Title	A Comparison of Malicious Interdiction Strategies Against Electrical Networks
Authors(s)	Cuffe, Paul
Publication date	2017-06
Publication information	IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 7 (2): 205-217
Publisher	IEEE
Item record/more information	http://hdl.handle.net/10197/8774
Publisher's statement	© 2017 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.
Publisher's version (DOI)	10.1109/JETCAS.2017.2704879
Notes	See corrigendum at http://hdl.handle.net/10197/8774

A Comparison of Malicious Interdiction Strategies Against Electrical Networks

Paul Cuffe, *Member, IEEE*

***Abstract*—How well can a typical electrical power system withstand a sophisticated malicious attack undertaken against its exposed branches? The present work seeks to articulate a comprehensive answer to this fundamental question of wide societal importance. New and established techniques that an attacker might use to select promising attack targets are considered, spanning complex network analysis, metaheuristics and classical optimization. By simulating this wide gamut of attack strategies on several test power systems, each modelled under many representative operating states, this work comprehensively articulates the expected robustness of electrical power grids against coordinated branch interdictions.**

***Keywords*—Cascading failure, directed attacks, branch interdiction, centrality, optimization, metaheuristics**

I. Introduction

Improving the reliability and security of supply of electricity are key drivers of emerging smart grid technologies [1], although the widening penetration of online components means that networks then become vulnerable to remote cyber-attacks and observation [2], [3]. For instance, serious supply interruptions in Ukraine in late 2015 are a documented example of malicious cyber-attack [4]. How might the nascent observability, and diversification of line loadings [5], of power grids affect their robustness against malicious attack? By simulating various strategies that a malicious attacker may use, while considering numerous systems in various states, the present work seeks to articulate a meaningful, defensible answer to this important question.

The present work proceeds under the realisation that a high voltage transmission line is inherently vulnerable [6]: one can be taken out of service by an errant kite, a deftly lobbed length of metal chain, or even remotely, by a cyber attack against its associated circuit breakers. By contrast, power system buses are typically housed within compounds whose perimeter could, at least notionally, be monitored and defended. For this reason, one limitation of much of the published literature on electric grid vulnerability is the common focus on bus removal scenarios [7]–[11].

Broadly speaking, electrical power systems are operated so that they can withstand the loss of any one of their branches, generators or other elements [12]. This $(N-1)$ criteria ensures that when a line is removed from a system, the redistribution of the flow it was carrying should not overload any other lines: if it did, *overload cascading* would occur [13]. However, the robustness of power systems against malicious $(N-k)$ outages is harder to asses [14], due to the combinatorial explosion of potential scenarios. The present paper seeks, in part, to address this lacuna.

Taken together, certain elisions and tendencies in the extant literature make it hard to draw a consensus conclusion on power grids' typical robustness against branch interdiction attacks. For instance, there is often an emphasis on bus attack strategies; a common reliance on abstract powerflow models; a tendency to model power system in just a few unrepresentative states; and a lack of domain knowledge in selecting which assets to attack. By contrast, the present work offers prescient insights by simulating many attacks, of varying sophistication, against the branches of numerous representative grids. The research question is simple: how much damage can a sophisticated attacker be expected to cause by removing a small number of branches from a power grid?

A literature review to substantiate the foregoing claims is provided in Section II; in Section III the present work's chosen branch attack strategies are described; the test platform for trialling these is discussed in Section IV; results are in Section V; and Section VI concludes.

II. Literature Review

A. Complex network approaches

The surveys in [15], [16] review the application of complex network techniques to electrical grids. Such work has typically come from practitioners of complex network analysis. Two threads are evident in the literature: purely descriptive works, which seek to characterise and categorise power grids based on their structural or centrality features, and works using these descriptors to infer the reliability or robustness of power systems: per [15] *"Another recurring theme [...] is the reliability analysis, and actually it is the main motivation that drives these kind of studies."* One limitation is that much of the influential, heavily cited research in this latter field, such as [7]–[11], [17]–[20], comes from outside the ambit of power engineering, and often uses idealised models of cascading failure propagation.

Fundamentally, inferences about power grid robustness that are not grounded in the physical realities of electrical power flow are somewhat questionable: [21] offers some useful review treatment of this issue. For instance, the power engineers who authored [22] had to conclude *"that evaluating vulnerability in power networks using purely topological metrics can be misleading."* Likewise, the review in [15] states *"We emphasize the inappropriateness of purely topological*

This work was conducted in the Energy Institute, University College Dublin, Ireland, which is supported by the Electricity Research Centres Industry Affiliates Programme (erc.ucd.ie/industry/)

P. Cuffe (paul.cuffe@ucd.ie) is with the School of Electrical & Electronic Engineering, University College Dublin.

measures, since they are not able to capture the essence of the power systems." The authors of [23] echo this, pointing out by the title of their paper that topological metrics are not just misleading, but can be overly-optimistically so: *"Context-independent centrality measures underestimate the vulnerability of power grids"*

B. Agent based modelling

A related way to gauge the robustness of a power grid, especially considering its interdependence with other critical infrastructures, is to model them as a holistic *complex adaptive system* [24]. Under this scheme, *agent based modelling* can be used to simulate the interaction of different actors in the network, such as generators, operators, communication links and conductors [25], [26].

C. Power engineering perspectives

In recent years certain researchers have begun to bridge the gap between power engineering and complex networks analysis. The work of Hines is foundational here, both in articulating the empiric topology of power grids [27]–[33] and in assessing their robustness against cascading failure [34]–[41]. The importance of using realistic models of power flow and cascade dynamics is emphasised throughout this corpus.

Likewise, the work of Bompard has articulated a notion of *structural vulnerability* in power grids [42]–[52]. Much of this work draws on new, or hybrid, topological measures, which seek to unite generic complex network concepts with electrically relevant metrics.

A similar body of work [53]–[59] has been developed by authors associated with the MATCASC software tool, which simulates cascading failures in electrical power systems. While this corpus is valuable, one limitation it embodies is that branch thermal limits are modelled in an unrealistic way, where the maximum permissible flow is taken as the base-case power flow multiplied by some tolerance parameter (as also in [60]). In reality, branch thermal limits will not have a simple relationship with initial branch flows, and also depend on ambient weather conditions.

