Structural Safety 31 (2009) 157–167

Contents lists available at ScienceDirect

Structural Safety

journal homepage: www.elsevier.com/locate/strusafe

Cascading failures in complex infrastructure systems

Leonardo Dueñas-Osorio *, Srivishnu Mohan Vemuru

Department of Civil and Environmental Engineering, Rice University, 6100 Main Street, MS-318, Houston, TX 77005, United States

ARTICLE INFO

Article history
Available online 13 August 2008

Keywords:
Network flows
Cascading failures
Complex topology
Multiple hazards
Infrastructure reliability
Flow congestion

ABSTRACT

This paper studies the effect of cascading failures in the risk and reliability assessment of complex infrastructure systems. Conventional reliability assessment for these systems is limited to finding paths between predefined components and does not include the effect of increased flow demand or flow capacity. Network flows are associated with congestion-based disruptions which can worsen path-based predictions of performance. In this research, overloads due to cascading failures are modeled with a tolerance parameter α that measures network element flow capacity relative to flow demands in practical power transmission systems. Natural hazards and malevolent targeted disruptions constitute the triggering events that evolve into widespread failures due to flow redistribution. It is observed that improvements in network component tolerance alone do not ensure system robustness or protection against disproportionate cascading failures. Topological changes are needed to increase cascading robustness at realistic tolerance levels. Interestingly, targeted topological disruptions of a small fraction of network components can affect system-level performance more severely than earthquake or lightning events that trigger similar fractions of element failure. Also, regardless of the nature of the hazards, once the triggering events that disrupt the networks under investigation occur, the additional loss of performance due to cascading failures can be orders of magnitude larger than the initial loss of performance. These results reinforce the notion that managing the risk of network unavailability requires a combination of redundant topology, increased flow carrying capacity, and other non-conventional consequence reduction strategies, such as layout homogenization and the deliberate inclusion of weak links for network islanding. Furthermore, accepted ideas that rare loss of performance events occur exponentially less frequent as the performance reduction intensifies contrast with more frequent network vulnerabilities that result from initial hazard-induced failures and subsequent cascading-induced failure effects. These compound hazard-cascading detrimental effects can have profound implications on infrastructure failure prevention strategies.

1. Introduction

This study quantifies the effects of natural hazards and targeted disruptions on the risk and reliability of complex infrastructures. A key feature of the performance assessment approach implemented in this work is the inclusion of *cascading* failures in addition to the traditional path-based method for network reliability analysis, which is limited to finding connecting paths among system components.

Infrastructure systems and their flow demands are growing at a rate that is outpacing the efforts to upgrade flow capacity and maintain safety margins. In addition, infrastructure systems are becoming more interdependent and failures within a given system are more likely to impact the performance of other systems [1–5]. These reduced safety margins and increased interdependencies make performance evaluation of lifeline systems less tractable. Additionally, the interactions among network constituent components operating at different flow-to-capacity regimens make networked systems more complex. In fact, modern infrastructures exhibit the hallmark properties of so-called complex systems: large number of interacting components, emergent properties difficult to anticipate from the knowledge of single components, adaptability to absorb random disruptions, and highly vulnerable to widespread failure under adverse conditions [6,7].

Power transmission grids are used in this research as examples of engineered complex systems [8,9]. Transmission grids display high voltage power lines in a mesh-like configuration, while distribution grids have radial topologies with low-voltage power lines. Power system reliability evaluation in transmission or distribution systems is typically performed at the *adequacy* assessment level,

* Corresponding author. Tel.: +1 713 348 5292; fax: +1 713 348 5268.
E-mail addresses: leonardo.duenas-osorio@rice.edu (L. Dueñas-Osorio), svv1@rice.edu (S.M. Vemuru).

0167-4730/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.strusafe.2008.06.007

where adequacy relates to the existence of sufficient facilities to ensure power supply and balance energy demand. This adequacy approach is associated with the static conditions of the power system that ensure the existence of paths between power generation points and power consumption sites or load points. Hence, adequacy does not account for the dynamic effects within the networks triggered by disruptive events [11–14].

The limitations of adequacy-based reliability assessment become evident when trying to capture time-dependent features of power systems. For instance, the increasing congestion of power flow in transmission and distribution lines has a direct impact in the ability of the system to absorb unforeseen disruptions [15]. This increased congestion, or decreased tolerance, implies not only that low-frequency hazards can significantly impact the performance of power systems, but also that common disruption causes can trigger large-scale performance loss due to cascading failures. For example, the North American blackout in August of 2003 was initiated by an untrimmed tree too close to high voltage transmission lines in the Midwest [16]. A similar mechanism of arcs to untrimmed trees tripped several transmission lines in the Western US blackout of 1996 [17].

This study uses numerical simulation methods to capture the effect of cascading failures on power transmission systems subjected to natural and intentional hazards. A "cascading susceptibility" metric is used to quantify the additional disruption to power systems as compared to conventional connectivity or path-based performance assessments. The evaluation of transmission system performance is carried out under natural hazards, such as earthquakes and lightning storms, under random hazards that capture common cause failures (e.g., aging, animals, vandalism, etc.), and under disruption scenarios that deliberately target the most connected and loaded nodes. Since each disruptive event triggers flow redistribution within the networks and can potentially lead to cascading failures, a tolerance parameter is introduced in this work to capture the relationship between network component flow capacity and flow demand levels, and monitor the system's propensity to become unstable. The power transmission systems used in this study correspond to test networks of the Institute of Electrical and Electronics Engineers (IEEE) on 118 and 300 nodes [18]. This study also makes use of a synthetic transmission and distribution system called the TD network, which is helpful in generating multiple spatial networks via tuneable topological attributes [19].

The sampling-based simulation approach of this study also provides information about the significance of cascading failures as the network tolerances vary. Systems displaying performance disruptions of multiple severity levels at a given tolerance point are believed to be governed by the laws of complex systems [20]. These laws imply that small perturbations can *also* trigger large scale consequences, warranting new methods for risk reduction. Preliminary evidence of this observation is provided by the historical sizes of blackouts in North America and simulation models of complex dynamics [21,22]. In addition, the results from the disruptions applied to the IEEE and idealized TD models of this study suggest that heightened risks due to cascading failures are a property of sparse geographically distributed infrastructure systems.

This paper is divided into six sections. Section 2 presents the benchmark IEEE and TD power transmission systems for reliability assessment. Section 3 introduces the disruptive actions from natural and targeted (intentional) hazards, and describes the reliability metrics used to quantify system performance under cascading regimens. Section 4 compares the simulated response of the power systems with and without cascading failures and for different flow tolerances after the triggering hazards take place. The implications of accounting for cascading failures in risk mitigation are discussed in Section 5, where the effectiveness of different strategies to reduce cascading failure size and associated risks are compared for multiple network configurations. Finally, Section 6 presents the conclusions of this research and discusses activities for future work.

2. Benchmark power transmission systems

Practical test networks are used to represent the power transmission systems of this study. The systems correspond to the IEEE 118-node and 300-node networks used for reliability studies in the electric engineering community [18,23]. The $IEEE_{118}$ system covers an area of approximately 140,000 km^2 (Fig. 1), and its topological properties are summarized in Table 1. The *order* of the network refers to the number of nodes and the *size* to the number of transmission lines. The set of nodes is defined as the union of three different types of nodes: generation nodes n_G, transmission nodes n_T, and distribution nodes n_D.

The IEEE network nodes correspond to high, medium, and low voltage electric substations. High voltage substations act as supply nodes to the system, while low and medium voltage substations act as transmission and demand nodes. The basic topological properties of the $IEEE_{300}$ grid are also listed in Table 1, where the order of the network is $n = 266$ due to having 34 isolated nodes that are not used in this study but are present in the archived node-to-node connection data. The topological layout of this $IEEE_{300}$ network is available at the power systems research site of the University of Washington [18] and not reproduced here. However, the network possesses the same underlying structure of geographically distributed transmission networks, such as the $IEEE_{118}$, where long range connections (links among distant nodes) are rare and the number of links makes the system sparse. The $IEEE_{300}$ network is simply sparser due to its larger geographical coverage, which leads to a network that mimics an assembly of three sub-networks.

