Hogyan befolyásolja a villamosenergia-hálózatról rendelkezésre álló információ a fizikai támadások által okozott sérülékenységről alkotott képet?

A hazai energiaszolgáltatás túlélőképessége

Hartmann Bálint

Eötvös Loránd Kutatási Hálózat, Energiatudományi Kutatóközpont, Budapest, Magyarország

Összefoglalás

A villamosenergia-rendszerek fizikai támadásokkal szembeni ellenálló képessége a közelmúltban világszerte történt események ismeretében egyre nagyobb hangsúlyt kap a tématerület kutatásaiban. Az ilyen eseményekre való megfelelő felkészüléshez elengedhetetlen az üzemeltetett infrastruktúrának, elsősorban annak gyengeségeinek pontos ismerete. A cikkben Magyarország villamosenergia-hálózatának adatai alapján készített súlyozatlan és súlyozott gráfokon végzünk vizsgálatokat, hogy megértsük a különböző stratégia mentén kiválasztott célpontok elleni támadások milyen mértékben csökkentik a topológiai hatékonyságot. A cikk célja egyben a magyar hálózat sérülékenységének általános bemutatása is, mely hasznos bemeneti információ lehet a kockázati tervek elkészítésekor.

Kulcsszavak: villamosenergia-rendszer, sérülékenység, komplex hálózat, támadás, köztiség

How grid information affects the perception of vulnerability of the power grid under physical attacks

Robustness of the Hungarian power grid

Bálint Hartmann

ELKH Centre for Energy Research, Budapest, Hungary

Summary

Tolerance of the power grid against physical intrusions has gained importance in the light of various attacks that have taken place around the world. To adequately prepare for such events, grid operators have to possess a deep understanding of their infrastructure, more specifically, of its weaknesses. A graph representation of the Hungarian power grid was created in a way that the vertices are generators, transformers, and substations and the edges are high-voltage transmission lines. All transmission and sub-transmission elements were considered, including the 132 kV network as well. The network is subjected to various types of single and double element attacks, objects of which are selected according to different aspects. The vulnerability of the network is measured as a relative drop in efficiency when a vertex or an edge is removed from the network. Efficiency is a measure of the network's performance, assuming that the efficiency for transmitting electricity between vertices i and j is proportional to the reciprocal of their distance. In this paper, simultaneous removals were considered, arranged into two scenarios (single or double element removal) and a total of 5 cases were carried out (single vertex removal, single edge removal, double vertex removal, double edge removal, single vertex and single edge removal). During the examinations, all possible removal

combinations were simulated, thus the 5 cases represent 385, 504, 73920, 128271 and 193797 runs, respectively. After all runs were performed, damage values were determined for random and targeted attacks, and attacks causing maximal damage were also identified. In all cases, damage was calculated for unweighted and weighted networks as well, to enable the comparison of those two models. The aims of this paper are threefold: to perform a general assessment on the vulnerability of the Hungarian power grid against random and targeted attacks; to compare the damage caused by different attack strategies; and to highlight the differences between using unweighted and weighted graphs representations. Random removal of a single vertex or a single edge caused 0.3–0.4% drop in efficiency, respectively, which indicates a high tolerance against such attacks. Damage for random double attacks was still only in the range of 0.6–0.8%, which is acceptable. It was shown that if targets are selected by the attacker based on the betweenness rank of the element, damage would be below the maximal possible values. Comparison of the damage measured in the unweighted and the weighted network representations has shown that damage to the weighted network tends to be bigger for vertex attacks, but the contrary is observed for edge attacks. Numerical differences between the two representations do not show any trend that could be generalised, but in the case of the most vulnerable elements significant differences were found in damage measures, which underlines the importance of using weighted models.

Keywords: power system, vulnerability, complex network, attack, betweenness

Bevezetés

Az Európai Unió energiapolitikájának egyik fő üzenete a váratlan helyzetekre való felkészülés szükségessége, a villamosenergia-rendszerek sérülékenységének csökkentése, melyek kapcsán több szabályozás is született az elmúlt években. A Bizottság 2017/1485 számú rendelete a villamosenergia-átviteli hálózat üzemeltetésére vonatkozóan módszertani javaslatokat fogalmaz meg az egyes hálózati elemek kiesésének relevanciája kapcsán *(Európai Unió 2017)*. A rendelet szövege szerint az összes rendszerirányító (TSO) „módszertant dolgoz ki legalább szinkronterületenként, hogy a kikapcsolás-összehangolás szempontjából értékeljék az átviteli rendszerben vagy elosztórendszerben" a hálózati elemek relevanciáját; ez pedig a hálózat sérülékenységéhez kapcsolódó modellezési és szimulációs vizsgálatokat tesz szükségessé. Az Európai Parlament és a Tanács 2019/941 rendelete a villamosenergia-ágazati kockázatokra való felkészülés kapcsán a szinkronterületen belüli koordináció fontosságát hangsúlyozza, melynek részeként minden tagállamnak nemzeti kockázati tervet kell kidolgoznia a regionális és tagállami villamosenergia-ellátási válságforgatókönyvek alapján *(Európai Parlament és Tanács 2019)*.

Mindkét rendelet szervesen kapcsolódik az elmúlt évtizedben publikált, a villamosenergia-rendszerek sérülékenységét vizsgáló kutatási eredményekhez. Jelen cikkben a szerző nem kíván teljes körű áttekintést nyújtani a nemzetközi szakirodalom tekintetében, de fontosnak tartja az igen széles spektrumot lefedő kutatások rövid bemutatását.

A villamosenergia-rendszer sérülékenységét jellemzően fizikai vagy kiberfizikai támadások esetén mutatott viselkedése alapján értékelhetjük. Utóbbi csoportba tartoznak az általános sérülékenység-vizsgálatok *(Singh–Mahajan 2020; Tu–Shen–Xia 2020)*, az egyes alkalmazásokra és technológiákra gyakorolt hatásokra fókuszáló cikkek *(Saraswat et al. 2020; Rajkumar et al. 2020; Wu et al. 2020)* és az egészen specifikus tanulmányok *(Zhou et al. 2020; Shen–Gao–Peng 2020; Pace et al. 2020)*. A nemzetközi tudományos diskurzusnak ezek mellett részét képezi a topológia optimalizációjának *(Aziz et al. 2020; Liu–Wang 2021)*, az adatbiztonságnak *(Lesieutre–Borden–Ramanathan 2020)*, a rosszindulatú tevékenységek észlelésének *(Xiong et al. 2020; Chen et al. 2020; He et al. 2020; Ghafouri et al. 2020)*, a megelőző és helyesbítő tevékenységek *(Jin et al. 2021; Khare–Mohapatra–Singh 2021)*, valamint a helyreállítás *(Edib et al. 2020; Sharma 2020)* kérdései is.