D. Risk analysis

There is also an established body of literature on the risk analysis of *accidental* cascading failure in power systems, of which the IEEE Cascading Failure Working Group have produced a number of authoritative surveys [5], [61], [62]. The state of the art here is sophisticated [63]: modern simulation tools e.g [64] can simulate many of the dynamics underlying cascading failures with impressive granularity. In this space, the triumvirate of Dobson, Newman and Carreras have, separately and jointly, produced an impressive nexus of work on cascading failure risk analysis in power systems [65]–[78]. Notably, such works, and others [64], have typically made their risk analyses on small numbers of systems, and generally haven't considered sophisticated attack scenarios, focusing instead on quantifying the risks of how *accidental* component outages may trigger cascades.

E. Attack modelling

A separation is clear in the extant literature: modelling of intentional attacks has mostly come from the complex networks community, and generally uses overly abstract conceptions of how power systems operate. On the other hand, the state of the art in power system engineering can model cascading failures with realism: for instance, [79] considers both short and medium term outage effects, and includes representations of e.g transient and frequency stability in the cascade simulation [80]. Of those engineering works that consider intentional attacks, optimal power flow techniques are popular for identifying sets of power system components to attack [81]–[83]. Likewise, metaheuristic formulations to identify promising attack targets are also common [37], [38], [40], [79], [84]–[88]. Finally, and as previously mentioned, network structural metrics are also used within the power systems literature on attack simulation [33], [46], [47], [54], [55], [89]–[91].

Due to a paucity of meaningful comparisons in the existing literature, it is not clear which of these broad approaches might be most effective for attacking a power system (though cf. [92] which makes some comparison of the efficacy of certain topological metrics)

F. Multilevel attacker/defender formulations

Another theme in the modelling of power system attacks is the use of *multilevel* formulations, as introduced by Salmerón et al [93], [94]. Within this paradigm, an attacker marshals their available resources to cause *maximum* damage, while simultaneously the system operator proactively uses their resources to *minimize* the impact of an attack (for instance, by post-attack generator redispatch or line switching.) The work of Arroyo implemented this model as a bilevel optimization problem in [95], with his subsequent work elucidating further refinements to such a formulation [96]–[99]. Others have also made important contributions to the multilevel modelling of power system attack and defence games [100]–[102]: some contributions additionally consider optimal pre-emptive defensive *hardening* of certain components [99], [103], [104].

G. Paper contributions

Laying aside their relative merits, both power engineering and complex network approaches to cascade attack analysis typically suffer from a reliance on small sample sizes (worthy exceptions to this trend include [35], [38], [39], which consider a number of $(N-1)$ secure dispatches for different system loadings. Likewise, works using the OPA simulation tool can take due account of multiple load growth snapshots e.g [105].) This paper compares and contrasts a wide range of possible techniques to select combinations of branch contingencies, and uses many snapshots of various systems to assess their effectiveness.

III. Methodology

This works seeks defensible conclusions on the attack robustness of plausibly parametrised power systems that are

simulated with approximate physical realism. This goal requires that each attack strategy is trialled against a number of test power systems, with each system considered in a large number of representative states. Likewise, as modern power grids typically use SCADA systems, it becomes conceivable for malicious actors to remotely monitor power flows and generator dispatches, and attack strategies that exploit such information must be included. While attacks on the SCADA system itself also offer various other ways to damage a power system [106], for the sake of clarity the present work maintains a focus on the direct electrical effects of branch removals.

A. Branch interdiction strategies

This work seeks a comprehensive comparison of a range of potential branch attack strategies. Eight strategies are considered: of these, three may be deemed *smart*, requiring some computational effort, with the remaining five simpler to calculate. Three of the strategies are static, and attack the same branches regardless of how network flows change from one snapshot to the next. Four of the attack strategies require observability of the instantaneous state of a power system.

Each strategy selects K branches to remove, where K is some small predefined integer reflecting anticipated attacker resources. All branches in the system are assumed to be equally available for attack: this disregards the idea of pre-emptive strategic hardening of certain components by the system operator (cf. Section II-F) The eight strategies considered are as follows:

`GA_demand` This interdiction strategy uses a standard genetic algorithm to select which lines to attack. The fitness function it seeks to minimise is the *demand survivability* [57]: this quantifies what portion of the demand can still be served after a cascade. The approach here is entirely, and deliberately, generic. This strategy should be seen as a baseline metaheuristic approach that an attacker might use to select branches to interdict. The lack of fine-tuning means that this strategy likely substantially *underestimates* the damage that this style of attack could cause.

`GA_link` This novel strategy is equivalent to that above, except here the fitness function minimized by the metaheuristic is the *link survivability* [57]. This measures the number of branches remaining in operation in the system after the cascade, which is a complementary measure of failure severity.

`MILP_overload` This strategy employs a more refined optimization formulation than the previous unsubtle metaheuristics. In essence, it uses mixed integer linear programming to select the K lines to remove from a system, where the novel objective function estimates post-removal line overloads (details of this formulation are given anon).

`Random` This simple strategy is included as a baseline control, as in [91]. For each power system snapshot to be attacked, the K lines to be removed are selected based on a pseudorandom integer generator.

`Loading` This is included as a simple *context-aware* metric. For each state of the power system to be attacked, the percentage line loading of each branch is calculated. The most-heavily loaded K lines are then removed. (A similar approach is taken in [107] and [108])

`Elec_between` This static metric of *electrical betweeness* was proposed in [109] (cf [45]). It uses the notion of unit transactions of power between each generator and each load, and sums each branch's involvement in the partial flows [110] that these transactions invoke.

`Topo_between` This static topological metric, known as *betweeness centrality* [111], is a classical measure of component importance in complex networks. It is calculated as the fraction of the shortest paths between every node pair that pass through a particular bus or branch.

`Shortcut` This static topological metric of *edge range* [9], [112] records the shortest path between the nodes that a branch connects, *after* that branch's removal. A low value indicates that, in terms of shortest paths, a branch enjoys some redundancy. If the branch is an *isthmus*, this metrics goes to infinity, and its removal from a power system will guarantee islanding.

B. Unit commitment and dispatch

1) System state creation: Each attack strategy is to be trialled against many representatives snapshots of each system's state, all of which are to be $(N-1)$ secure. Creating generation profiles for each snapshot therefore requires a security-constrained unit commitment and dispatch procedure. The formulation employed here to do this is conventional and entirely deterministic. Generators are dispatched solely to meet the demand, and no dynamic reserves are carried (though such reserves may indeed affect a system's robustness)

The quadratic cost function to be minimized is given by:

$$min \sum_{g}^{g^+} c_{g,1} P_g^2 + c_{g,2} P_g + c_{g,3} \tag{1}$$

Where P is a decision variable giving the power output for each generator (index: g cardinality: g^+) The c parameters describe the heat rate costs for each generating unit.