Additional topological parameters are also included in Table 1 to clarify the intrinsic characteristics of typical networked systems. The introduced parameters correspond to network efficiency L', average vertex degree $d(G)$, clustering coefficient γ, and redundancy ratio R_R [9,10]. The L' parameter measures how easy the communication across network nodes is on average. It is an indicator of global connectivity. As a reference point, highly idealized networks whose nodes are connected to every other node are denoted as *complete graphs*, and have an $L' = 1.0$. The $d(G)$ parameter measures the average number of connections per node in the network. The clustering coefficient γ, represents the average local connectivity of a network. It measures the likelihood of having the neighbours of a particular node v (nodes directly connected to v) connected to each other. Again, ideal complete graphs exhibit $\gamma = 1.0$. Finally, R_R measures the average availability of alternative paths to send flow out of the immediate neighbourhood of a node v in case of localized disruptions. Complete graphs also exhibit $R_R = 1.0$. It can be seen that real networks exhibit topological properties that are well below those of complete graphs, mainly because of real network needs to comply with geographical and economical constraints. Both the $IEEE_{118}$ and $IEEE_{300}$ networks have similar $d(G)$ and R_R values due to their identical power transmission nature, but differ in the γ and L' values. These differences are due to the sparseness effect that takes place in the $IEEE_{300}$ system as it expands its geographical coverage, making less likely the formation of local clusters within the sub-networks and making the power flow traverse larger distances.

Additionally, an improved synthetic transmission and distribution (TD) network is discussed in this paper to statistically represent real IEEE networks, and enable the construction of topologically diverse systems [19]. The superior TD network model of this paper takes input parameters that can be tuned to construct minimally

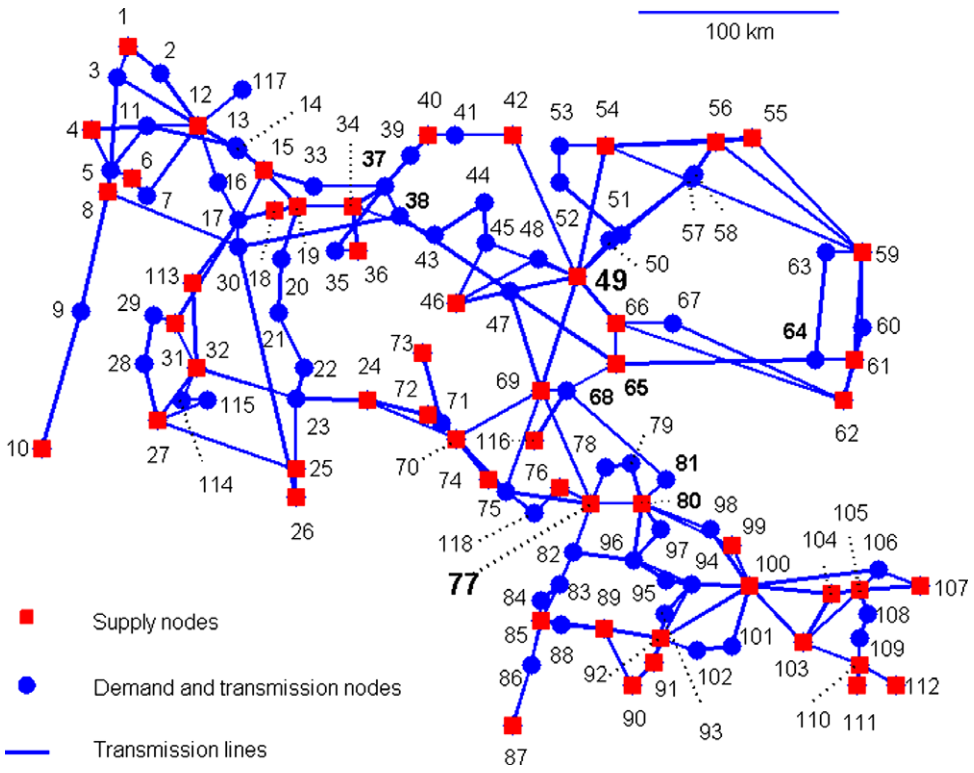

Fig. 1. Topology of the IEEE 118-node power transmission reliability test system.

Table 1
Topological properties of the benchmark IEEE and TD power transmission systems

Network	Network order, n	Network size, m	Generation subset order, n_G	Transmission and distribution subset order, $n_T \cup n_D$	Bypass parameter, β	Network efficiency, L'	Average degree, $d(G)$	Clustering coefficient, γ	Redundancy ratio, R_R
$IEEE_{118}$	118	179	54	64	–	0.21	3.03	0.17	0.18
$IEEE_{300}$	266	372	122	144	–	0.14	2.80	0.09	0.18
TD_{118}	121	179	54	64	0.50	0.21	2.96	0.17	0.20
TD_{300}	256	372	122	144	0.50	0.15	2.91	0.15	0.20
$TD_{Minimal}$	121	120	54	64	1.00	0.07	1.98	0.00	0.13
TD_{Grid}	121	220	54	64	1.00	0.20	3.63	0.00	0.22
$TD_{Enhanced}$	121	418	54	64	0.00	0.31	6.91	0.24	0.28

connected networks, homogeneous degree networks, and highly connected networks, among others. These idealized systems are squared networks whose order and size can be specified by the user. In addition, the preference for having long-range connections, or bypasses, can be tuned with the parameter $-1 \leqslant \beta \leqslant 1$, where -1 indicates networks with long-rage links that only connect *non-immediate* neighbours within the network, and 1 indicates networks with short-range links that connect *immediate* neighbours only. TD_{Grid}, $TD_{Minimal}$, and $TD_{Enhanced}$ have the same order as the $IEEE_{118}$ system, but with different β and m. These TD choices permit global performance comparisons and evaluation of containment strategies against cascading failures that only depend on network topology. TD_{118} and TD_{300} are models of the real IEEE systems, where $\beta = 0.5$ indicates a preference for short-range links, but with a certain probability of possessing long-range links. Fig. 2 illustrates the versatility of the tuneable TD models of distributed lifeline systems, and Table 1 summarizes their topological properties.

3. Disruptive events, cascading failures, and network performance

Disruptions of different nature are imposed to the power transmission systems of this study. Two main categories describe the types of hazard: disruptions based on historical natural hazard rates, and disruptions targeting specific network components. In the first category, seismic and lighting hazards are defined according to their rate of occurrence at different intensity levels in the Western and Midwest parts of the United States. The occurrence of seismic events is estimated from the annual hazard rates reported by the United States Geological Survey at two locations: Seattle, WA (WUS) and Memphis, TN (CEUS) [24]. These hazard rates are used to approximate the annual probability of exceedance of peak ground accelerations (PGA) [25], which in this study corresponds to lognormal distributions with medians $PGA_{m\text{-}WUS} = 0.0123$ g and $PGA_{m\text{-}CEUS} = 0.0024$ g, and coefficients of variation $COV_{PGA\text{-}WUS} = 1.08$ and $COV_{PGA\text{-}CEUS} = 1.58$. The same hazard levels are applied to all network nodes given their limited geographical coverage.