Amennyiben a jelen cikk által is a vizsgálatok középpontjába helyezett, villamosenergia-hálózattal kapcsolatos munkákra fókuszálunk, jellemzően olyan cikkeket olvashatunk, melyek vagy csomópontok (alállomások) *(Albert–Albert–Narakado 2004; Crucitti–Latora–Marchiori 2004a; Kinney et al. 2005; Holmgren 2006; Rosas-Casals–Valverde–Solé 2007; Solé et al. 2008; Wang–Rong 2009; Hines et al. 2010; Wang–Scaglione–Thomas 2010; Han–Zhang 2011; Brummit–D'Souza–Leicht 2012; Fang et al. 2021)*, vagy élek (távvezetékek) *(Crucitti–Latora–Marchiori 2004a; Pepyne 2007; Rosato–Bologna–Tiriticco 2007; Arianos et al. 2009; Bompard–Napoli–Xue 2009; Dwivedi–Yu–Sokolowski 2009; Dwivedi–Yu–Sokolowski 2010; Pahwa et al. 2010; Wang et al. 2010; Long–Chen 2020)* kieséséne k hatását vizsgálják. Lényegesen kevesebb munka tárgyalja a két eset együttes bekövetkezését *(Chassin–Posse 2005; Holmgren–Jenelius–Westin 2007; Gouhua et al. 2008; Bompard–Wu–Xue 2010; Mei–Zhang–Cao 2011a; Pagani–Aiello 2011; Gao–Pu–Li 2020; Galindo-González–Angulo-Garcia–Osorio 2020)*. Amennyiben a hálózati kieséseket rosszindulatú tevékenységek eredményeként interpretáljuk, különbséget tehetünk véletlenszerű támadások, illetve bizonyos információn alapuló támadások között. Az utóbbi esetben feltételezhetjük, hogy a támadó célja a maximális károkozás, a támadott hálózati elem kiválasztását pedig valamilyen villamos vagy fizikai jellemző alapján végzi. Ilyen jellemzők lehetnek a hálózat topológiai paraméterei (tipikusan az adott csomóponthoz kapcsolódó élek száma, az élek központi szerepe), melyek egy gráfrepre-

zentáció segítségével könnyen számíthatók. Több arra utaló munka is napvilágot látott, hogy a legnagyobb köztiséggel rendelkező hálózati elemek támadása nemcsak a véletlenszerűen kiválasztott célpontokhoz képest okoz nagyobb kárt, de a legtöbb esetben alkalmasak az egy támadással kivitelezhető legnagyobb kár okozására is *(Mei–Zhang–Cao 2011b; Wang et al. 2020; Paniraghi–Maity 2020)*. (Gráfok esetén két csomópont köztisége megmutatja, hogy azok milyen messze vannak egymástól, ha egy kijelölt harmadik csomópont érintésével kell az utat megtennünk.) Jelen cikk vizsgálatainak egyik tárgya ennek a hipotézisnek az ellenőrzése valós villamosenergia-hálózati modell használatával.

A fizikai támadások által okozott károk mérésére több, alapvetően a komplex rendszerek területéről származó metrikát használ a szakirodalom, ezek közül a hálózati elrendezés erősségének mérésére a topológiai hatékonyság az egyik legalkalmasabb, melynek alkalmazására több példát találunk valós (Olaszország *[Crucitti–Latora–Marchiori 2004a; Crucitti–Latora–Marchiori 2004b]*, Észak-Amerika *[Kinney et al. 2005]*, Horvátország *[Sičanica–Vujaklija 2020]*, Európa *[Rosato–Bologna–Tiriticco 2007]*) és szintetikus hálózati modellek *(Arianos et al. 2009; Dwivedi–Yu–Sokolowski 2009)* használatával. Fontos hiányossága azonban ezen munkák döntő többségének, hogy nem tesznek különbséget a különböző feszültségszintek között (súlyozatlan gráfot használnak), így pedig nem tudnak teljes képet adni a hálózat valós sérülékenységéről.

Jelen cikk célja, hogy (i) bemutassa Magyarország villamosenergia-hálózatának sérülékenységét véletlenszerű és szándékolt támadásokkal szemben, (ii) hogy összehasonlítsa a különböző támadási stratégiák okozta károkat, és (iii) hogy rámutasson a súlyozatlan és súlyozott reprezentációk használata közötti kvalitatív különbségekre.

Vizsgálati anyag és módszerek

A vizsgálatokhoz Magyarország villamosenergia-hálózatának 2019. évi állapotát használtuk. A gráfreprezentáció elkészítésekor a termelőegységeket, transzformátorokat és alállomásokat csomópontként, a távvezetékeket élként képeztük le. A reprezentáció a 132 kV-os és nagyobb feszültségszintű hálózati elemeket tartalmazza. A topológia elkészítéséhez nyílt adatbázisokat használtunk (vállalati kiadványok, térképek stb.), melyek biztonsági szempontból OSINT (open source intelligence) jellegű információnak tekinthetők. A súlyozott gráf élsúlyainak megállapításához az egyes feszültségszinteken üzemelő távvezetékek tipikus terhelhetőségét használtuk fel, mely szintén több helyen hozzáférhető adat, illetve releváns erősáramú szakismeretekkel jól becsülhető.

Az így létrehozott gráfra kiszámítottuk a csomópontok fokszám-eloszlását, az átlagos fokszámot, az átmérőt, a modularitást, az átlagos úthosszt, valamint a klaszterezési és a kisvilág együtthatókat. Ezek közül a csomópontok fokszáma, illetve a hálózat átmérője általánosan használt gráfelméleti fogalom, így azok definiálásától eltekintünk.

A gráf modularitása, Q megmutatja, hogy a gráf pillanatnyi felosztása mellett hogy viszonyul egymáshoz a csoportosulásokon belül, illetve között futó élek száma az eredeti gráfba:

$$Q = \frac{1}{\langle k \rangle} \sum_{ij} \left(A_{ij} - \frac{k_i k_j}{\langle k \rangle} \right) \delta(g_i, g_j) \qquad (1)$$

ahol $\langle k \rangle$ a csomópontok átlagos fokszáma, A_{ij} a szomszédsági mátrix, $\delta(i,j)$ pedig a Kronecker-delta függvény.

Az átlagos úthossz, L a gráf csomópontjai közötti legrövidebb úthosszak átlaga:

$$L = \frac{1}{N(N-1)} \sum_{j \neq i} d(i,j) \qquad (2)$$

ahol N a csomópontok száma, $d(i,j)$ pedig az i és j csomópontok távolsága. Véletlen gráfok esetén L a következő formulával közelíthető *(Fronczak–Fronczak–Hołyst 2004)*:

$$L_r = \frac{ln(N) - 0{,}5772}{ln\langle k \rangle} + 0{,}5 \qquad (3)$$

A gráf klaszterezési együtthatója, C *(Watts–Strogatz 1998)* definícióját használva:

$$C = \frac{1}{N} \sum_i \frac{2E_i}{k_i(k_i - 1)} \qquad (4)$$

ahol E az i csomópont szomszédjait összekötő élek száma. Véletlen gráfok esetén a klaszterezési együttható az alábbiak szerint közelíthető:

$$C_r = \frac{\langle k \rangle}{N} \qquad (5)$$

A kisvilág együttható, σ kiszámítása (2–5) egyenletek felhasználásával történik *(Fronczak–Fronczak–Hołyst 2004)*:

$$\sigma = \frac{C/C_r}{L/L_r} \qquad (6)$$

Általános megegyezés szerint egy hálózat kisvilág tulajdonsággal rendelkezőnek tekinthető, ha $C << C_r$ és $L \geq L_r$, azaz σ nagyobb egynél.