A binary decision variable, S, determines whether each unit is online. This variable is incorporated within the minimum and maximum output power constraint for each unit:

$$S_g P_g^- \leq P_g \leq S_g P_g^+ \tag{2}$$

As this is a security-constrained formulation, the optimal generation schedule must respect branch thermal limits following all credible contingencies (i.e the individual removal of each line, unless this would cause islanding) Including these contingencies (index c) increases the dimensionality of the powerflow variables, as denoted in their superscript.

Kirchoff's laws are enforced at every bus (index b):

$$P_{net,b}^c = P_{g,b} + P_{d,b} \tag{3}$$

The parameter $P_{d,b}$ is a vector describing the fixed power demands at each bus, while $P_{g,b}$ identifies the generator connecting at bus b. The vector of branch power flow variables

for each contingency, F_l^c, also contributes to the power balance at each bus:

$$P_{net,b}^c = F_l^{cT} A_{l,b}^c \tag{4}$$

The parameter matrix $A_{l,b}^c$ is the system's incidence matrix, appropriate to the prevailing contingency.

For a branch connecting bus i to bus j, with reactance X_l, the power flow is determined by the voltage angle difference that prevails in those contingency conditions, ϕ^c:

$$F_{l,i\to j}^c = \frac{\phi_i^c - \phi_j^c}{X_l} \tag{5}$$

The vital thermal limits are imposed in the intact condition by:

$$-F_l^+ \leq F_l^{c=0} \leq F_l^+ \tag{6}$$

As more generous thermal limits are briefly tolerated under contingency conditions, emergency limits can be applied there:

$$-F_l^{++} \leq F_l^c \leq F_l^{++} \tag{7}$$

2) System load normalization: The present work seeks to draw comparisons between different test systems in an even-handed way. As such, the preprocessing of each system includes a load normalization procedure, as otherwise it is unclear if the snapshot loadings in the case descriptor represent high or low loading conditions for that system.

For this normalization, the previous security constrained unit commitment procedure is adapted. A uniform scaling variable α is introduced for each nodal demand, which are now considered as variables ($P_{d,b}^{Orig}$ is the parameter recording the nodal load specified in the case descriptor)

$$P_{d,b} = \alpha P_{d,b}^{Orig} \tag{8}$$

The maximum load that can be served while respecting the security constraints is obtained with this objective function:

$$max(\alpha) \tag{9}$$

This maximum loading provides a harmonized benchmark between systems, so that their loading levels can be varied below this limit in a consistent way.

C. `MILP_overload` implementation

One novel contribution of this work is articulating a new linear optimization approach to attacking a power system: `MILP_overload`. Within this optimization, prevailing generator outputs and bus loads are taken as known parameters and the only decision variables are binary selectors on which branches should be attacked. The same load flow approach as previously is used, though security constraints are omitted.

The binary decision vector O determines which branches are to be maliciously outaged, taking a value of 1 at lines which are to be removed from service. As only a limited number of branches, K, can be attacked simultaneously:

$$\sum_l O_l \leq K \tag{10}$$

Logical constraints [113] are imposed to model the effects of a line removal (this maintains linearity in a way that a multiplicative approach would not, and doesn't force voltage angles to be equal for buses at either end of an outaged branch)

$$F_{l,i\to j} = \begin{cases} \frac{\phi_i - \phi_j}{X_l}, & \text{if } O_l = 0 \\ 0, & \text{if } O_l = 1 \end{cases} \tag{11}$$

The objective function for this optimization should gauge the damage that the combined line outages impose on the system. An obvious approach is to maximise the flows across all remaining branches following the removals. However, as the variable F_l is inherently *signed*, its absolute value would have to be taken to implement this objective function directly, which would break linearity. Instead, the present implementation exploits a simplifying rule-of-thumb here. While removing a small number of lines from service will certainly affect power flow profiles, we can anticipate that power flow directions will not generally reverse completely on lines. As such we can generate a "predicted direction" parameter, D_l, based on the known pre-removal flows in the systems, F_l^{Orig}.

$$D_l = \begin{cases} 1, & \text{if } F_l^{Orig} > 0 \\ -1, & \text{if } F_l^{Orig} \leq 0 \end{cases} \tag{12}$$

Using this helper parameter, a linear objective function which sums the "assumed positive" flows can be written:

$$max \sum_l \frac{D_l F_l}{F_l^+} \tag{13}$$

The branch thermal ratings, F_l^+, are included, so this calculates percentage, rather than absolute, loadings.

For the avoidance of doubt: this attack strategy approximately maximises overloads in the system immediately after the attack set of lines are outaged, but gives no consideration to subsequent cascade dynamics. While it uses optimization techniques, there should be no expectation that it will find the globally optimal attack strategy for forcing a system into cascading failure.

IV. Test platform

A. Test network selection

This work uses nine small-to-medium sized test power systems from the NESTA archive [114]. This archive provides versions of many well known test systems: crucially, realistic branch thermal limits are included ([115] discusses some of the issues surrounding test case accuracy for cascading failure analysis.) Augmenting these vital thermal limits, branch short time emergency ratings (F_l^{++}) are set equal to 130% of normal thermal limits, consistent with [116]–[118]. In simulating cascade progression, branches are removed when their loading exceeds this level.