The probabilities of failure of power transmission system elements (e.g. electric substations of different voltage levels) are defined by their structural fragilities as a function of PGA. These fragilities have been estimated by the Federal Emergency Management Agency for use with its multi-hazard loss estimation methodology HAZUS-MH [26]. For supply nodes or high-voltage electrical substations (ESS5) with anchored components in the WUS region, the probability of exceeding a "slight" level of damage is described by a lognormal distribution with median $PGA_{m\text{-}ESS5} = 0.11$ g and

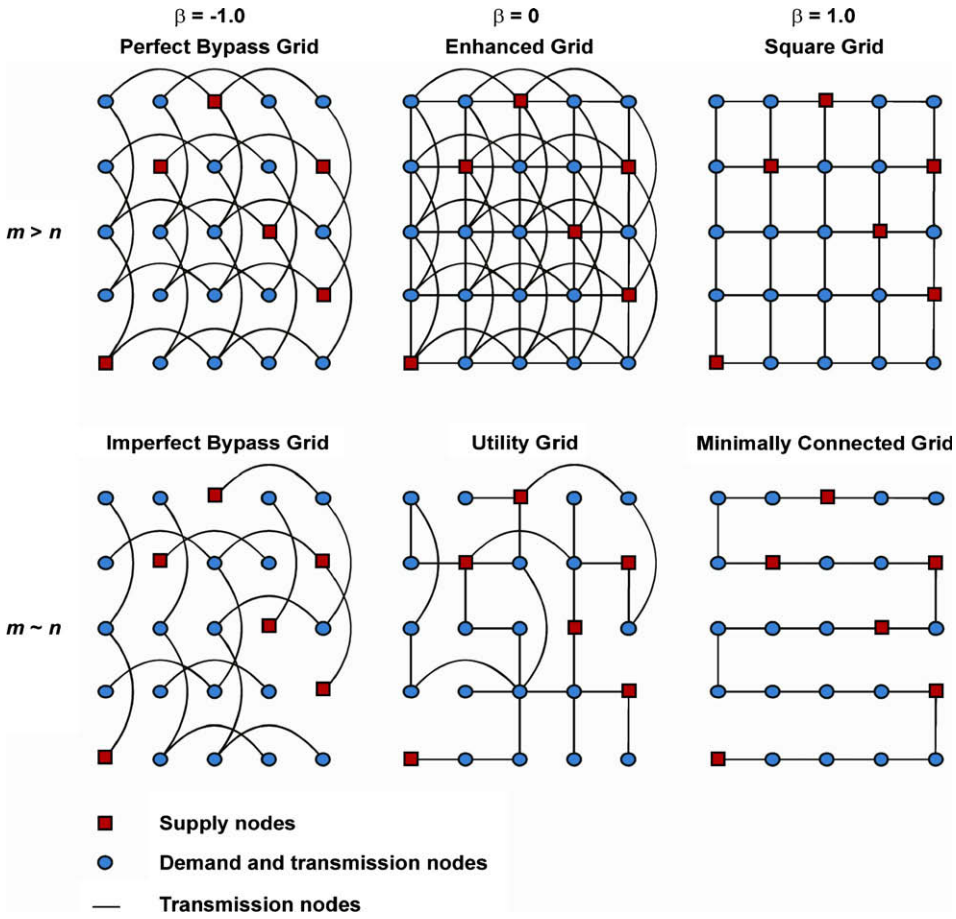

Fig. 2. Tunable TD model for constructing diverse geographically distributed network topologies.

coefficient of variation $COV_{ESS5} = 0.50$. The "slight" damage state is defined as failure in 5% of the substation equipment and with restoration time of less than one day. Failure of substation equipment is commonly due to their misalignment, sliding, tipping over, and minor damage induced by the structure that houses the substation equipment. The slight damage state is the only level considered in this study because of its higher probability of being exceeded during the life of power substations. If extensive or complete damage states were observed, the initial physical damage to the network would be so severe – failure in 70% and 100% of the substation equipment, respectively – that flow-induced cascading failures cannot develop after exceeding complete damage, and will be rare after extensive damage due to a shortage of functional surviving network elements. Table 2 summarizes the seismic hazard and fragilities for slight damage of high-, medium- and low-voltage electrical substations at the two US locations.

Lightning hazards are estimated from recorded ground flash densities in the continental United States. Typical mean annual flash densities N_g for WUS and CEUS range uniformly between $N_{g\text{-WUS}} = 0$–0.5 flashes/km^2/year with a standard deviation $\sigma_{Ng\text{-WUS}} = 0.14$, and $N_{g\text{-CEUS}} = 5$–7 flashes/km^2/year with a standard deviation $\sigma_{Ng\text{-WUS}} = 0.58$ [27]. The effect of lightning hazards on network transmission lines depends on N_g and is estimated from the flashover rate $\lambda_L(N_g)$ at which lightning strikes the power transmission lines [28]. The total flashover rate, which includes the effects of direct and indirect lightning on overhead lines, is used to calculate the probability of voltage overload using a spatially distributed Poisson process. Line failure occurs if at least one flash overloads the line. Hence, defining L_{ij} as the length in km of the ij transmission line, the probability of failure of a link from the Poisson process of lightning-induced failure is:

$$P_{ij}(\text{Failure}) = 1 - e^{-\lambda_L L_{ij}}. \quad (1)$$

Fig. 3 presents the *daily* probability of exceeding seismic (EQ) and lightning (LG) hazard intensity levels associated to each of the two US sites of this study. The plots show the hazard levels observed during a 500-year simulation time frame. As expected, the slope of the CEUS seismic hazard is smaller than the WUS counterpart, suggesting that for large hazard intensities there is a higher likelihood of earthquake occurrence at CEUS locations relative to WUS sites. This trend is implied by the approaching curves at intensity levels of PGA > 0.1 g, and it is consistent with the deep intra-plate and uncertain seismic environment of the CEUS region.

Table 2
Lognormal models for seismic and lightning hazards, and substation seismic fragility at slight damage levels

Hazard or fragility	Probability model	WUS		CEUS	
		Median	COV	Median	COV
Annual seismic hazard in PGA (g)	Lognormal	0.0123	1.08	0.0024	1.58
Low-voltage substation (ESS1)	Lognormal	0.15	0.70	0.13	0.65
Medium-voltage substation (ESS3)	Lognormal	0.15	0.60	0.10	0.60
High-voltage substation (ESS5)	Lognormal	0.11	0.50	0.09	0.50

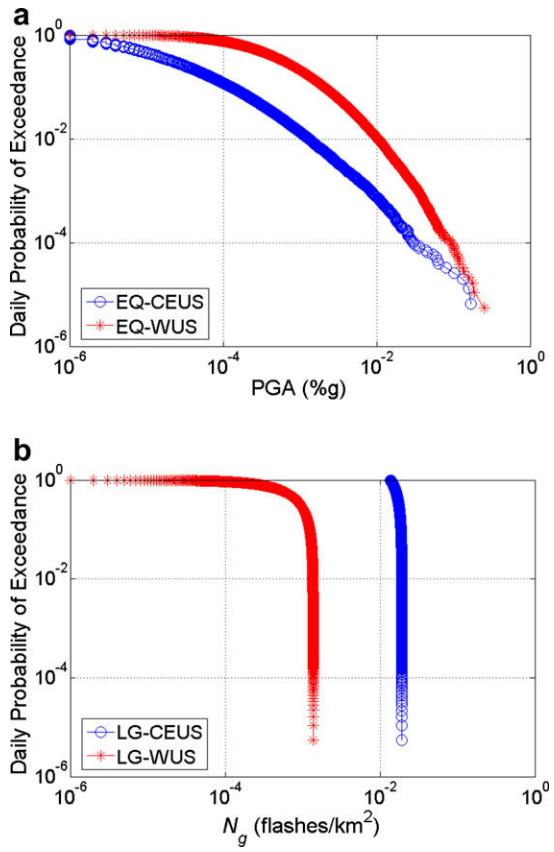

Fig. 3. Probabilities of exceeding increasing levels of hazard intensity at two representative US sites: (a) seismic hazards and (b) lightning hazards.

The lightning hazard characterization exhibits a low level of uncertainty and a narrow range of activity supported by the large amount of data recorded by the National Lightning Detection Network (NLDN), which over the 1989–1996 period registered more than 100 million flashes in the continental US [27]. Using the NLDN lighting hazard models over the 500-year simulation, well defined ranges of lightning activity for each of the US locations under consideration are observed.