A hálózatban a támadás hatására bekövetkező károk nagyságát a topológiai hatékonyságban bekövetkező relatív csökkenéssel ($\Delta eff./eff_0$) mértük. A topológiai hatékonyság olyan mutató, mely feltételezi, hogy az i és j csomópontok közötti teljesítményátvitel fordítottan arányos a csomópontok távolságával:

$$eff = \frac{1}{N(N-1)} \sum_{j \neq i} \frac{1}{d(i,j)} \quad (7)$$

A (7) egyenletből látható, hogy a topológiai hatékonyság koncepciója súlyozatlan gráfokra került kialakításra. Ennek a megközelítésnek súlyos hiányossága, hogy nem tesz különbséget az egyes távvezetékek eltérő teljesítményátviteli képességei között; ennek kiküszöbölésére a cikkben a súlyozott topológiai hatékonyságot használjuk:

$$weff = \frac{1}{N(N-1)} \sum_{j \neq i} \frac{1}{wd(i,j)} \quad (8)$$

ahol $wd(i,j)$ az i és j csomópontok közötti súlyozott gráftávolság. A gráf éleinek súlyait az egyes feszültségszintekre jellemző megengedett áramterhelés alapján határoztuk meg, mely értékek rendre, 2000, 1815, 885 és 781 A voltak a 750, 400, 220 és 132 kV-os feszültségszinteken. Az élsúlyok ezen értékek reciprokaként kerültek meghatározásra, így a (8) egyenlet már valóban képes a villamosenergia-rendszer azon sajátosságát is leképezni, hogy egyes vezetékei kitüntetett szerepűek.

A vizsgálatokat támadási stratégia szerint két csoportba rendeztük (egyszeres és kétszeres szimultán támadások), összesen öt esetet vizsgálva (egy csomópont támadása, egy él támadása, két csomópont támadása, két él támadása, kombinált szimultán támadás egy csomópont és egy él ellen), melyek összesen rendre 385, 504, 73920, 128271 és 193797 futtatást tettek szükségessé. A szimulációkat véletlenszerűen és tudatosan kiválasztott célpontokkal is elvégeztük, illetve minden esetben azonosítottuk a legnagyobb kárt okozó támadásokat. A károk súlyozatlan és súlyozott gráf esetére is kiszámításra kerültek a két reprezentáció összehasonlítása érdekében.

Eredmények

1. táblázat | A magyar villamosenergia-hálózat főbb paraméterei

Csomópontok száma		385
Élek száma		504
Vezetékhossz [km]	132 kV	6536
	220 kV	1099
	400 kV	2297
	750 kV	266
Csomópontok átlagos fokszáma	<k>	2,6181
Átlagos úthossz L		6,7353
Klaszterezési együttható C		0,0716
Átmérő d		15
Modularitás Q		0,469
Kisvilág együttható σ		9,5250

Az eredményeket több alfejezetre osztva tárgyaljuk. Elsőként a magyar villamosenergia-hálózat gráftulajdonságait mutatjuk be, majd a hálózat sérülékenységét ismertetjük, egyszeres és kétszeres támadások esetére. Utóbbi két alfejezetben külön tárgyaljuk a véletlenszerű és a célzott támadások hatásait, illetve azonosítjuk a legnagyobb kárt okozó támadásokat is, mind a súlyozatlan, mind a súlyozott gráfreprezentáció esetére.

Gráftulajdonságok

Az *1. táblázat* Magyarország modellezett villamosenergia-hálózatának legfontosabb villamos paramétereit és a gráfreprezentáció tulajdonságait ismerteti. Ezek alapján elmondható, hogy 2019. évi állapotában a hálózat kisvilág tulajdonságot mutatott; az ilyen hálózatok viszonylag kis átlagos úthosszakkal és nagy klaszterezési együtthatókkal rendelkeznek, így a fontos szerepet betöltő alállomások és vezetékek támadása jelentős károkat okozhat.

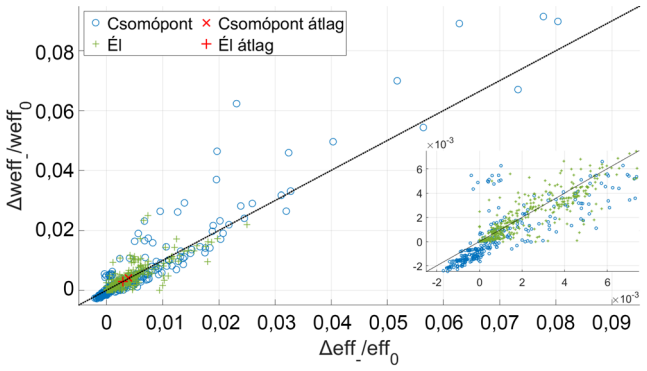
Egyszeres támadás

Az egyszeres támadások által okozott sérülések nagyságát a *2. táblázat* foglalja össze. Megfigyelhető, hogy az egyszeres támadások által okozható károk még a legsúlyosabb esetben sem nagyok; a legfontosabb csomópontok eltávolítása a topológiai hatékonyság 8-9%-os csökkenését okozza, míg élek eltávolításánál ez mindössze 2,5%. A legnagyobb kárt okozó támadások hatása kb. egy nagyságrenddel nagyobb a véletlen támadásokhoz viszonyítva, utóbbiak pedig 1% alatti hatással bírnak. Ezek az eredmények alátámasztják az előző alfejezet megállapítását a magyar villamosenergia-hálózat kisvilág tulajdonságát illetően. Amennyiben a célzott támadások hatásait vizsgáljuk, érdemi különbséget láthatunk a csomópontok és az élek ellen intézett támadások között. Előbbi esetben a gráfot jellemző köztiség mutató segítségével a súlyozatlan reprezentáció esetén sikerült a legsérülékenyebb elemet kiválasztani, és a súlyozott reprezentáció esetén is közel jártunk ehhez. Ezzel szemben, ha a köztiség alapján választjuk ki a támadandó élt, a maximálisan okozható kár felét sem érjük el.