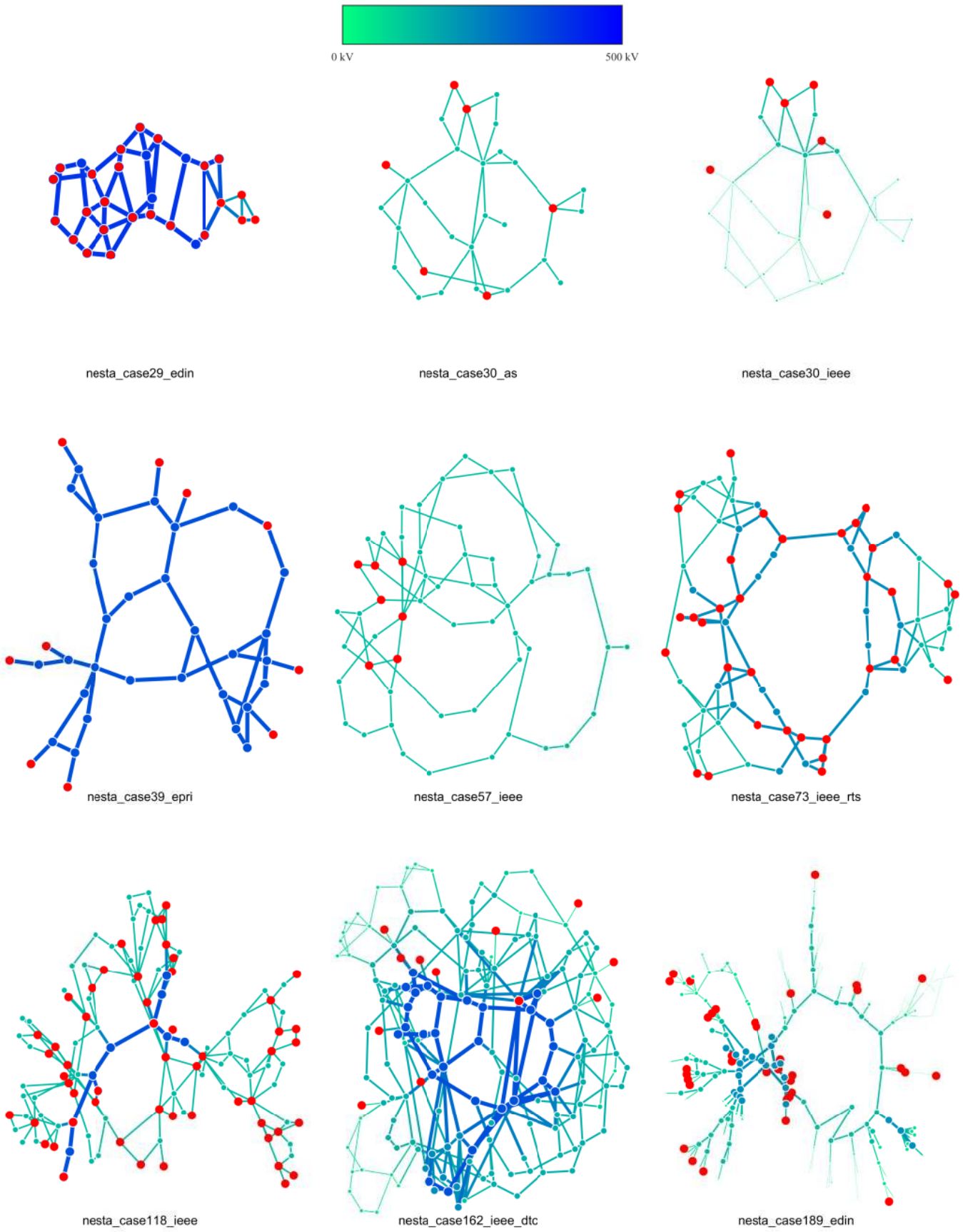

Fig. 1: Network diagrams for each test system considered. Generator nodes are plotted in red.

TABLE I:
Test System Characteristics

	nesta_case29_edin	nesta_case30_ieee		nesta_case57_ieee		nesta_case118_ieee			nesta_case189_edin
		nesta_case30_as		nesta_case39_epri		nesta_case73_ieee_rts		nesta_case162_ieee_dtc	
# Buses	29	30	30	39	57	73	118	162	189
# Branches	99	41	41	46	80	120	186	284	206
# Gen. Buses	24	6	6	10	7	33	54	12	35
Demand (GW)	81.492	0.357	0.278	6.228	1.377	10.216	5.037	5.283	1.863
Gen. Cap. (GW)	82.385	0.435	0.884	7.367	1.377	10.215	7.134	9.685	3.012

The diagrams in figure 1 show each of the test networks used, drawn as electrically meaningful diagrams per [119]. Note that `nesta_case29_edin` does not have nominal voltage levels specified, so it arbitrarily plotted here at 132 kV. System characteristic are given in Table I.

B. System and load normalisation

In each system, where multiple branches connected the same two buses, they were merged. This allows a fairer application of topological measures which don't consider that edges can have inherent redundancy. The merged line's impedance and thermal limits were updated to match the electrical characteristics of the multiline parallel combination. Overhead lines, cables and transformer are all treated equivalently, with no attack strategy making distinctions based on the class of branch.

1) System snapshot creation: As described in Section III, an optimisation procedure is used to discern the maximum possible loading that each system can serve while respecting the security constraints. These maximum loadings then provide a uniform benchmark from which system snapshots can be created in a fair way. Fifty representative system states were created for each system, so that meaningful statistical inferences can be made about each system's typical robustness. To create each snapshot, a pseudorandom number was first selected on a uniform distribution between 50% and 100%. This number was used to uniformly scale down all the spot loads in the system (By the normalization, loadings above 100% are known to be infeasible) Then, considering each snapshot separately, the generators are committed and dispatched to serve the prevailing loads in a security-constrained way.

As power grids will experience diverse power flow profiles over the coming years, due to variable renewables, load changes, outages and fuel price fluctuations, the set of snapshots should be widely heterogeneous in their generation schedules. To this end, the rows of cost parameters, c, were *shuffled* between generators for each snapshot. In this way, different generators become comparatively cheaper or costlier in each snapshot, and the optimization will, accordingly, produce a set of widely diverse generation schedules. This provides a broad sample of conceivable power flow profiles which also respecting $(N-1)$ security constraints: notably, purely random generation schedules cannot satisfy the latter criteria.

C. Attack simulation

The evolution of cascading failures is simulated using the MATCASC tool [58]. Each time it is invoked, it takes as input a particular system in a specific state, as well as pre-computed set of lines to attack, corresponding to a particular strategy.

In the first stage of each cascade simulation, the branches slated for attack are removed from the system, and a DC power flow calculation is performed. Subsequently, any lines whose active power flows exceed their emergency limits are also removed, and so on until an equilibrium is reached. Where islands form, load and generation are rebalanced there to maintain a local supply/demand balance. This tool is adequate to simulate the basic propagation mechanism of overload cascades, but it neglects various other effects which may arise in practice [115]:

- Reactive power and voltage magnitudes are entirely absent under the DC assumptions, so voltage stability is ignored
- Generator dynamics are not considered, so loss of synchronism and frequency instability are not considered
- Operator defensive actions, as recounted in Section II-F, are not simulated. It is assumed that the attacked branches are removed simultaneously, and that the resulting overload cascade propagates too rapidly for operator intervention.

For the avoidance of doubt: the MATCASC tool is used to simulate how effective each attack strategy might be. In addition to this role as an attack simulator, it is also used elsewhere by the genetic algorithm that constructs the `GA_demand` and `GA_link` attack sets.

D. Computational platform

Power system optimizations are formulated using YALMIP [120] and MATPOWER [121] in MATLAB [122], and use the Gurobi solver [123]. When calculating the `MILP_overload` attacks, Gurobi is given a time budget $= 30s$, simply due to the number of different attacks that must be simulated.

The `GA_demand` and `GA_links` attacks are found using the standard genetic algorithms settings and implementations in MATPOWER [122], [124], again with a $30s$ time limit imposed.