Other disruptive events that systematically target particular network components are based on aiming at the most connected nodes, and highest loaded nodes. This is a deterministic process since the topology of the network is known at every point in time. To further explore the effects of systematic removals, nodes disrupted at random are also included in the analysis. The connectedness of a node is measured by its vertex degree $d(v)$, which counts the number of transmission lines that arrive and leave node v. The node with the largest degree $d(v)_{\max}$ is chosen for vertex degree attacks, and $d(v)_{\max}$ is recalculated after every node removal when more than one element is eliminated according to the intensity of the disruptive events. The maximum load or amount of flow passing through a node is measured by the vertex betweenness $B(v)$, which is calculated as the number of shortest paths that pass trough a vertex v when flow is sent from each available generation node to each distribution node. The node with the highest vertex betweenness $B(v)_{\max}$ is the node trough which the most electric power flows within the system, and is chosen for load-based attacks; this parameter is also recalculated after every element removal takes place. Random removals $R(v)$ are also performed as a strategy in which every node has the same probability of being disrupted. Any network performance measure derived from random failures is calculated from an average of 10 independent trials. These random component removals belong to the systematic disruption strategies and are independent of the 182,500 Monte Carlo simulations of daily natural hazard occurrence.

The possibility of observing cascading failures is enabled by assigning flow capacities to each of the nodes of the system. If any of these capacities are exceeded during power transmission, flow redistribution takes place to maintain the supply-demand balance of the grid. The vertex betweenness $B(v)$ is used as an approximation of the load $L(v)$ that flows through each vertex v. Since engineered systems are optimized for maximum capacity and minimum cost, it is assumed that the capacity of the nodes $C(v)$ is proportional to the initial load $L(v)$ [29–31]:

$$C(v) = (1+\alpha)L(v), \tag{2}$$

where $\alpha \geqslant 0$ is the *tolerance* parameter or added flow capacity relative to the original capacity, and $v = 1,2,\ldots,n$. Despite the simplicity of the α concept, this parameter allows a systematic evaluation of the aggregated effects of network element over-design on cascading failure containment. Also, while real systems exhibit elements with potentially unique α_v values that change with time, the system-level α model still provides useful insights about the efficacy of congestion-based failure avalanche prevention given flow-capacity expansions. Hence, when a disruption to the network occurs, the distribution of loads or flow patterns changes within the system, and depending on the value of $\alpha_v = \alpha$ for all v some nodes will fail because they are unable to handle the redistribution when $C(v) < L(v)$. These additional failures require a new redistribution of loads, which either stabilizes and the failures are locally absorbed, or grows until a large number of nodes are compromised to a failure point.

The parameters to monitor the performance of the power system focus on quantifying the ability of the system to transfer flow from supply to demand nodes. The concept of *connectivity loss*, C_L, is useful to quantify the average decrease of the ability of distribution nodes to receive flow from the generation vertices [32]. The calculation of this parameter relies on the topological structure of the network and the available least-resistance pathways. Denoting by n_G the order of the generation subset at the unperturbed state of the network, and n_G^i the number of generation units able to supply flow to distribution vertex i after disruptions take place, C_L can be calculated as

$$C_L = 1 - \frac{1}{n_D}\sum_{i}^{n_D}\frac{n_G^i}{n_G}, \tag{3}$$

where the averaging is done over every distribution vertex i of the network, and the flow through each transmission line is assumed to be undirected, as power grids are at the transmission level.

To quantify the added effects of cascading failures in network performance loss, another parameter is introduced as the *cascading susceptibility*, C_s. This parameter measures the added C_L induced by cascading failures after a disruptive event occurs, relative to the C_L resulting from the disruptive events without flow redistribution and cascading failures. Essentially, this parameter relates C_L due to the disruptive event $CL_{Trigger}$, and the total C_L after the cascading failure occurs and stabilizes or $CL_{Cascade}$.

$$C_s = \frac{CL_{Cascade} - CL_{Trigger}}{CL_{Trigger}}. \tag{4}$$

4. Power system performance

A more elemental performance metric than C_L or C_s for networked systems refers to the size of the initial failure set triggered by an external disruption. This metric simply monitors how many

network elements, regardless of their type, get initially affected by external perturbations without accounting for cascading effects. Lightning hazards are more frequent and affect a few of the system's transmission lines per event, whereas earthquakes are less frequent but can affect several electric transmission substations at once upon their occurrence. Systematic removals based on vertex degree, vertex betweenness, and random selection also affect network nodes, but only a small percentage per attack. Fig. 4 presents the topological response of the $IEEE_{118}$ system when subjected to earthquake and lightning hazards for a period of 182,500 days. Fig. 4a shows the mean level of seismic hazard associated to the events in which the initial failure sets are of increasing size. The failure set sizes are expressed as a percentage of the intact network order n. For example, a mean PGA = 0.175 g in WUS is responsible of network failures – those exceeding slight damage states – that compromise 70% of the nodes. Fig. 4b relates initial failure set sizes with their frequency of occurrence. The 70% failure size occurred only once among 337 failure events recorded during the 500-year simulation. The total number of failure events in the CEUS area was only 25. It is worth indicating that the response of the $IEEE_{300}$ network (not shown) follows similar failure trends to the $IEEE_{118}$ system response.

Regarding lightning hazards, the narrow range of the mean flash densities N_g associated to each US location produces a steep relationship with respect to the failure set size (Fig. 4c). Rare events, such as the failure of approximately 9% of the edges occurred only four times out of the 117,589 failure event cases observed during the 500-year period in the CEUS region. Smaller failure size events are observed thousands of times, making the failure set size and frequency of failure occurrence trends very stable. The total number of lightning-induced failure events in the WUS region summed 7763. It is important to highlight that the coefficients of variation (COV) of the natural hazard levels in Fig. 4a and c that are associated to a particular failure size (%n), remain relatively low at both locations: $COV_{PGA} < 50\%$ and $COV_{Ng} < 30\%$.

4.1. Cascading failures

To investigate the effects of cascading failures, the IEEE and TD systems are subjected to different triggering failure events induced by external hazards – EQ, LG, $d(v)$, $B(v)$, and $R(v)$. Once the triggering events occur, flow redistribution takes place as a mechanism to equilibrate supply and demand constraints. In this study, the flow redistribution process is monitored by introducing an artificial time step t_i, $i = 0,1,2,\ldots$ where t_0 represents the networks at their intact state, t_1 the networks after the initial hazard-induced failures occur, and $t_{\geqslant 2}$ describes the cascading failure progression as nodes overload and cause further failures in neighbouring elements.

For the $IEEE_{118}$ system under consideration, the cascading process is monitored until t_7, where the response stabilizes for all disruptive events. Fig. 5 presents the cascade evolution of the $IEEE_{118}$ network when subjected to all disruptive mechanisms. The triggering event consists of removing 1% of the network elements – a very small perturbation – according to the conditions of each removal strategy. Network response is monitored by the connectivity loss C_L for two tolerance values $\alpha = 0$ and $\alpha = 1$. In general, cascading failures evolve rapidly after the triggering event. The steady-state C_L is especially high for load- and degree-based attacks due to their direct impact on flow traversal. The node with highest load has $B(77) = 1028$ units of flow (number of flow paths between generation and distribution nodes) and connects the upper and lower portions of the network. At the same time the network has 20% of the nodes with null $B(v)$, which are designed with low capacity specifications. Hence, attacking node v_{77} results in widespread flow redistributions that only stabilize when the network losses more

