvivalens:

1. A G = (V,E) gráf k-szorosan él-összefüggő.
2. Tetszőleges u,v ∈ V(G) esetén van k darab éldiszjunkt u-v út, azaz k darab olyan u-v út, melyekre teljesül, hogy semelyik kettőnek nincs közös éle.

*Állítás*: Az alábbi két állítás ekvivalens:

1. A G = (V,E) gráf k-szorosan összefüggő.
2. Tetszőleges u,v ∈ V(G) esetén van k darab belsőleg pontdiszjunkt u-v út, azaz k darab olyan u-v út, melyekre teljesül, hogy semelyik kettőnek nincs közös pontja a kezdőponttól és a végponttól eltekintve.

A fenti két állítás alapján definiálhatjuk gráfok lokális él-összefüggőségét, illetve lokális összefüggőségét.

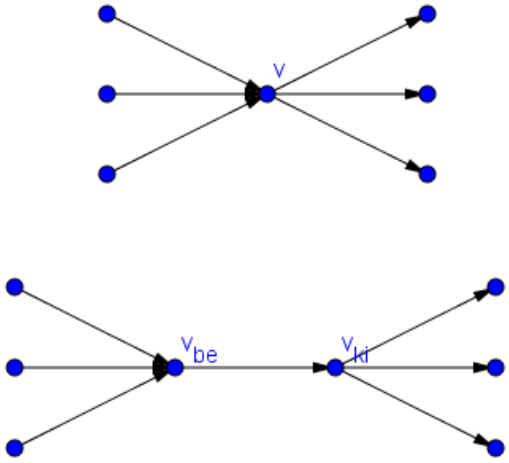
*Definíció*: Legyen G = (V,E) gráf, és u,v ∈ V(G) tetszőleges csúcsok. Az u és v csúcsok közötti *lokális él-összefüggőség* az u és v közötti éldiszjunkt utak maximális száma, melyet $\lambda(u,v)$ jelöl.

*Definíció*: Legyen G = (V,E) gráf, és u,v ∈ V(G) tetszőleges csúcsok. Az u és v csúcsok közötti *lokális összefüggőség* az u és v közötti belsőleg pontdiszjunkt utak maximális száma, melyet $\kappa(u,v)$ jelöl.

Megjegyezzük, hogy egy gráf globális él-összefüggőségi száma a lokális él-összefüggőségi számok minimuma, formálisan $\lambda(G) = \min\{\lambda(u,v) \mid u,v \in V(G)\}$. Hasonlóan, egy gráf globális összefüggőségi száma megegyezik a lokális összefüggőségi számok minimumával, azaz $\kappa(G) = \min\{\kappa(u,v) \mid u,v \in V(G)\}$.

## Hálózati folyamok

A továbbiakban ismertetjük a hálózati folyamok fogalmát, és ennek alkalmazását a lokális összefüggőség kiszámítására. A folyam fogalmát irányított gráfokon fogjuk bevezetni, de ez nem jelent valódi megszorítást, ugyanis bármely irányítatlan gráfot tudunk úgy módosítani, hogy a gráf minden éle helyett felveszünk egy párhuzamos élpárt, és ezen élpár egyik tagját az egyik végpont felé, a másik tagját a másik végpont felé irányítjuk. Általában a maximális folyam kiszámítására készített algoritmusokkal a lokális él-összefüggőséget tudjuk kiszámítani. Ahhoz, hogy a lokális összefüggőség kiszámítását algoritmizálni tudjuk ilyen módon, a következő transzformációt kell elvégeznünk a gráfunkkal. Legyen most G = (V,E) egy irányított gráf, s,t ∈ V(G) és tegyük fel, hogy $\kappa(s,t)$ értékét szeretnénk kiszámolni. Ehhez minden v ∈ V(G) \ {s,t} csúcs esetében elvégezzük a következő, csúcsszéthúzásnak nevezett műveletet. Vezessünk be a v csúcs helyett egy $v_{be}$ és egy $v_{ki}$ csúcsot. A korábban v-be belépő élek végpontja legyen $v_{be}$, a v-ből kilépő élek kezdőpontja legyen $v_{ki}$, és adjuk hozzá a gráfhoz a $v_{be}v_{ki}$ élt. Legyen az így kapott gráf G'. A csúcsszéthúzás műveletét az alábbi két ábra szemlélteti.




**2. ábra** A csúcsszéthúzás művelete

Könnyen látható, hogy G-ben két s-t útnak pontosan akkor van közös csúcsa, ha G'-ben a megfelelő két s-t útnak van közös éle.

A hálózati folyamok definiálásához legyen G = (V,E) irányított gráf, s, t ∈ V(G), és legyen c : E(G) → $\mathbb{R}_+$ az élekhez nemnegatív valós számokat rendelő függvény. Erre a c függvényre a kapacitásfüggvény elnevezést fogjuk használni. A kitüntetett szerepű s csúcsot forrásnak, a t csúcsot pedig nyelőnek hívjuk. Ezen két csúcs között fogjuk a folyam értékét kiszámolni.