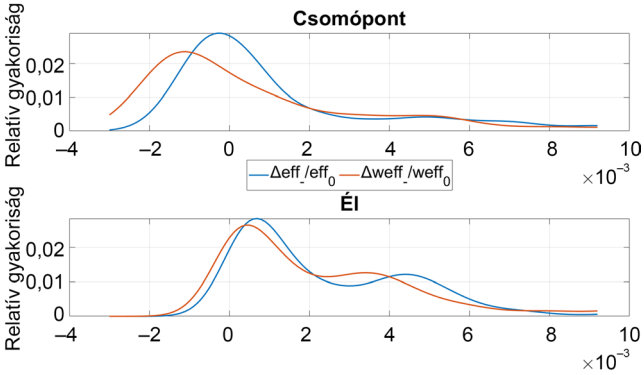
Amennyiben célpontok szempontjából vizsgáljuk a támadásokat, megállapítható, hogy a legsérülékenyebb csomópontok a súlyozatlan és a súlyozott reprezentáció esetében gyakorlatilag azonosak: a 220 és 400 kV-os át-

2. táblázat | Egyszeres támadások által okozott sérülések

Támadás típusa	Egyszeres csomópont		Egyszeres él	
Kár	$\Delta eff./eff_0$	$\Delta weff./eff_0$	$\Delta eff./eff_0$	$\Delta weff./eff_0$
Véletlen támadás	0,0039	0,0041	0,0029	0,0028
Célzott támadás	0,0804	0,0898	0,0121	0,0144
Maximális kár	0,0804	0,0915	0,0250	0,0249



1. ábra | Súlyozatlan és súlyozott reprezentáció összehasonlítása egyszeres támadás esetén



2. ábra | Az egyszeres támadások által okozott károk sűrűségfüggvényei, konvolúciós szűrő használatával

viteli hálózat azon alállomásai, melyekhez sok vezeték kapcsolódik. Megtalálható közöttük a legnagyobb fokszámú hálózati csomópont, de az esetek többségében fontosabb szerepet játszik, hogy földrajzi értelemben az ország közepén helyezkednek el. Az élek elleni támadások hatása nagyobb szórást mutat. A súlyozatlan gráfreprezentáció használata esetén a legnagyobb sérüléseket látszólag jelentéktelen 132 kV-os vezetékek eltávolítása okozza. Ennek oka, hogy ezen élek eltávolítása a gráf több részre eséséhez vezet, szigetüzemű ellátási területeket létrehozva. A súlyozott reprezentáció esetében viszont az öt legsúlyosabb támadásból már csak kettő ilyen jellegű, a fennmaradó három esetben vagy központi szerepű 400 kV-os vezetékről van szó, vagy a 400 és 132 kV-os rendszert összekötő hurkolásról. Megfigyelhető továbbá, hogy ha a támadó a köztiségmutató értéke alapján kívánja a célpontot kiválasztani, az előbb említett öt elem közül csak egyet tud azonosítani, négy esetben pedig kevésbé fontos vezetéket választana ki. Az eredmények is igazolják, hogy a magyarországi 400 kV-os hálózat egyszeres vezetékkiesések ellen védett, és az ilyen célú támadások sem tudnának érdemi károkat okozni.

A súlyozatlan és a súlyozott reprezentációk eredményeinek összehasonlítását az *1. ábra* alapján végezzük el, melyen minden egyszeres támadás feltüntetésre került. Látható, hogy csomóponti támadások esetén a súlyozott reprezentáció szerint mért károk nagyobbak, mint a súlyozatlan szerintiek (az adatpontokra illesztett egyenes meredeksége 1,15), míg vezetékek elleni támadások esetén fordított a helyzet (0,9-es meredekség). Érdekesség továbbá, hogy csomóponti támadások esetén negatív változások is előfordulnak. Ez azt jelenti, hogy bizonyos csomópontok eltávolítása esetén a gráf topológiai hatékonysága javul; az ebbe a csoportba tartozó csomópontok jellemzően a 132 kV-os hálózat egyetlen összeköttetéssel rendelkező alállomásai.

A támadások által okozott károk sűrűségfüggvényeit konvolúciós (Kernel) szűrő használatával ábrázoltuk *(2. ábra)*. Az eredmények egyrészt vizuálisan is megerősítik a súlyozatlan és a súlyozott reprezentációk közötti különbségek meglétét, másrészt fontos információt tartalmaznak az eloszlások jellegéről is. A csomópontok elleni támadások unimodális jellegűek (azaz jellemzően bármely csomópont támadása hasonló nagyságú kárt okoz), az élek elleni támadások azonban enyhe bimodalitást mutatnak. Utóbbiból arra következtethetünk, hogy azonosítható a távvezetékeknek egy csoportja, mely topológiai hatékonyság szempontjából kulcsfontosságú szerepet játszik.

Kétszeres támadás

A két elem szimultán támadása által okozott sérülések nagyságát a *3. táblázat* foglalja össze. A *2. táblázattal* összehasonlítva megállapítható, hogy a kétszeres támadások körülbelül kétszer akkora kárt okoznak, mint az egyszeresek. A csomópontok elleni támadások a topológiai hatékonyság 16–25%-os csökkenését eredményezik, míg élek esetén 5%-nál nagyobb értékkel nem találkozunk. Kombinált, egy csomópontot és egy élt érintő támadás hatására 14–21%-kal csökkenhet a topológiai hatékonyság. A csomópontok ellen végrehajtott véletlenszerű és maximális kárt okozó támadások hatása között több mint egy nagyságrendnyi a különbség. (Érdemes megjegyezni, hogy két véletlenszerűen kiválasztott

3. táblázat | Kétszeres támadások által okozott sérülések

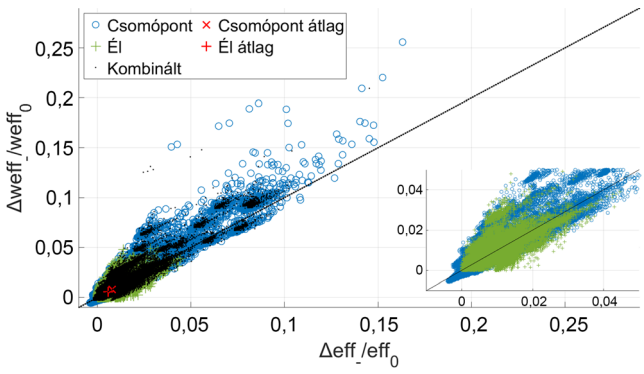
Támadás típusa	Kétszeres csomópont		Kétszeres él		Kombinált csomópont+él	
Kár	$\Delta eff_/eff_0$	$\Delta weff_/eff_0$	$\Delta eff_/eff_0$	$\Delta weff_/eff_0$	$\Delta eff_/eff_0$	$\Delta weff_/eff_0$
Véletlen támadás	0,0079	0,0082	0,0058	0,0058	0,0068	0,0070
Célzott támadás	0,1196	0,1366	0,0159	0,0232	0,0811	0,0903
Maximális kár	0,1631	0,2557	0,0445	0,0490	0,1454	0,2094

csomópont támadása a rendszer egésze szempontjából nem okoz érdemben nagyobb kárt, mint egy véletlenszerűen kiválasztott csomópont támadása.) A köztiség értéke alapján kiválasztott célpontok elleni támadások ebben az esetben nem érik el a maximálisan lehetséges károkozást.

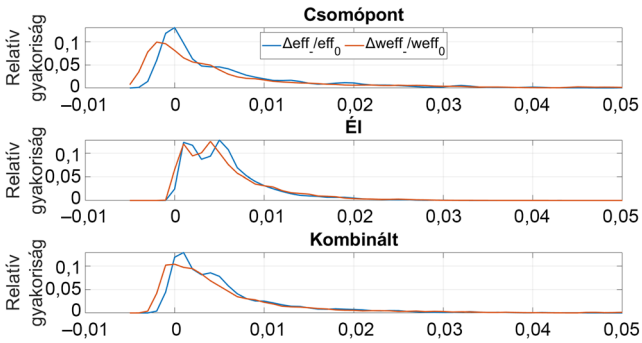
Az eredményeket a célpontok szempontjából vizsgálva azt láthatjuk, hogy a legnagyobb károkat okozó csomópontok elleni támadások mutatnak némi átfedést a súlyozatlan és a súlyozott reprezentációk esetén, de érdemi különbségek is találhatók. A csomópont-párok gráfelméleti értelemben vett távolsága jellemzően 1 vagy 2, ami az n–1 elv mentén kialakított hurkolt topológia gyenge pontjára világít rá, azaz hogy egyszeres kiesésekkel képes jól megbirkózni, de ha a hurkot több ponton felhasítjuk, az a topológiai hatékonyság érdemi csökkenését eredményezi.