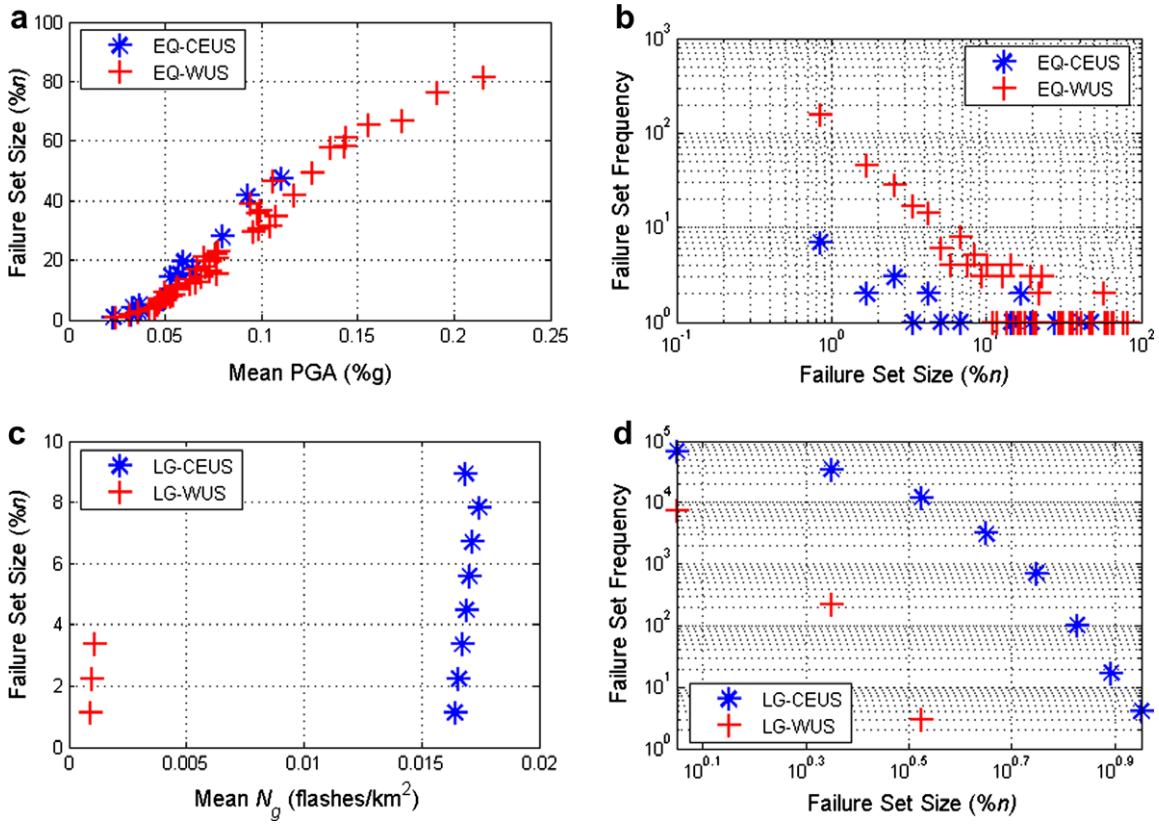

Fig. 4. Topological response of the $IEEE_{118}$ network to earthquake and lightning hazards. Part (a) displays the initial failure set size as a function of PGA and (b) displays the frequency of earthquake-induced failure set size occurrence. Parts (c) and (d) present similar information as a function of N_g and lightning-induced failure set size occurrence.

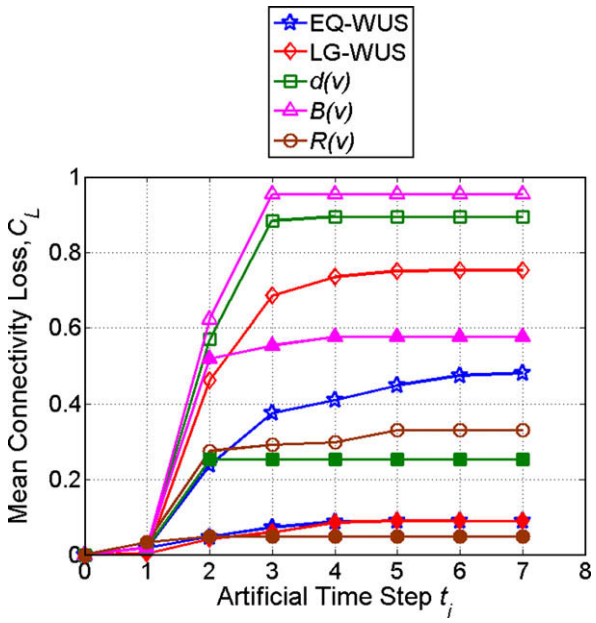

Fig. 5. Cascade evolution of the $IEEE_{118}$ test system when subjected to disruptions that consist of failures in 1% of the elements (hollow markers indicate a tolerance $\alpha = 0$, while solid markers indicate $\alpha = 1.0$).

than 90% of its connectivity. This sensitivity to $B(v)$ attacks reflects the inability of real networks to handle flow redistribution when their most *congested* elements fail, because neighbouring elements are also working close to their full capacity and are incapable of handling additional flows. Degree-based attacks affect nodes that serve as local hubs, but that not necessarily handle the highest network loads. In particular, the absence of node v_{49} with $d(49) = 9$ affects multiple flow pathways whose *compound* effect is large flow redistribution and subsequent connectivity loss. Since the identification of nodes with the highest loads and degrees is a deterministic process, the C_L reported in Fig. 5 corresponds to the exact C_L, while for other hazards the results are the mean of C_L. Regarding failures from random selection $R(v)$, they are unlikely to trigger large mean C_L due to the infrequent selection of critical nodes, such as v_{77} or v_{49}.

The cascading evolution from natural hazards is triggered by the failure events whose failure set size corresponds to 1% of the network elements (1 node for seismic hazards and 2 links for lightning hazards). The mean results in Fig. 5 include the natural hazards in the WUS area. Out of 337 seismic-induced failure events in the 182,500 daily trials, 156 events correspond to a failure size of 1%. Regarding lightning-induced failure events, 220 out of 7763 are of 1% failure set size. It is clear that LG-related failures pose a significant threat to the network, mainly because the links that fail more often are the longest ones, which in general are either at the periphery of the network or serve internally as feeders or connectors to high rank nodes within flow dispatch pathways. The links with "feeder" role help conducting flow in a least-resistance manner via high rank nodes (either high degree or high betweenness). Edges with end nodes {61,65} and {68,81} are examples of long links within pathways feeding flow to congestion points. The areas of most congestion in the $IEEE_{118}$ network are in the neighbourhood of nodes v_{77}, v_{80}, v_{65}, v_{68}, v_{37}, and v_{38}.

Regarding failures from seismic hazards, the non-functionality state of nodes is established when their *slight* limit state is exceeded, resulting in a more frequent failure of low-voltage substations. These substations have higher median PGA than high-voltage substaions, but at the low PGA levels causing 1% failure set sizes the dispersion of their lognormal model makes them more likely to fail. This preference results in moderate C_L effects, due to the more frequent failure of non-critical nodes (low-voltage substations), whose flow can be absorbed locally. The assumption of statistical independence in node failures can also contribute to the low C_L values, but its existence is not readily quantifiable in practice and is not addressed in this study.

Intuitively, increasing the flow-carrying capacity of the network elements should significantly decrease cascading failure effects. To explore this capacity increase approach, the tolerance parameter is set to $\alpha = 1.0$ and the disruptive events are applied to the $IEEE_{118}$ system again (solid markers). It is clear that doubling the capacity of the network elements reduces the extent of the cascades because flow redistribution can be handled at the local scale. However, the improvement for load-based attacks is the smallest among all threats, because capacity increase reinforces the use of certain pathways that enable efficient node to node flow exchange, and their failure still requires significant flow redistribution. To decrease element congestion, *global* interventions are required since local bypasses only shift the bottlenecks to nearby sites.

Given that node capacity increments are able to reduce the effects of cascading failures to some extent, the tolerance parameter effects are explored in more detail by varying it from 0 to 2.5, or from $C(v) = L(v)$ to $C(v) = 3.5 \times L(v)$, in increments of 0.1 while the C_L is recorded at the steady-state level. Fig. 6 presents the results for the $IEEE_{118}$ network under all considered threats. The figure shows overall improved network performance and the dominance of degree-based $d(v)$ and load-based $B(v)$ attacks on functionality. Even for large tolerance values of $\alpha = 2.5$, the residual C_L is only approximately 20%. Interventions to increase tolerance levels above $\alpha = 1.0$ may not be feasible in practice. Hence, these $d(v)$ and $B(v)$ threats may require not only capacity increase, but also topological changes in the layout of the network to prevent cascades.