V. Results

Each attack strategy was applied to fifty different instantiations of each of the nine test systems. The attack strategies were calculated for each of $K = \{2, 3, 4, 5\}$.

TABLE II:
Mean Demand Survivability ($K = 2$)

	GA_link	GA_demand	MILP_overload	Loading	Elec_between	Topo_between	Shortcut	Random
nesta_case29_edin	0.2947	0.3604	0.5956	0.5905	0.5495	0.6224	0.5776	0.5622
nesta_case30_as	0.6971	0.8390	0.9337	0.9498	0.9049	0.9512	0.9512	0.9517
nesta_case30_ieee	0.7561	0.8034	0.9000	0.8302	0.9512	0.9512	0.9512	0.9517
nesta_case39_epri	0.7417	0.8174	0.9357	0.9565	0.9565	0.9565	0.8870	0.9513
nesta_case57_ieee	0.8890	0.9605	0.9663	0.9735	0.9598	0.9750	0.9750	0.9733
nesta_case73_ieee_rts	0.8627	0.8810	0.9753	0.9673	0.9833	0.9833	0.9833	0.9792
nesta_case118_ieee	0.5586	0.6594	0.7894	0.8320	0.8045	0.8083	0.8708	0.8622
nesta_case162_ieee_dtc	0.9087	0.9217	0.9521	0.9710	0.9669	0.9907	0.9743	0.9783
nesta_case189_edin	0.6227	0.6672	0.9187	0.9596	0.9806	0.9806	0.9850	0.9651

TABLE II:
Mean Demand Survivability ($K = 3$)

	GA_link	GA_demand	MILP_overload	Loading	Elec_between	Topo_between	Shortcut	Random
nesta_case29_edin	0.2594	0.3499	0.5576	0.6085	0.5495	0.5384	0.6341	0.5598
nesta_case30_as	0.4537	0.7410	0.7229	0.9205	0.8785	0.9200	0.9268	0.9239
nesta_case30_ieee	0.2683	0.3756	0.2229	0.8122	0.9024	0.9268	0.9268	0.9244
nesta_case39_epri	0.5900	0.7057	0.8722	0.8648	0.9348	0.9348	0.7513	0.9239
nesta_case57_ieee	0.7835	0.8645	0.9145	0.9597	0.9472	0.9625	0.9625	0.9592
nesta_case73_ieee_rts	0.7907	0.8192	0.9450	0.9462	0.9750	0.9750	0.9710	0.9700
nesta_case118_ieee	0.5329	0.6217	0.7383	0.8057	0.7991	0.7747	0.8917	0.8401
nesta_case162_ieee_dtc	0.8671	0.9198	0.9232	0.9423	0.9625	0.9872	0.9693	0.9748
nesta_case189_edin	0.6013	0.6540	0.8327	0.9354	0.9631	0.9631	0.9803	0.9717

TABLE II:
Mean Demand Survivability ($K = 4$)

	GA_link	GA_demand	MILP_overload	Loading	Elec_between	Topo_between	Shortcut	Random
nesta_case29_edin	0.2390	0.3158	0.5608	0.5925	0.5099	0.5384	0.6341	0.5481
nesta_case30_as	0.3410	0.7283	0.6707	0.8893	0.8312	0.8205	0.9024	0.8922
nesta_case30_ieee	0.0951	0.1985	0.2649	0.7941	0.8780	0.9024	0.9024	0.9010
nesta_case39_epri	0.4922	0.6196	0.8013	0.8174	0.9130	0.9130	0.6078	0.9026
nesta_case57_ieee	0.7190	0.8142	0.8538	0.9290	0.9315	0.9500	0.9500	0.9460
nesta_case73_ieee_rts	0.7647	0.7767	0.9118	0.9327	0.9667	0.9507	0.9667	0.9490
nesta_case118_ieee	0.5185	0.6245	0.7232	0.7992	0.7847	0.7302	0.8484	0.8224
nesta_case162_ieee_dtc	0.8799	0.8909	0.8889	0.9160	0.9596	0.9619	0.9663	0.9682
nesta_case189_edin	0.5625	0.6531	0.7973	0.9123	0.9583	0.9414	0.9755	0.9403

TABLE II:
Mean Demand Survivability ($K = 5$)

	GA_link	GA_demand	MILP_overload	Loading	Elec_between	Topo_between	Shortcut	Random
nesta_case29_edin	0.2196	0.3271	0.5568	0.5770	0.5099	0.5354	0.6321	0.5166
nesta_case30_as	0.3005	0.6951	0.6395	0.8576	0.7961	0.7800	0.8780	0.8571
nesta_case30_ieee	0.0688	0.1498	0.1551	0.7727	0.4439	0.8780	0.8780	0.8459
nesta_case39_epri	0.4304	0.5657	0.7417	0.7783	0.8913	0.8696	0.6070	0.8800
nesta_case57_ieee	0.6800	0.7538	0.6900	0.9138	0.9180	0.9375	0.9375	0.9310
nesta_case73_ieee_rts	0.7355	0.7663	0.8998	0.9287	0.9583	0.9507	0.9583	0.9397
nesta_case118_ieee	0.4996	0.5752	0.7305	0.7835	0.7335	0.7040	0.8397	0.8273
nesta_case162_ieee_dtc	0.8461	0.8896	0.8751	0.9063	0.9391	0.9747	0.9626	0.9675
nesta_case189_edin	0.5591	0.6202	0.7130	0.8816	0.9534	0.9087	0.9708	0.9476

A. Summary statistics

The first high level summary of this data is given Tables II to V (underlying raw data is available at [125]). These tables show the mean efficacy of each attack strategy, as measured by the post-cascade demand survivability ($0 \rightarrow$ total blackout, $1 \rightarrow$ no effect). The attack strategies are ordered with the most effective shown to the left, with darker, redder shading highlighting the most worrying mean survivability value.

As expected, increasing K decreases the demand survivability across the board: all attack strategies become more effective as more branches are removed.

1) Computational attack strategies: The three intelligent computational strategies are the most effective, by a wide margin. This shows that indicators and predictors for nonlinear phenomena like cascading failure cannot compete with direct simulations and contextual knowledge.

The two genetic algorithm approaches have largely equivalent performance, with both routinely capable of triggering large, damaging cascades. With $K = 3$ or 4, a typical attack with these strategies is potentially devastating, with half the load in the system interrupted in many cases. Knowledge of the system state, coupled with even crude computational techniques, allows hugely disruptive attacks to be orchestrated, where removing just a few exposed assets triggers widespread damage. Recall also that the $30s$ time budget for these computations is merely an expedient for the present research: in practice, more computational resources could be used, and yet more damaging attacks found.