Érdekes jelenség figyelhető meg az élek elleni támadások esetén: jóllehet a súlyozatlan és a súlyozott reprezentáció használatával is hasonló nagyságú károk mérhetők, az azokat kiváltó okok eltérőek. Súlyozatlan esetben az egyszeres támadásoknál már említett szigetüzemet létrehozó, 132 kV-os vezetékek elleni támadások vezetnek nagy károkhoz, míg a súlyozott esetben a 400 kV-os hurkok felhasítása. A köztiség alapján kiválasztott célpontok minden esetben egymáshoz földrajzi szempontból közel elhelyezkedő vezetékek (mely egyben kis gráftávolságot is feltételez). Fontos információ azonban, hogy ezek a kétszeres él elleni támadások még mindig kisebb kárt okoznak, mint az éleket összekötő csomópont elleni egyszeres támadások.

A csomópontok és élek elleni kombinált támadások eredményei jól mutatják, hogy a csomópontok játsszák az elsődleges szerepet; a legnagyobb kárral járó támadások kb. 80%-ánál az ország két központi alállomásának egyike érintett. További érdekes megállapítása a célpontok vizsgálatának, hogy a kombinált támadások inkább az ország Dunától keletre eső területein okozhatnak károkat.



3. ábra Súlyozatlan és súlyozott reprezentáció összehasonlítása kétszeres támadás esetén



4. ábra A kétszeres támadások által okozott károk sűrűségfüggvényei, konvolúciós szűrő használatával

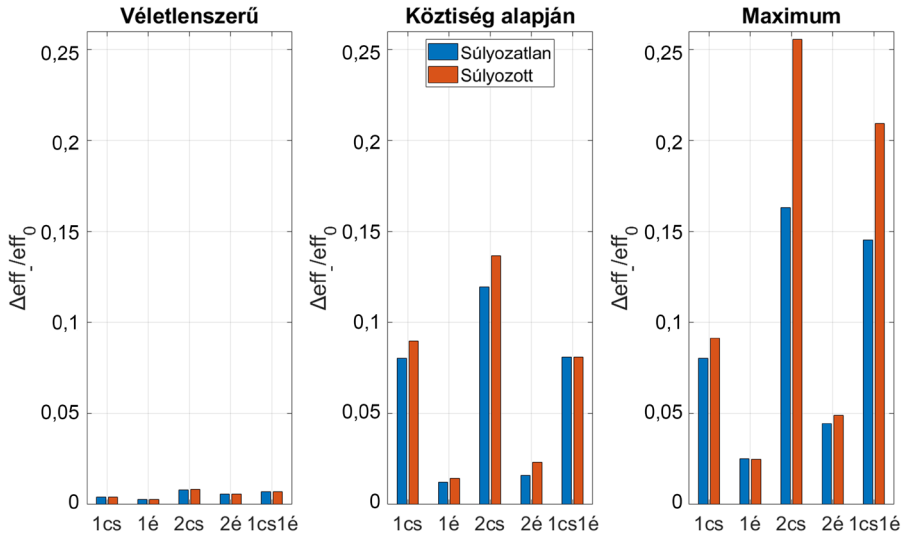
A *3. ábra* a súlyozatlan és a súlyozott reprezentációk közötti különbségeket mutatja. Csomópontok elleni támadásoknál ismét a súlyozott változaton mérhető károk nagyobbak (az adatpontokra illesztett egyenes meredeksége 1,15), élek esetén pedig fordított összefüggés áll fenn (0,9-es meredekség). A kombinált támadások az ábrán megfigyelhető módon elsősorban bizonyos kiemelt fontosságú csomópontok körül sűrűsödnek, a támadásban érintett él másodlagos fontosságú a kár szempontjából.

A kétszeres támadások által okozott károk sűrűségfüggvényeit konvolúciós szűrő használatával ábrázoltuk *(4. ábra)*. Az egyszeres esetekhez hasonlóan a csomópontok elleni támadások hatása unimodális jelleget mutat, de 0,005 értékű kár alatt enyhe plató is található. Az élek támadása által okozott károk bimodálisak, mely rámutat a fontosabb (400 kV) és kevésbé fontos (132 kV) hálózati elemek eltérő modellezésének (és így a súlyozott reprezentációk használatának) fontosságára. A kombinált támadásokra jellemző sűrűségfüggvények az előbbi két eset tulajdonságait ötvözik, illetve arra is utalnak, hogy a súlyozott reprezentáció használata erősíti a csomópontok súlyát a numerikus eredményekben.

Diszkusszió

Az *5. ábra* a megelőző alfejezetek eredményeit foglalja össze grafikus formában. Az ábrán megfigyelhető, hogy a véletlenszerűen kiválasztott célpontok elleni támadások minden esetben sokkal kisebb kárt okoznak a célzott támadásoknál. Ezek az eredmények alátámasztják, hogy a magyar villamosenergia-rendszer kisvilág tulajdonságot mutat, ami fontos információ a sérülékenységi és kockázati tervek készítésekor. Az ábrán az is látható, hogy amennyiben a támadás célpontját a köztiség paraméter nagysága alapján választjuk ki, általában nem sikerült maximális kárt okoznunk; az egyetlen kivételt az egyszeres, csomópont elleni támadás jelenti, ahol a legnagyobb fokszámú csomópont támadása vezet a topológiai hatékonyság legnagyobb mértékű csökkenéséhez.

A kutatás során vizsgáltuk azt is, hogy mely célpontok esetén van a legnagyobb eltérés a súlyozatlan és a súlyozott gráfreprezentáción mért kár között. Minden táma-



5. ábra | A támadások által okozott károk összefoglalása

dás esetére kiszámítottuk a károk arányát, majd ezen értékekből átlagos százalékos abszolút hibaértékeket (Mean Average Percentange Error, MAPE) számoltunk.

Egyszeres, csomópont elleni támadásoknál a MAPE 2,69 volt, a legnagyobb eltérések pedig 49,70 és 84,71 között mozogtak, azonban ezek között csak egyetlen 400 kV-os hálózatelem volt található. Egyszeres, él elleni támadások esetén a MAPE értéke 0,44, maximuma 2,85 és 7,77 közötti. Az értékek ismét rámutatnak arra, hogy a súlyozott reprezentáció használata az élek elleni támadások vizsgálatakor kevesebb többlet információval bír. Ugyanakkor a legnagyobb eltérések kivétel nélkül 400 kV-os távvezetékekhez tartoztak, így a modell érzékenységének további vizsgálata is szükséges lehet.