The results of Fig. 6 also show that the largest improvements amongst most hazards are achieved for $\alpha < 1.0$. Sharp transitions occur when neighbouring nodes to high rank nodes are finally able to handle the redistribution of flow due to enough tolerance increase. The sharp transitions represent *emergent* properties of networked systems. When the failure of a decisive node is prevented due to enough flow redistribution capacity, then entire chain reactions are stopped from occurring and large differences in system response are observed.

Regarding natural hazards and random removals, the reduction in C_L as a function of α is a result of improvements in the local ability to absorb flow redistribution. Since 1% failure sets for EQ and $R(v)$ removal strategies affect nodes that in general are not critical in network flow, any tolerance increment reduces the extent of the

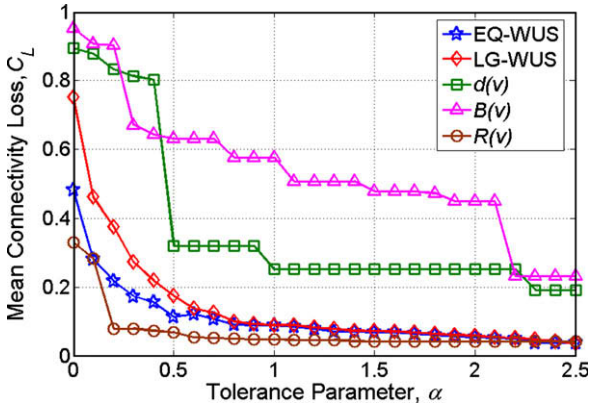

Fig. 6. Steady-state $IEEE_{118}$ network response as a function of system tolerance α for events of 1% triggering failure set size.

cascade at their local area, improving the global value of C_L (specially in the low α range). In the case of LG-induced failures, small increases in element capacity enable high rank nodes to absorb the failure of internal link feeders and display steady improvements as a function of α.

The cascading susceptibility C_s is measured for the $IEEE_{118}$ system under all hazards to further characterize the tendency of networked systems to undergo cascading failures (Fig. 7). The trends are similar to the results shown in the C_L vs. α plot, where as the tolerance increases, the detrimental failure effects on network performance decrease. The largest drops in C_s also occur for tolerances $\alpha < 1.0$, which are of practical implementation. The magnitude of the susceptibility is important: degree- and load-based local disruptions result in global detrimental effects as large as 50 times the system performance loss if cascading is prevented. This susceptibility is a clear flag for preventing the triggering event to occur as an efficacious mitigation strategy, as opposed to containment of the event once it is triggered. Such susceptibility illustrates the concept of network *emergent* response, where a very small perturbation can result in disproportionate system damage.

The lightning hazards bring a unique case of network susceptibility to cascading failures. The results shown in Fig. 7 for LG-induced failures are a lower bound of the actual susceptibility, which may be unbounded in certain cases. For instance, when a few number of links fail, it is possible that the effect of the initial perturbation failures results in $CL_{Trigger} = 0$, and if the cascading failure is activated by the benign triggering event, the steady-state cascade can be close to $CL_{Cascade} = 1.0$. These events, which are not necessarily infrequent, yield a theoretical $C_s \to \infty$ excluded from the reported mean C_s.

The results shown so far have mostly been obtained from the practical $IEEE_{118}$ test system. However, to explore the effects of *topology* on the response of networked systems, the $IEEE_{300}$ system and the set of TD networks ($TD_{Minimal}$, TD_{Grid}, $TD_{Enhanced}$, TD_{118}, and TD_{300}) are also subjected to natural and intentional hazards and their C_L is monitored for multiple levels of α. Fig. 8a shows that the practical IEEE test systems display a continuous improvement in performance as the tolerance is increased under seismic hazards. However, the $IEEE_{300}$ system is more vulnerable at $\alpha = 0$, due to the failure of low voltage stations that help interconnecting the three constituent sub-networks of the real system. The TD models of the IEEE test systems follow the trend better for the 118-node network than for the 300-node network. The real $IEEE_{300}$ system is able to let the sub-networks separate at low $\alpha \leqslant 1.0$, and to keep them together with high $\alpha \geqslant 1.0$, whereas the TD model is not yet able to model sub-networked systems, allowing massive cascades without early disconnection of distinct portions of the network.

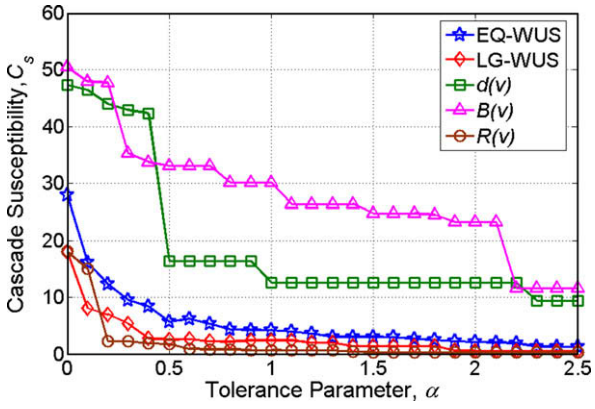

Fig. 7. Mean cascading susceptibility of the $IEEE_{118}$ test system subjected to natural and intentional hazards, multiple tolerance levels, and triggering events associated with 1% of the network elements removed.

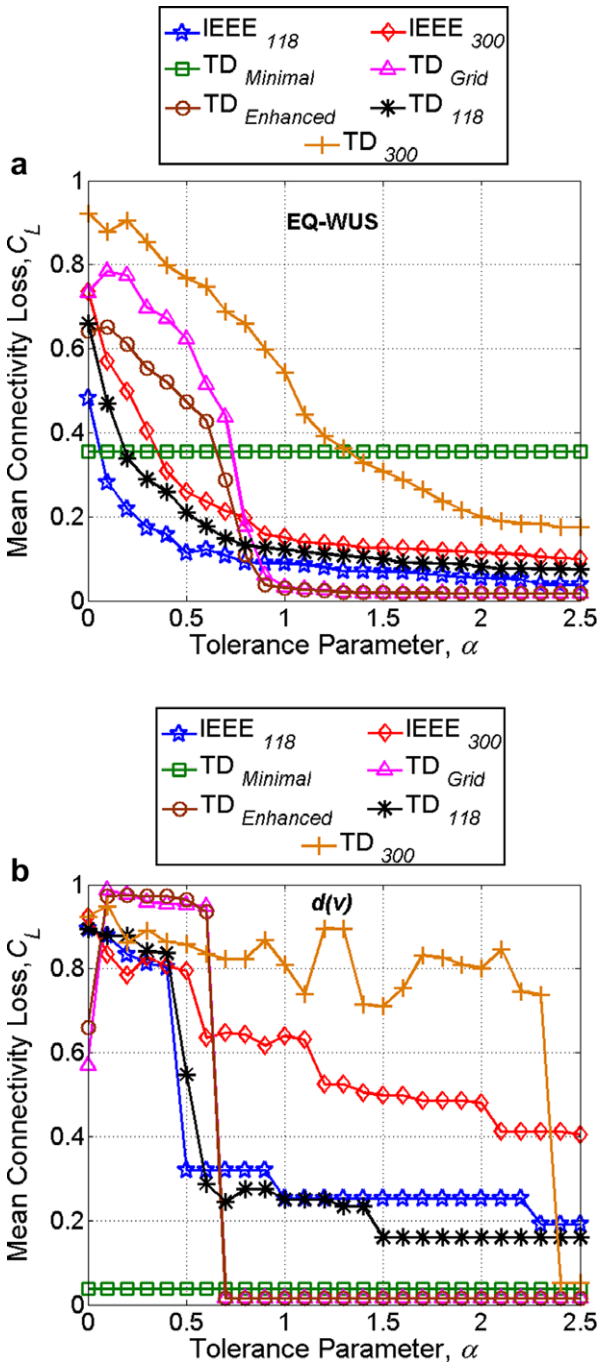

Fig. 8. Mean steady-state C_L for practical and ideal networks as a function of increasing tolerance. Part (a) shows cascades triggered by failures of 1% of the network elements under seismic hazards in the WUS area, and (b) cascades triggered by degree-based attacks.