*Definíció*: *Hálózati folyamnak* egy olyan f : E(G) → $\mathbb{R}$ függvényt nevezünk, amelyre teljesülnek az alábbiak.

- Minden e ∈ E(G)-re teljesül, hogy $0 \leq f(e) \leq c(e)$, azaz a folyam értéke minden élen nemnegatív, és nem lépi túl a kapacitásfüggvény értékét.
- Teljesül f-re a megmaradási törvény, azaz minden v ∈ V(G) \ {s,t} csúcs esetén a v-be belépő éleken a folyamértékek összege megegyezik a v-ből kilépő éleken a folyamértékek összegével. Ha tehát $f_{be}(v)$-vel (illetve $f_{ki}(v)$-vel) jelöljük a v–be belépő (illetve kilépő) éleken a folyamértékek összegét akkor a megmaradási törvény megfelel az $f_{be}(v) = f_{ki}(v)$ egyenlőségnek.

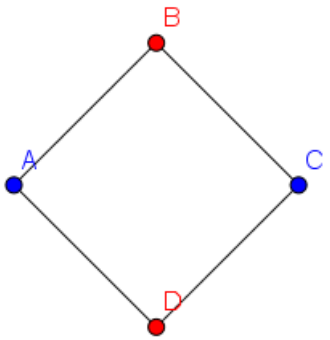
A folyam értéke az $f_{be}(s) - f_{ki}(s)$ érték. Maximális értékű folyam kiszámítására az egyik legismertebb algoritmus a Ford-Fulkerson algoritmus, melyet [1] tárgyal részletesen. Hangsúlyozzuk azonban, hogy a Ford-Fulkerson algoritmust nem a leggyorsabb folyamalgoritmusok között tartjuk számon, és kritikus infrastruktúrákra vonatkoztatva a probléma bármilyen folyamalgoritmussal megoldható. További folyamalgoritmusok részletes megismerésére javasoljuk a [7] és a [6] jegyzeteket.

## ALKALMAZÁS KRITIKUS INFRASTRUKTÚRÁKBAN

Tekintsünk egy kritikus infrastruktúrát, és az azt modellező G = (V,E) gráfot. A gráf csúcsai ebben az esetben infrastruktúra elemeket reprezentálnak, melyeket két csoportba osztunk a hozzájuk tartozó biztonsági kockázat mértéke szerint. A biztonsági kockázat formalizálására az [4] szerinti ajánlást fogjuk használni gráfelméleti megfogalmazással. A gráf minden csúcsához definiálunk egy kockázati értéket az alábbiak szerint. Legyen r : V(G) → $\mathbb{R}_+$ a következő függvény.

$$r(v) = \sum_{t \in T(v)} p(t)d(t) \qquad (1)$$

ahol r(v) a v csúcshoz tartozó biztonsági kockázat mértéke, T(v) a v csúcsot fenyegető lehetséges támadások halmaza, p(t) a t fenyegetés bekövetkezésének valószínűsége, d(t) pedig a t fenyegetés bekövetkeztével okozott kár mértéke. Definiáljunk továbbá egy $T \geq 0$ küszöbszámot, amely a kockázatos, illetve nem kockázatos komponenseket választja el egymástól, aszerint, hogy ha $r(v) \leq T$, akkor a v csúcs nem kockázatos, ha pedig $r(v) > T$, akkor a v csúcs kockázatos. Ez alapján a G gráf csúcshalmazát felbonthatjuk két diszjunkt halmaz uniójára oly módon, hogy $V(G) = V_0 \cup V_1$, ahol $V_0 = \{v \in V(G) \mid r(v) \leq T\}$ és $V_1 = \{v \in V(G) \mid r(v) > T\}$. A kockázati besorolás után életszerűbb a modellt úgy felépíteni, hogy a kockázatos, illetve nem kockázatos csomópontok esetében más lokális összefüggőségi értéket követelünk meg. Tegyük fel tehát, hogy a nem kockázatos elemek esetében azt szeretnénk ellenőrizni, hogy a lokális összefüggőségi szám elér-e egy adott $k_0$ értéket. Ezzel szemben a kockázatos elemek esetében azt vizsgáljuk, hogy a lokális összefüggőségi szám elér-e valamely $k_1 \geq k_0$ értéket. Formálisan, azt vizsgáljuk, hogy igaz-e a $\kappa(u,v) \geq k_1$ összefüggés, minden $u,v \in V_1$ pontpárra, valamint igaz-e a $\kappa(u,v) \geq k_0$ a többi pontpárra. Megjegyezzük, hogy ezen értékek vizsgálata semmit nem árul el a $V_1$ által feszített részgráf összefüggőségi számáról. Erre az alábbi gráf szolgáltat példát. A pirossal jelölt B és D csúcsok által veszített részgráf mindössze két izolált csúcsból áll, bár lokális összefüggőségükre teljesül, hogy $\kappa(B,D)=2$.