A kétszeres, csomópont elleni támadásoknál a MAPE 20,65 volt, a legnagyobb eltérések pedig szélsőséges értékeket vettek fel (1179551), azonban érdemi tendenciák nem voltak kiolvashatóak az eredményekből. A kétszeres, él elleni támadások esetén a MAPE 0,36 volt, a legnagyobb különbségek pedig 47,8 és 63,97 között mozogtak. Utóbbi csoportba általában olyan vezetékek kerültek, melyek egymáshoz közeli pontokat kötnek össze (nemritkán városon belüli vezetékekről beszélhetünk). Végül, a kombinált támadások esetén a 3,27-es MAPE mellett ismét kiugró maximumokkal (10656–48132) találkoztunk.

Az előzőekben ismertetett numerikus eredmények összefoglalásaként elmondható, hogy amikor eltért a súlyozatlan és a súlyozott reprezentáción számolt károk nagysága, akkor is ritkán érintett ez fontos hálózati elemet. Ez alapján feltételezhető, hogy a véletlenszerűn kiválasztott célpontok elleni támadások hatásának felmérésekor nem okoz érdemi hibát a súlyozatlan reprezentáció használata. Ezzel szemben a legnagyobb kárt okozó támadások értékelésénél már jelentős különbségek alakultak ki, így ezek tárgyalásakor mindenképpen érdemes a súlyozott reprezentációval dolgozni.

Konklúziók

A cikk a magyar villamosenergia-rendszer véletlenszerűen és célzottan kiválasztott elemei elleni támadások által okozott károkat vizsgálta szimulációk segítségével. A károkozás mértékét a topológiai hatékonyság csökkenése adta, míg a hálózat topológiáját súlyozatlan és súlyozott gráfreprezentációk képezték le. Öt különböző támadási típus (egy csomópont támadása, egy él támadása, két csomópont támadása, két él támadása, kombinált szimultán támadás egy csomópont és egy él ellen) összes lehetséges esetét megvizsgáltuk, kiszámítva az okozott károkat. Egyetlen véletlenszerűen kiválasztott csomópont vagy él eltávolítása mindössze átlagosan 0,3–0,4%-kal csökkentette a topológiai hatékonyságot, és még a kétszeres támadások esetén is csak 0,6–0,8% között mozgott ez az érték. A súlyozatlan és a súlyozott gráfreprezentációk összehasonlítása rámutatott, hogy előbbi az élek, utóbbi a csomópontok elleni támadások által okozott károkat hajlamos nagyobbra értékelni, ugyanakkor általános trendek nem voltak megfigyelhetők. A súlyozott reprezentációk használata mellett szól ugyanakkor, hogy a fontos hálózati elemek (elsősorban a 400 kV-os feszültségszint) elleni támadásoknál jelentősen eltérő károk voltak mérhetők egyik és másik gráfmodell használata esetén.

Kutatásainkat a jövőben kiterjesztjük más országok villamosenergia-hálózataira, illetve a többszörös támadások esetén vizsgálni kívánjuk annak hatását, ha a célpontok nem szimultán, hanem szekvenciális módon kerülnek kiválasztásra, a gráftulajdonságok újraszámolásával.

Irodalomjegyzék

Albert, R., Albert, I., & Nakarado, G. L. (2004) Structural vulnerability of the North American power grid. Physical Review E, Vol. 69. No. 2. DOI: https://link.aps.org/doi/10.1103/PhysRevE.69.025103

Arianos, S., Bompard, E., Carbone, A., & Xue, F. (2009) Power grid vulnerability: A complex network approach. Chaos: An Interdisciplianry Journal of Nonlinear Science, Vol. 19. No. 1. DOI: https://doi.org/10.1063/1.3077229

Aziz, T., Lin, Z., Waseem, M., & Liu, S. (2020) Review on optimization methodologies in transmission network reconfiguration of power systems for grid resilience. International Transactions on Electrical Energy Systems, Vol. 31. No. 3. DOI: https://doi.org/10.1002/2050-7038.12704

Beyza, J., Garcia-Paricio, E., Ruiz, H. F., & Yusta, J. M. (2020) Geodesic Vulnerability Approach for Identification of Critical Buses in Power Systems. Journal of Modern Power Systems and Clean Energy, Vol. 8. pp. 727–736. DOI: https://doi.org/10.35833/MPCE.2018.000779

Bompard, E., Napoli, R., & Xue, F. (2009) Analysis of structural vulnerabilities in power transmission grids. International Journal of Critical Infrastructure Protection, Vol. 2., No. 1–2. pp. 5–12. DOI: https://doi.org/10.1016/j.ijcip.2009.02.002

Bompard, E., Wu, D., & Xue, F. (2010) The concept of betweenness in the analysis of power grid vulnerability. Proc. Complexity in Engineering, 2010 (COMPENG'10), Rome, Italy, 22–24 February 2010, pp. 52–54. DOI: https://doi.org/10.1109/COMPENG.2010.10

Brummitt, C. D., D'Souza, R. M., & Leicht, R. (2012) Suppressing cascades of load in interdependent networks. Proceedings of the National Acemy of the United States of America, Vol. 109. No. 12. E680–E689, DOI: https://doi.org/10.1073/pnas.1110586109

Chassin, D. P., & Posse, C. (2005) Evaluating North American electric grid reliability using the Barabási–Albert network model. Physica A, Vol. 355. No. 2–4. pp. 667–677. DOI: https://doi.org/10.1016/j.physa.2005.02.051

Chen, Z., Zhu, J., Li, S., & Luo, T. (2020) Detection of False Data Injection Attack in Automatic Generation Control System with Wind Energy based on Fuzzy Support Vector Machine. Proc. IECON 2020 The 46th Annual Conference of the IEEE Industrial Electronics Society, Singapore, 2020, pp. 3523–3528. DOI: https://doi.org/10.1109/IECON43393.2020.9255020

Crucitti, P., Latora, V., & Marchiori, M. (2004a) A topological analysis of the Italian electric power grid. Physica A, Vol. 338. No. 1–2. pp. 92–97. DOI: https://doi.org/10.1016/j.physa.2004.02.029

Crucitti, P., Latora, V., & Marchiori, M. (2004b) Model for cascading failures in complex networks. Physical Review E, Vol. 69. No. 4. DOI: https://link.aps.org/doi/10.1103/PhysRevE.69.045104

Crucitti, P., Latora, V., Marchiori, M. (2005) Locating critical lines in high-voltage electrical power grids. Fluctuation and Noise Letters, Vol. 5. No. 2. L201–L208, DOI: https://doi.org/10.1142/S0219477505002562

Cuadra, L., Salcedo-Sanz, S., Ser, J., Jiménez-Fernández, S., & Geem, Z. W. (2015) A Critical Review of Robustness in Power Grids Using Complex Networks Concepts. Energies, Vol. 8. No. 9. pp. 9211–9265. DOI: https://doi.org/10.3390/en8099211

Dwivedi, A., Yu, X., & Sokolowski, P. (2009) Identifying vulnerable lines in a power network using complex network theory. Proc. IEEE International Symposium on Industrial Electronics (ISIE 2009), Seoul, Korea, 5–8 July 2009, pp. 18–23. DOI: https://doi.org/10.1109/ISIE.2009.5214082