Interesting outcomes are displayed by the ideal networks constructed from the TD models. At one topological extreme, the grid and enhanced architectures results in ordered flow patterns and regular interconnections that are capable of handling cascading failures provided that their tolerance is high ($\alpha \geqslant 1.0$). For lower tolerances but greater than zero, these regular topologies may substantially *increase* the C_L. This apparent contradiction is due to the flow patterns that result within regular topologies, which follow patterns with highest congestion at the center portions of the grid,

and gradually decreasing congestion towards the periphery. For $\alpha = 0$, a single node failure causes low-capacity neighbouring elements to fail in a long chain reaction, eventually disconnecting a large portion of the network, but stabilizing due to the reduced demand from "islanding" sections of the system. For the range $0.1 \leqslant \alpha \leqslant 0.5$, the nodes with high load receive the largest absolute capacity increase and do not fail, whereas the lower load and capacity nodes still fail in a hierarchical mode. These lower-load nodes trigger long cascade propagation events, but this time from the outside to the inside, compromising very large portions of the network due to the lack of early islanding.

At the other topological extreme, a minimally connected network gets disconnected with the failure of any element. Once the network disconnects, demand decreases due to the islanding, and cascades are never developed – there are no alternative paths to overload and the network is insensitive to tolerance increases. The behaviour of these different networks suggests that homogeneous topologies with adequate tolerance, as well as weak links for early disconnection or islanding are warranted for the reliable and cascade-controlled operation of modern lifeline systems. Fig. 8b shows network performance trends under degree-based attacks, displaying more abrupt transitions, less accurate predictive capabilities of the TD_{300} network (due to the lack of sub-network islanding), and visible overall improvements for approximately $0.6 < \alpha < 1.0$.

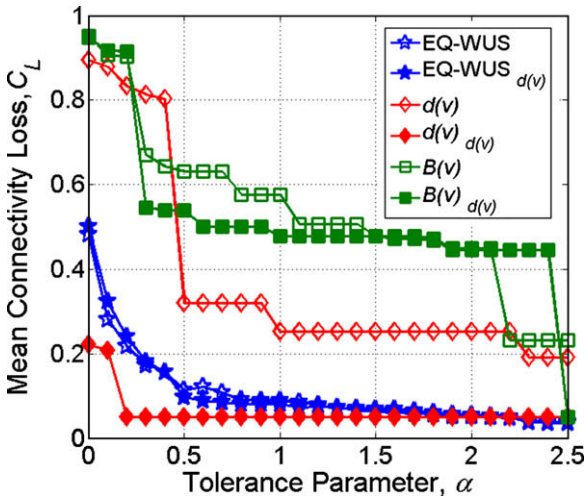

Fig. 10. Effect of minimally invasive degree-based interventions on the response of the $IEEE_{118}$ system under different hazard events. The events triggered by the hazard correspond to 1% failure set sizes. Solid markers include the effects of topological interventions.

5. Infrastructure interventions

Since the operation of geographically distributed infrastructures is sensitive to system layout, a few topological mitigation actions are explored using the $IEEE_{118}$ system. Current operating practices and deregulated markets push infrastructures to work closer to their maximum design regimens, and traditional countermeasures, if implemented, focus on improving the capacity of congested elements. This current approach does not guarantee protection against cascading failures. Hence, the concept of homogeneous topology is implemented by reducing the vertex degree of the four most connected $IEEE_{118}$ nodes: v_{49}, v_{100}, v_{12}, and v_{80}. These nodes are modified by reducing their $d(v)$ from 9, 8, 7 and 7, respectively, to $d(v) = 6$. The modifications are not intrusive and can be achieved in practice. The process consists of replacing a direct connection with short paths between nodes as illustrated in Fig. 9. This process is implemented in the four $IEEE_{118}$ nodes and reported in Fig. 10. Solid markers show the modified network response, which improves dramatically against degree-based attacks. Load-induced failures also benefit from the attempts to homogenizing $d(v)$ and reducing bottlenecks due to existing correlations between high vertex betweenness and high vertex degree. The benefits of this degree-based intervention to reduce EQ-induced failure are not significant, mainly because seismic hazards at low PGA levels affects low voltage substations, which are not the most connected elements.

Discussions of the response of the $IEEE_{118}$ system to natural hazards have been limited to WUS area failure events associated with damage in 1% of the network elements. CEUS failure events associated with damage in 1% of the network elements are similar to WUS failure sets, but occur less frequently for EQ and more frequently for LG. The small 1% perturbation sets in either area serve to highlight the concept that networked systems can experience large disruptions from seemingly benign triggering events. Obviously, large network disruptions are also observed as a result of larger triggering events, which in addition to the small-trigger large-consequence events result in a high frequency of observing large disruptions – more than traditionally acknowledged.

6. Conclusions

Conventional path-finding or connectivity-based reliability assessment for infrastructure systems can lead to significant underestimation of their expected performance. Connectivity-based methods focus on finding enough connected components within the network so that supply and demand can be balanced.

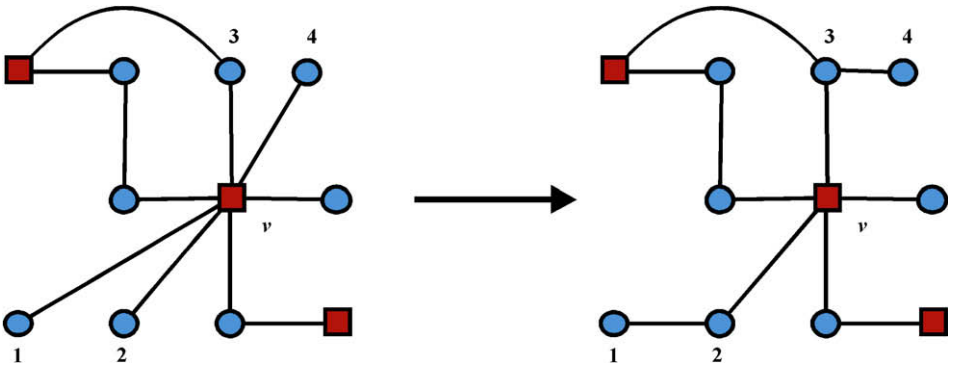

Fig. 9. Practical strategy to homogenizing high vertex degree nodes in flow transmission and distribution systems; the illustration shows a change from $d(v) = 7$ to $d(v) = 5$ – enough to modify flow patterns globally.

However, these methods are unable to capture flow dynamics within the network.

When flow dynamics are included in the reliability assessment, the systems are likely to undergo large-scale cascading failures. These failures are caused by flow redistribution after the occurrence of disruptive events. Since most engineered systems are designed to operate close to their capacities, any increase in flow demand decreases the tolerance of their components. This phenomenon can slowly drive the systems into critical states to the point where a *single* element failure or a small removal fraction of network elements can trigger large-scale disruptions, such as power outages in electric transmission and distribution systems. The dynamics of flow redistribution and cascading failure is also observed to occur rapidly. This study shows that the first time step after the triggering disruption accounts for the largest loss of performance with respect to the residual functionality of the network after reaching its steady-state response level.