Oddly, the genetic algorithm which minimizes the link survivability, `GA_link`, achieved the lowest mean values for demand survivability, and outperforms the strategy specifically targeting that metric, `GA_demand`.

While the linear programming approach is firmly in third place overall, it cannot compete with the (deliberately simplistic) genetic algorithms which directly enumerate effective attack strategies. Even with its tailored objective function, the nonlinear dynamics of overload cascades pose a serious challenge to classical optimization techniques

2) `Loading` attack strategy: The `Loading` attack here is the fourth most damaging, and can typically interrupt perhaps 10% of system demand: its demonstrated effectiveness is consistent with works such as [107]. It solely exploits contextual knowledge of instantaneous power flow levels, and in so doing it outperforms the topological measures. This shows that the prevailing conditions on a power system are vital when assessing its robustness. This also underlines the need for simulating cascades on multiple snapshots of a system: a system's propensity to failure is not simply dependant on its static topology. It also suggests that if a power system's state can be remotely monitored by malicious cyber intrusions, than the system's physical security becomes jeopardised.

3) Topological attack strategies: The three topological attack strategies exhibit similarly benign performance: none typically do much damage to a power system for the K values considered. While the domain-specific `Elec_between` does marginally the best of the three, it is still outperformed by the simple strategy of attacking the most heavily loaded lines. The broadly equivalent performance of `Elec_between` and `Topo_between` cast doubt on works such as [42], which discerned a categorical distinction between these measures.

As expected, the random attack strategy is the least effective.

4) Network specific robustness: The robustness of each network varies widely: for instance, `nesta_case29_edin` is rather fragile, while `nesta_case162_ieee_dtc` appears quite secure. Likewise, even though `nesta_case30_as` and `nesta_case30_ieee` are similar in connective structure (see figure 1), their response to attacks are markedly different.

B. Effect of prevailing demand level for $K = 5$

The scatterplot matrix in figure 2 disaggregates the summary statistics presented in Table IV, showing the prevailing load level and achieved demand survivability for every snapshot considered for the $K = 5$ case (space restrictions preclude such a display for every K value)

The two leftmost columns in figure 2 again show how very effective the metahueristic approach to branch interdiction is. If `nesta_case57_ieee` is disregarded, being impregnably robust, than nearly all other attacks on the eight other systems, in their fifty diverse conditions, are successful. This establishes that the mean values discussed previously are meaningful summary statistics.

1) System loading level and robustness: While intuition may suggest that power grids are most vulnerable when they are most heavily loaded, this in not necessarily so. For instance, the authors of [38] observe: *"Surprisingly, this calculation illustrates that risk can sometimes decrease as load increases."*

Certain panes in figure 2 strongly support this: consider the `nesta_case30_ieee` system under the `Loading` attack. Here two regimes are evident: some portion of the attacks are ineffective, resulting in the flat green line to the top of the pane. On the other hand, some attacks are very effective indeed, represented by the piecewise linear red line to the bottom of the pane. Note that the severity of attacks in the lower regime is *lessened* with *increasing* load. None of the fifty simulated attacks falls between these regimes. Note also that the three smart attack strategies to the left of (`nesta_case30_ieee`, `Loading`) are near-universally effective at crippling this system, whereas at the four rightmost strategies are near-universally ineffective. Only the `Loading` strategy straddles these, and it does so in a curiously bimodal way.

In no other panes is the relationship between survivability and loadings so clearly linear, though the same general trend can be inferred in e.g (`nesta_case162_ieee_dtc`, `Loading`) and (`nesta_case162_ieee_dtc`, `MILP_overload`). Conversely, the opposite trend, where higher loadings predict lower survivability, also manifests, for instance in (`nesta_case30_as`, `GA_demand`) and (`nesta_case30_as`, `MILP_overload`)

There are also stepchanges in how loading affects survivability. The clearest example here is (`nesta_case189_edin`, `Topo_between`), where the attack strategy become suddenly more effective when net system load exceeds $\sim 70\%$. A less clearly defined regime seperation is evident in the bottom right of (`nesta_case189_edin`, `GA_link`), where devastating