**3. ábra** A lokális összefüggőség, és a megfelelő feszített részgráf összefüggősége közötti különbség

Ezek után rátérünk a lokális él-összefüggőség kiszámítására folyam algoritmussal. Fontos tulajdonsága a maximális értékű folyam kereső algoritmusoknak, hogy ha a c kapacitásfüggvény egészértékű, úgy a maximális folyam is választható egészértékűnek. Emlékeztetünk rá, hogy folyamokkal lokális él-összefüggőséget tudunk számolni, így minden s,t csúcspár esetében a folyam algoritmus futtatása előtt el kell végeznünk a csúcsszéthúzás műveletét minden $v \in V(G) \setminus \{s,t\}$ csúcsra. Legyen a csúcsszéthúzással kapott gráf G'. Válasszuk meg úgy c kapacitásfüggvényt, hogy $c(e) = 1$ legyen minden $e \in E(G')$ esetén. Ekkor, mivel a kapacitásfüggvény minden élen egészértékű, a maximális folyam is választható egészértékűnek. Ennek következtében a folyam értéke G' minden élén 0 vagy 1 lehet kizárólag. Tekintsük most azon élek által feszített részgráfot, melyekre $f(e) = 1$. Legyen ez a részgráf H. Ekkor a H részgráfban az s és t csúcsok kivételével minden csúcs befoka és kifoka is 1, tehát H nem más, mint néhány éldiszjunkt út egyesítése, továbbá ezen éldiszjunkt utak kezdőpontja s, végpontja pedig t. Mivel minden egyes ilyen úton a folyam értéke 1 (hiszen az út minden élére teljesül $f(e) = 1$), a folyam értéke nem lesz más, mint az éldiszjunkt s-t utak maximális száma G'-ben, amely Menger tétele alapján nem más, mint az s és t közötti lokális élösszefüggőségi szám, $\lambda(s,t)$. Mivel G'-t G-ből csúcsszéthúzásokkal kaptuk meg, ez az érték megegyezik a G-beli, s és t közötti lokális összefügőségi számmal, $\kappa(s,t)$-vel, és éppen ezt akartuk kiszámolni. Ezt az eljárást megismételve minden csúcspárra ellenőrizni

tudjuk, hogy az előírt lokális összefüggőségi értékek teljesül-e az infrastruktúra minden elemére.

## KÖVETKEZTETÉSEK

A fentiek értelmében bármely kritikus infrastruktúrához, amely jól modellezhető gráfokkal, hatékony algoritmust lehet adni az infrastruktúra hibatűrő képességének becslésére. A dolgozat fő eredményeként ismertettük, hogy a gráfelméletben széleskörűen használt hálózati folyamokat, és a hozzájuk kapcsolódó algoritmusokat hogyan lehet e problémakör megoldására felhasználni.

Érdekes továbblépési lehetőség azt megvizsgálni, hogy ha egy kritikus infrastruktúra nem tesz eleget a megbízhatósági követelményeknek, akkor hogyan lehet kiegészíteni a lehető legkevesebb él hozzávételével úgy, hogy megfelelő biztonságot nyújtson. Ennek egy általánosítása, ha nem az élek darabszámát szeretnénk minimalizálni, hanem minden élhez tartozik egy költség, ami a csomópontok közötti kapcsolat kiépítésének erőforrás igényének felel meg. Ebben az esetben a kiegészítésre használt élek összköltségének a minimalizálása a feladat.

## FELHASZNÁLT IRODALOM

[1] FORD, L. R.; FULKERSON, D. R.: *Maximal flow through a network*, Canadian Journal of Mathematics. 8, 1956, 399–404 old.

[2] KATONA Y. Gy, RECSKI A., SZABÓ Cs.: *A számítástudomány alapjai*, Typotex, Budapest, 2002, 69-70. old.

[3] LOVÁSZ L., PELIKÁN J., VESZTERGOMBI K.: *Diszkrét matematika.* Typotex kiadó, Budapest, 2010

[4] *Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 12. számú ajánlása* – BODALKI Á., CSERNAY A., MÁTYÁS P., MUHA l., PAPP Gy., VADÁSZ D.: Informatikai Rendszerek Biztonsági Követelményei – Budapest, 1996.

[5] BABOS T.: *The First Critical Infrastructure Protection Research Project in Hungary*, Springer Publishing Company, 2016, 1-22. old.

[6] http://www.cs.elte.hu/~frank/jegyzet/graf/graf.2014.pdf (letöltve: 2017.01.12.)

[7] http://www.cs.elte.hu/~kiraly/Algelm.pdf (letöltve: 2017.01.12.)

[8] http://uni-nke.hu/downloads/konyvtar/kovasz/kritikus_infrastrukturak.pdf (letöltve: 2016.12.13.)