The tolerance to flow overload in infrastructure systems displays a critical value α_c, below which the largest improvements in C_L occur. For most of the networks under investigation subjected to different hazards $\alpha_c \approx 1$. Increasing the tolerance beyond the critical value does not significantly improve the robustness to prevent disproportionate cascading failures, which implies that only upgrading the tolerance of existing systems is not an effective solution. Hence, improving topology is shown to have a positive effect on not only increasing robustness, but also decongesting the system, decentralizing it, and increasing the number of alternative routes in the event of natural and targeted hazards. This work shows that homogeneous network layouts coupled with weak links for early containment of cascade propagations represent viable strategies to prevent the adverse effects of cascading failure. Islanding is a strategy that deliberately disconnects portions of the networks to prevent larger consequences. However, this strategy is not widely used in practice, except for special cases in the power industry, which relies on the judgement of human controllers in time-constrained contexts. The cascading analysis method of this study coupled with topological insights of the networked systems can lead to *a priori* identification of network points for topology and load pattern homogenizations, identification of optimal element tolerances, and selection of weak link locations.

Network disruptions based on their vertex degree and vertex betweenness proved to impose the largest loss of network performance for a given triggering event of small size. Natural hazards appeared to be less harmful in network performance losses due to the exclusive use of events with small failure set size as triggering events. However, the choice of small triggering size events highlighted the development of cascading failures from seemingly harmless perturbations.

Overall, the susceptibility of infrastructure systems to decreased tolerance and reduced local interconnections leads to more frequent cascading failures. Service impairment even from simple disruptions can be exceedingly large, and these large-scale cascades are more common than currently assumed in connectivity-based reliability assessments. This critical behaviour is typical of complex systems and has been observed in practical IEEE test systems and generic transmission and distribution systems such as the TD models.

Future work to advance the field of infrastructure system risk and reliability includes the following topics: inclusion of restoration processes and times to repair on cascade-susceptible system performance under natural, operational, and targeted hazards [33], development of *analytical* methods to establish universal network topological effects on system performance [19], expansion of optimization-based system reliability [34] to capture network flows and cascading failures beyond traditional path assessments, and quantification of infrastructure robustness in the context of disproportionate *risks* triggered by cascading failures [35].

Acknowledgements

The work reported here has been funded in part by the National Science Foundation grant CMMI-0728040. The first author also wishes to thank Mr. Isaac Hernandez-Fajardo at Rice University for the computer implementation of the TD model, and Dr. Satish Nagarajaiah also at Rice University for providing GRA support.

References

[1] Chang SE, Seligson HA and Eguchi RT. Estimation of the economic impact of multiple lifeline disruption: Memphis light, gas, and water division case study. Technical Report No. NCEER-96-0011. Multidisciplinary Center for Earthquake Engineering Research (MCEER), Buffalo, New York; 1996.
[2] Haimes YY, Horowitz BM, Lambert JH, Santos JR, Lian C, Crowther KG. Inoperability input–output model for interdependent infrastructure sectors. I: Theory and methodology. J Infrastruct Syst 2005;11(2):67–79.
[3] Adachi T, Ellingwood B. Serviceability of earthquake-damaged systems: effects of electrical power availability and back-up systems on system vulnerability. Reliab Eng Syst Safety 2008;93(1):78–88.
[4] Dueñas-Osorio L, Craig JI, Goodno BJ. Seismic response of critical interdependent networks. Earthquake Eng Struct Dyn 2007;36(2):285–306.
[5] Pederson P, Dudenhoeffer D, Hartley S, Permann M. Critical infrastructure interdependency modeling: a survey of US and international research. Report INL/EXT-06-11464, Idaho Falls: Idaho National Laboratory; 2006.
[6] Boccara N. Modeling complex systems. New York: Springer; 2004.
[7] Ottino JM. Engineering complex systems. Nature 2004;427:399.
[8] Watts DJ. Small worlds: the dynamics of networks between order and randomness. Princeton (NJ): Princeton University Press; 1999.
[9] Newman MEJ. The structure and function of complex networks. SIAM Rev 2003;45(2):167–256.
[10] Dueñas-Osorio L, Craig JI, Goodno BJ, Bostrom A. Interdependent response of networked systems. J Infrastruct Syst 2007;13(3):185–94.
[11] Billinton R, Li W. Reliability assessment of electric power systems using Monte Carlo methods. New York: Springer; 2006.
[12] Balijepalli N, Venkata SS, Christie RD. Modeling and analysis of distribution reliability indices. IEEE Trans Power Deliv 2004;19(4):1950–5.
[13] Li W. Risk assessment of power systems: models, methods, and applications. Piscataway (NJ): IEEE Press; 2005.
[14] Warren S, Saint R. IEEE reliability indices standards – major event day calculations and how they relate to small utilities. IEEE Industry Appl Mag 2005(January/February).
[15] Bush R. The future of transmission in North America. Transm Distrib World 2003;5(1):27–32.
[16] United States – Canada power system outage task force (2004). Final report on the August 14th, 2003 blackout in the United States and Canada: causes and recommendations. United States Department of Energy and Canadian Department of Natural Resources.
[17] Kosterev DN, Taylor CW, Mittelstad WA. Model validation for the August 10th, 1996 WSCC system outage. IEEE Trans Power Syst 1999;14(3):967–79.
[18] Christie RD. Power systems test case archive. Department of Electrical Engineering, University of Washington. 24 March 2007, 1999. Available from: ⟨http://www.ee.washington.edu/research/pstca⟩.
[19] Dueñas-Osorio L. Interdependent response of networked systems to natural hazards and intentional disruptions. Chapter 4: Network models. Dissertation, Georgia Institute of Technology. Atlanta: Georgia Tech Library, UMI 3198529; 2005.
[20] Jensen HJ. Self-organized criticality – emergent complex behavior in physical and biological systems. Cambridge: Cambridge University Press; 1998.
[21] NERC. Disturbances, load reductions, and unusual occurrences. Disturbance analysis working group, North American Electric Reliability Corporation (NERC). 24 March 2007. Available from: http://www.nerc.com/~dawg.
[22] Carreras BA, Lynch VE, Dobson I, Newman DE. Complex dynamics of blackouts in power transmission systems. Chaos 2004;14(3):643–52.
[23] Chowdjury BH, Baravc S. Creating cascading failure scenarios in interconnected power systems. IEEE Power Engineering Society General Meeting, Montreal, Canada, July 18–22, 2006.
[24] USGS (2007). "Seismicity rates". Earthquake hazards program, United States Geological Survey. 25 March 2007. Available from: http://earthquakes.usgs.gov/research/hazmaps.
[25] McGuire, Robin K. Seismic hazard and risk analysis. Monograph MNO-10, Earthquake Engineering Research Institute. Oakland: EERI; 2004.
[26] FEMA, 2006. HAZUS-MH Technical Manual. Chapter 8, Direct damage to lifelines. Federal Emergency Management Agency (FEMA), Washington, DC.
[27] Huffines GR, Orville RE. Lightning ground flash density and thunderstorm in the continental United States: 1989–1996. J Appl Meteorol 1999;38:1013–9.

[28] IEEE (1997). IEEE guide for improving the lightning performance of electric power overhead distribution lines, IEEE-1410. Institute of Electrical and Electronics Engineers (IEEE), New York.
[29] Motter AE, Lai Y-C. Cascade-based attacks on complex networks. Phys Rev E 2002;66:065102. 1–4.
[30] Crucitti P, Latora V, Marchiri M. Model for cascading failures in complex systems. Phys Rev E 2004;69:045104. 1–4.
[31] Zhao L, Park K, Lai Y-C. Attack vulnerability of scale-free networks due to cascading breakdown. Phys Rev E 2004;70:035101. 1–4.
[32] Albert R, Albert I, Nakarado GL. Structural vulnerability of the North American power grid. Phys Rev E 2004;69(2):025103. 1–4.
[33] Adachi T. Impact of cascading failures on performance assessment of civil infrastructures systems. Dissertation, Georgia Institute of Technology. Atlanta: Georgia Tech Library; 2007.
[34] Song J, Der Kiureghian A. Bounds on systems reliability by linear programming. J Eng Mech 2003;129(6):627–36.
[35] Baker JW, Schubert M, Faber MH. On the assessment of robustness. Struct Safety 2008;30(3):253–67.