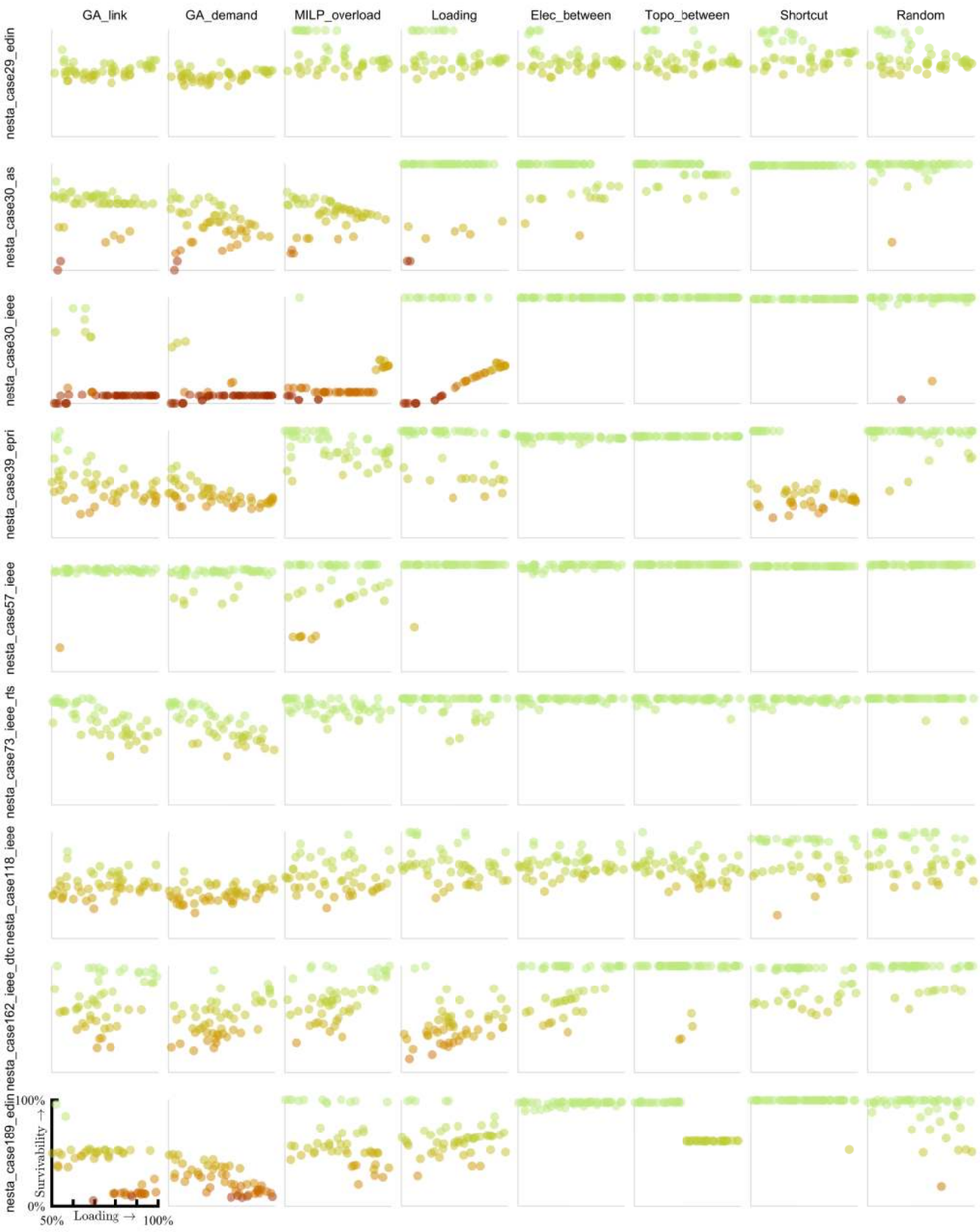

Fig. 2: The demand survivability versus the system loading level, shown for the fifty snapshots considered for the $K = 5$ case

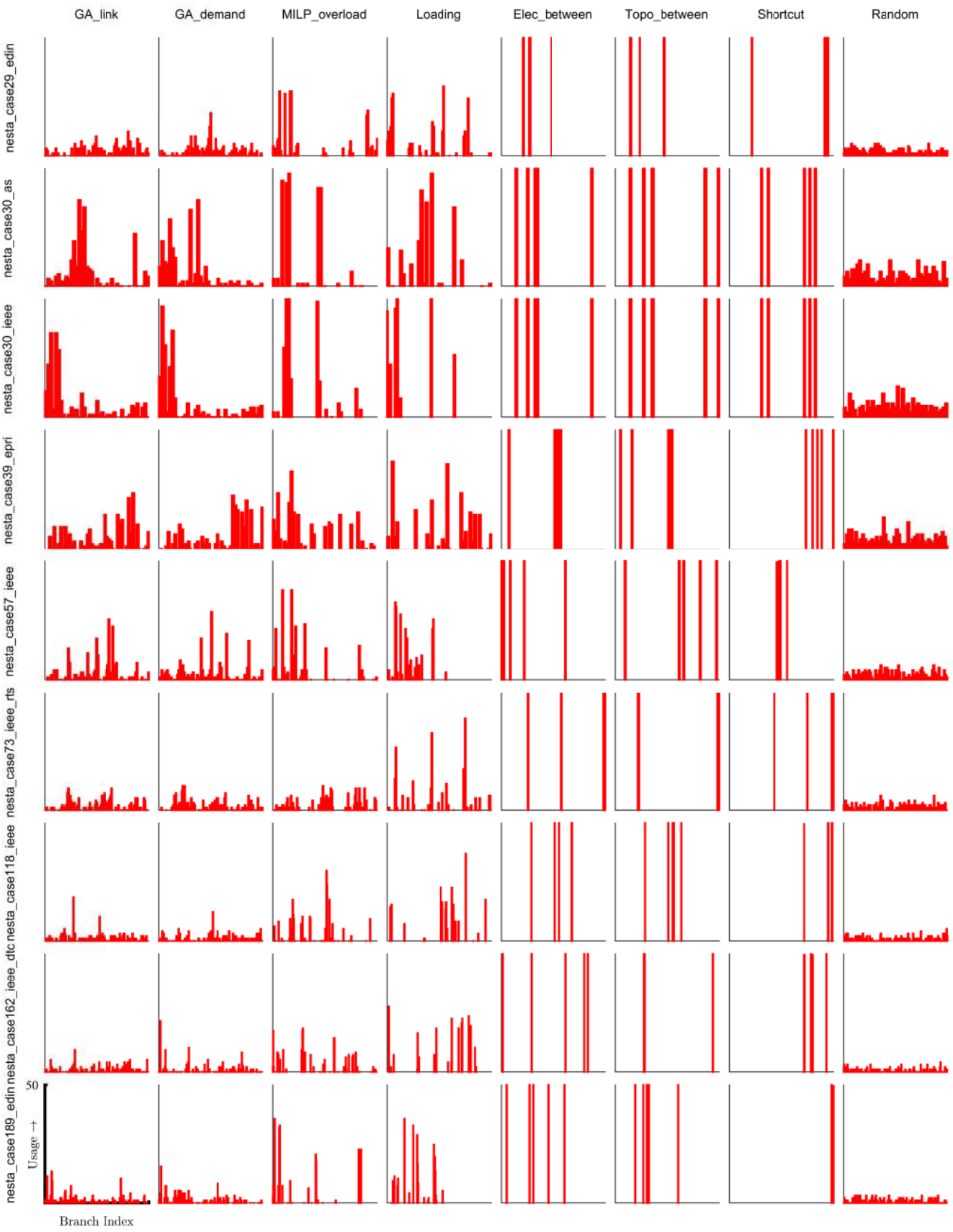

Fig. 3: Histograms showing how often each individual line was interdicted over the fifty snapshots of each system simulated for the $K = 5$ case

attacks become possible, though not certain, when loadings exceed $\sim 80\%$. A third example of loading stepchanges is in (`nesta_case39_epri`, `Shortcut`), where once loadings exceed $\sim 65\%$ all attacks become significant, though of diverse severity.

The disaggregation in figure 2 also shows how much attack effectiveness varies between each system snapshot simulated. Many of the panes here show diffuse and noisy data, making clear that each individual data point offers very limited insight on the general robustness of a network. It is clear that a network's propensity to cascading failure is deeply connected to the prevailing initial conditions, and this conclusion is consistent with [126], which states clearly that *"each cascade is strongly and jointly influenced by the initial system state and the trigger event."*

C. Branch selection analysis for $K = 5$

The barchart matrix in figure 3 complements figure 2. Each vertical bar corresponds to a specific branch in each system, and its height shows how often it was included as part of a particular attack combination over the fifty simulated snapshots. Three of the strategies considered are static and topology based, and do not vary between snapshots, so these panes are of limited interest. Likewise, the `Random` column to the far right simply approximates a uniform distribution, as expected. The four leftmost columns are of most interest, as they offer insights on whether consistently effective attack strategies make repeated use of certain branches when attacking systems under fluctuating conditions.