Dwivedi, A., Yu, X., & Sokolowski, P. (2010) Analyzing power network vulnerability with maximum flow based centrality approach. Proc. 8th IEEE International Conference on Industrial Informatics (INDIN), Osaka, Japan, 1–16 July 2010, pp. 336–341. DOI: https://doi.org/10.1109/INDIN.2010.5549398

Edib, S. N., Lin, Y., Vokkarane, V., Qiu, F., Yao, R., & Zhao, D. (2020) PMU and Communication Infrastructure Restoration for Post-Attack Observability Recovery of Power Grids. Proc. 2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Tempe, AZ, USA, 2020, pp. 1–6. DOI: https://doi.org/10.1109/SmartGridComm47815.2020.9303014

Európai Parlament és Tanács (2019) Az Európai Parlament és a Tanács (EU) 2019/941 rendelete (2019. június 5.) a villamosenergia-ágazati kockázatokra való felkészülésről és a 2005/89/EK irányelv hatályon kívül helyezéséről

Európai Unió (2017) A Bizottság (EU) 2017/1485 rendelete (2017. augusztus 2.) a villamosenergia-átviteli hálózat üzemeltetésére vonatkozó iránymutatás megalkotásáról.

Fang, J., Wu, J., Zheng, Z., & Tse, C. K. (2021) Revealing Structural and Functional Vulnerability of Power Grids to Cascading Failures. IEEE Journal on Emergingand Selected Topics in Cirtuits and Systems, Vol. 11. No. 1. pp. 133–143. DOI: https://doi.org/10.1109/JETCAS.2020.3033066

Fronczak, A., Fronczak, P., & Hołyst, J. A. (2004) Average path length in random networks. Physical Review E, Vol. 70. No. 5. DOI: https://link.aps.org/doi/10.1103/PhysRevE.70.056110

Galindo-González, C. C., Angulo-Garcia, D., & Osorio, G. (2020) Decreased resilience in power grids under dynamically induced vulnerabilities. New Journal of Physics, Vol. 22. DOI: https://doi.org/10.1088/1367-2630/abb962

Gao, X., Pu, C., & Li, L. (2020) Vulnerability assessment of power grids against cost-constrained hybrid attacks. IEEE Transactions on Circuits and Systems II, Vol. 68. No. 4. pp. 1477–1481. DOI: https://doi.org/10.1109/TCSII.2020.3033545

Ghafouri, M., Au, M., Kassouf, M., Debbabi, M., Assi, C., & Yan, J. (2020) Detection and Mitigation of Cyber Attacks on Voltage Stability Monitoring of Smart Grids. IEEE Transactions on Smart Grid, Vol. 11. No. 6. pp. 5227–5238. DOI: https://doi.org/10.1109/TSG.2020.3004303

Gouhua, Z., Ce, W., Jianhua, Z., Jingyan, Y., Yin, Z., & Manyin, D. (2008) Vulnerability assessment of bulk power grid based on complex network theory. Proc. Third International Conference on Electric Utility Deregulation and Restructuring and Power Technologies (DRPT 2008), Nanjuing, China, 6–9 April 2008, pp. 1554–1558. DOI: https://doi.org/10.1109/DRPT.2008.4523652

Han, P., & Zhang, S. (2011) Analysis of cascading failures in small-world power grid. International Journal of Energy Science, Vol. 1. No. 2. pp. 99–104.

He, Z., Jiang, F., Qian, F., Li, F., Yuan, X., Sang, Z., & Xie, Y. (2020) Defense Resources Optimization for AC-DC Hybrid System Against the Coordination Attack of False Data Injection Attack and Physical Attack. Proc. 2020 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia), Weihai, China, 2020, pp. 657–662. DOI: https://doi.org/10.1109/ICPSAsia48933.2020.9208447

Hines, P., Blumsack, S., Sanchez, E. C., & Barrows, C. (2010) The topological and electrical structure of power grids. Proc. 43th Hawaii International Conference on System Sciences (HICSS), Honolulu, HI, USA, 5–8 January 2010, pp. 1–10. DOI: https://doi.org/10.1109/HICSS.2010.398

Holmgren, Å. J. (2006) Using graph models to analyze the vulnerability of electric power networks. Risk Analysis, Vol. 26. No. 4. pp. 955–969. DOI: https://doi.org/10.1111/j.1539-6924.2006.00791.x

Holmgren, Å. J., Jenelius, A., & Westin, J. (2007) Evaluating strategies for defending electric power networks against antagonistic attacks. IEEE Transactions on Power Systems, Vol. 22. No. 1. pp. 76–84. DOI: https://doi.org/10.1109/TPWRS.2006.889080

Jin, M., Lavaei, J., Sojoudi, S., & Baldick, R. (2021) Boundary Defense Against Cyber Threat for Power System State Estimation. IEEE Transactions on Information Forensics and Security, Vol. 16., pp. 1752–1767. DOI: https://doi.org/10.1109/TIFS.2020.3043065

Khare, G., Mohapatra, A., & Singh, S. N. (2021) A Real-Time Approach for Detection and Correction of False Data in PMU Measurements. Electric Power Systems Research, Vol. 191. DOI: https://doi.org/10.1016/j.epsr.2020.106866

Kinney, R., Crucitti, P., Albert, R., & Latora, V. (2005) Modeling cascading failures in the North American power grid. The European Physical Journal B, Vol. 46., pp. 101–107. DOI: https://doi.org/10.1140/epjb/e2005-00237-9

Lesieutre, B., Borden, A., & Ramanathan, P. (2020) Preserving Confidentiality of Critical Energy Infrastructure Information. Principles of Cyber-Physical Systems: An Interdisciplinary Approach. Cambridge University Press. DOI: https://doi.org/10.1017/9781107588981

Liu, Z., & Wang, L. (2021) Leveraging Network Topology Optimization to Strengthen Power Grid Resilience Against Cyber-Physical Attacks. IEEE Transactions on Smart Grid, Vol. 12. No. 2. pp. 1552–1564. DOI: https://doi.org/10.1109/TSG.2020.3028123

Long, X., & Chen, C. (2020) Study on the Vulnerability of Power Grid Cascade Failures Based on Complex Network Theory. In: Jia Y., Zhang W., Fu Y. (eds) Proceedings of 2020 Chinese Intelligent Systems Conference. CISC 2020. Lecture Notes in Electrical Engineering, Vol. 706., pp. 307–315. DOI: https://doi.org/10.1007/978-981-15-8458-9_33

Mei, S., Zhang, X., & Cao, M. (2011a) Complex Small-World Power Grids. Power Grid Complexity, pp. 161–178. DOI: https://doi.org/10.1007/978-3-642-16211-4_5

Mei, S., Zhang, X., & Cao, M. (2011b) Power grid growth and evolution. *Power Grid Complexity*, pp. 133–160. DOI: https://doi.org/10.1007/978-3-642-16211-4_4

Pace, G. D., Wang, Z., Benin, J., He, H., & Sun, Y. (2020) Evaluation of Communication Delay Based Attack Against the Smart Grid. Proc. 2020 IEEE Kansas Power and Energy Conference (KPEC), Manhattan, KS, USA, 2020, pp. 1–6. DOI: https://doi.org/10.1109/KPEC47870.2020.9167543

Pagani, G. A., & Aiello, M. (2011) Towards decentralization: A topological investigation of the medium and low voltage grids. IEEE Transactions on Smart Grid, Vol. 2. No. 3. pp. 538–547. DOI: https://doi.org/10.1109/TSG.2011.2147810

Pahwa, S., Hodges, A., Scoglio, C., & Wood, S. (2010) Topological analysis of the power grid and mitigation strategies against cascading failures. Proc. 4th Annual IEEE Systems Conference, San Diego, CA, USA, 5–8 April 2010, pp. 272–276. DOI: https://doi.org/10.1109/SYSTEMS.2010.5482329

Panigrahi, P., & Maity, S. (2020) Structural vulnerability analysis in small-world power grid networks based on weighted topological model. International Transactions on Electrical Energy Systems, Vol. 30. No. 7. e12401, DOI: https://doi.org/10.1002/2050-7038.12401

Pepyne, D. L. (2007) Topology and cascading line outages in power grids. Journal of Systems Science and Systems Engineering, Vol. 16. pp. 202–221. DOI: https://doi.org/10.1007/s11518-007-5044-8

Rajkumar, V. S., Tealane, M., Ştefanov, A., Presekal, A., & Palensky, P. (2020) Cyber Attacks on Power System Automation and Protection and Impact Analysis. Proc. 2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), The Hague, Netherlands, pp. 247–254. DOI: https://doi.org/10.1109/ISGT-Europe47291.2020.9248840

Rosas-Casals, M., Bologna, S., Bompard, E., D'Agostino, G., Ellens, W., Pagani, G.A, Scala, A, & Verma, T. (2015) Knowing power grids and understanding complexity science. International Journal of Critical Infrastructures, Vol. 11. No. 1. pp. 4–14. DOI: https://dx.doi.org/10.1504/IJCIS.2015.067399

Rosas-Casals, M., Valverde, S., & Solé, R. V. (2007) Topological vulnerability of the European power grid under errors and attacks. International Journal of Bifurcation and Chaos, Vol. 17. No. 7. pp. 2465–2475. DOI: https://doi.org/10.1142/S0218127407018531

Rosato, V., Bologna, S., & Tiriticco, F. (2007) Topological properties of high-voltage electrical transmission networks. Electric Power Systems Research, Vol. 77. No. 2. pp. 99–105. DOI: https://doi.org/10.1016/j.epsr.2005.05.013

Saraswat, G., Rui, Y., Yajing, L., & Yingchen Z. (2020) Analyzing the Effects of Cyberattacks on Distribution System State Estimation: Preprint, United States: N. p., 2020. Web. https://www.osti.gov/biblio/1737538

Sharma, D., Lin, C., Luo, X., Wu., D., Thulasiraman, K., & Jiang, J.N. (2020) Advanced techniques of power system restoration and practical applications in transmission grids. Electric Power Systems Research, Vol. 182., 106238, DOI: https://doi.org/10.1016/j.epsr.2020.106238

Shen, M., Gao, X., & Peng, M. (2020) Effects of Malware Attacks on the Cascading Failure of Cyber-physical Power System. Journal of Physics, Conference Series, 1624, 062005, DOI: https://doi.org/10.1088/1742-6596/1624/6/062005

Sičanica, Z., & Vujaklija, I. (2020) Resilience to cascading failures. A complex network approach for analysing the Croatian power grid. Proc. 2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO), Opatija, Croatia, 2020, pp. 918–922. DOI: https://doi.org/10.23919/MIPRO48935.2020.9245160

Singh, N. K., & Mahajan, V. (2020) Analysis and Evaluation of Cyber-attack Impact on Critical Power System Infrastructure. Smart Science, Vol. 9. pp. 1–13. DOI: https://doi.org/10.1080/23080477.2020.1861502

Solé, R. V., Rosas-Casals, M., Corominas-Murtra, B., & Valverde, S. (2008) Robustness of the European power grids under intentional attack. Physical Review E, Vol. 77. No. 2. 026102, DOI: https://link.aps.org/doi/10.1103/PhysRevE.77.026102

Tu, H., Shen, H-L., & Xia, Y. (2020) Cascading Failures of Power System with the Consideration of Cyber Attacks. Proc. 2020 IEEE International Symposium on Circuits and Systems (ISCAS), Sevilla, pp. 1–4. DOI: https://doi.org/10.1109/ISCAS45731.2020.9180816

Wang, G., Kong, X., Zhu, C., Xu, J., & Cao, Y. (2010) Identification of key lines in complex power grid based on power flow entropy. Proc. 2010 China International Conference on Electricity Distribution (CICED), Nanjing, China, 13–16 September 2010, pp. 1–6.

Wang, J. W., & Rong, L. L. (2009) Cascade-based attack vulnerability on the US power grid. Safety Science, Vol. 47. No. 10. pp. 1332–1336. DOI: https://doi.org/10.1016/j.ssci.2009.02.002

Wang, W., Song, Y., Li, Y., & Jia, Y. (2020) Research on Cascading Failures Model of Power Grid Based on Complex Network. Proc. 2020 Chinese Control And Decision Conference (CCDC), Hefei, China, 2020, pp. 1367–1372. DOI: https://doi.org/10.1109/CCDC49329.2020.9164048

Wang, Z., Scaglione, A., & Thomas, R. J. (2010) The node degree distribution in power grid and its topology robustness under random and selective node removals. Proc. 2010 IEEE International Conference on Communications Workshops (ICC), Capetown, South Africa, 23–27 May 2010, pp. 1–5. DOI: https://doi.org/10.1109/ICCW.2010.5503926

Watts, D., & Strogatz, S. (1998) Collective dynamics of 'small-world' networks. Nature, Vol. 393. pp. 440–442. DOI: https://doi.org/10.1038/30918

Wu, Y., Chen, J., Ru, Y., Xu, H., Roger, M., & Ni, M. (2020) Research on Power Communication Network Planning Based on Information Transmission Reachability Against Cyber-Attacks. IEEE Systems Journal, Early Access, Vol. 15. No. 2. pp. 2883–2894. DOI: https://doi.org/10.1109/JSYST.2020.3026997

Xiong X., Sun, D., Hao, S., Lin, G., & Li, H. (2020) Detection of False Data Injection Attack Based on Improved Distortion Index Method. Proc. 2020 IEEE 20th International Conference on Communication Technology (ICCT), Nanning, China, 2020, pp. 1161–1168. DOI: https://doi.org/10.1109/ICCT50939.2020.9295794

Zhou, X., Canady, R., Li, Y., Koutsoukos, X., & Gokhale, A. (2020) Overcoming Stealthy Adversarial Attacks on Power Grid Load Predictions Through Dynamic Data Repair. In: Darema F., Blasch E., Ravela S., Aved A. (eds) Dynamic Data Driven Applications Systems. DDDAS 2020. Lecture Notes in Computer Science, Vol. 12312., Springer, Cham., pp. 102–109. DOI: https://doi.org/10.1007/978-3-030-61725-7_14