1) Specific branch vulnerability: Do certain branches always form promising attack vectors, even as system conditions change? There does not appear to be universal answer to this question. For instance, the systems `nesta_case30_as` and `nesta_case30_ieee` appear to have consistently vulnerable branches: note the strong peaks evident in the leftmost four histograms for these systems. However, each attack strategy seems to have its own particular set of favoured selections here.

This is not the case for other systems. For instance, the highly effective (per Table IV) `GA_link` attack against `nesta_case189_edin` selects over a wide gamut of branches, to interdict as circumstances dictate. The flatness of this pane makes clear that no branches in this system have any innate vulnerability: rather, their attractiveness as attack targets is a function of the prevailing conditions.

VI. Conclusion

This work used a simplified cascading failure model to assess how electrical grids might fare against attacks deliberately orchestrated against their branches. Contextual, topological and computational techniques were deployed to select which branches to attack. Some clear trends emerged:

Untuned, generic metaheuristic algorithms, with just a short computational time permitted, can find consistently damaging branch interdiction strategies. If the system state is known, and five branches can be removed from service, than most electrical grids will sustain serious damage most of the time. While mathematical optimization can also find promising branches to attack, the formulation used in the present work was outperformed by the simple metaheuristics. As only limited computational time was made available to compute these attacks, and as the attack simulations only considered simple overload cascade dynamics, it is likely that metaheuristic based attacks would be *yet more* effective in reality.

Attack strategies which exploit knowledge of the instantaneous state of the power system substantially outperform static topological measures from the complex network literature, even where such measures incorporate some electrical flavour. It appears that the robustness of electric power systems varies widely depending on the prevailing conditions.

The effective attack strategies selected widely from the available branches depending on the prevailing system conditions. This speaks against the idea of particular branches having innate criticality for the system's integrity.

Most attack strategies on most systems showed diverse performance as the system state changed: one instantaneous snapshot of a system is therefore inadequate for drawing general conclusions on its robustness.

Acknowledgment

The author would like to thank Yakup Koç, who graciously provided the MATCASC software for performing cascading failure analyses.

References

[1] H. A. Khan, Z. Xu, H. Iu, *et al.*, "Review of technologies and implementation strategies in the area of smart grid," in *Power Engineering Conference, 2009. AUPEC 2009. Australasian Universities*, Sep. 2009, pp. 1–6.

[2] C.-W. Ten, A. Ginter, and R. Bulbul, "Cyber-based contingency analysis," *IEEE Transactions on Power Systems*, vol. 31, no. 4, pp. 3040–3050, 2016.

[3] A. Srivastava, T. Morris, T. Ernster, *et al.*, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 235–244, Mar. 2013.

[4] G. Liang, S. R. Weller, J. Zhao, *et al.*, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, 2016.

[5] Vaiman, Bell, Chen, *et al.*, "Risk assessment of cascading outages: Methodologies and challenges," *IEEE Transactions on Power Systems*, vol. 27, no. 2, pp. 631–641, May 2012.

[6] Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack Board on Energy and Environmental Systems Division on Engineering and Physical Sciences, *Terrorism and the Electric Power Delivery System*. The National Academies Press, 2012.

[7] R. V. Solé, M. Rosas-Casals, B. Corominas-Murtra, *et al.*, "Robustness of the european power grids under intentional attack," *Phys. Rev. E*, vol. 77, p. 026 102, 2 Feb. 2008.

[8] M. Rosas-Casals, S. Valverde, and R. V. Solé, "Topological vulnerability of the European power grid under errors and attacks," *International Journal of Bifurcation and Chaos*, vol. 17, no. 07, pp. 2465–2475, 2007.

[9] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Phys. Rev. E*, vol. 69, p. 025 103, 2 Feb. 2004.

[10] A. J. Holmgren, "Using graph models to analyze the vulnerability of electric power networks," *Risk Analysis*, vol. 26, no. 4, pp. 955–969, 2006.

[11] J.-W. Wang and L.-L. Rong, "Cascade-based attack vulnerability on the US power grid," *Safety Science*, vol. 47, no. 10, pp. 1332–1336, 2009.

[12] "Policy 3: Operational security," in *Continental Europe Operation Handbook*, ENTSO-E, ch. 3.

[13] J. Bialek, E. Ciapessoni, D. Cirio, *et al.*, "Benchmarking and validation of cascading failure analysis tools," *IEEE Transactions on Power Systems*, vol. PP, no. 99, pp. 1–14, 2016.

[14] Q. Chen and J. D. McCalley, "Identifying high risk nk contingencies for online security assessment," *IEEE Transactions on Power Systems*, vol. 20, no. 2, pp. 823–834, 2005.

[15] G. A. Pagani and M. Aiello, "The power grid as a complex network: A survey," *Physica A: Statistical Mechanics and its Applications*, vol. 392, no. 11, pp. 2688–2700, 2013.

[16] K. Sun, "Complex networks theory: A new method of research in power grid," in *2005 IEEE/PES Transmission Distribution Conference Exposition: Asia and Pacific*, 2005, pp. 1–6.

[17] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks," *Rev. Mod. Phys.*, vol. 74, pp. 47–97, 1 Jan. 2002.

[18] D. P. Chassin and C. Posse, "Evaluating North American electric grid reliability using the Barabasi-Albert network model," *Physica A: Statistical Mechanics and its Applications*, vol. 355, no. 2–4, pp. 667–677, 2005.

[19] P. Crucitti, V. Latora, and M. Marchiori, "A topological analysis of the Italian electric power grid," *Physica A: Statistical Mechanics and its Applications*, vol. 338, no. 1–2, pp. 92–97, 2004.

[20] R. Kinney, P. Crucitti, R. Albert, *et al.*, "Modeling cascading failures in the North American power grid," *The European Physical Journal B-Condensed Matter and Complex Systems*, vol. 46, no. 1, pp. 101–107, 2005.

[21] E. Bompard, L. Luo, and E. Pons, "A perspective overview of topological approaches for vulnerability analysis of power transmission grids," *International Journal of Critical Infrastructures 7*, vol. 11, no. 1, pp. 15–26, 2015.

[22] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability?" *Chaos*, vol. 20, no. 3, 033122, 2010.

[23] T. Verma, W. Ellens, and R. E. Kooij, "Context-independent centrality measures underestimate the vulnerability of power grids," *International Journal of Critical Infrastructures 7*, vol. 11, no. 1, pp. 62–81, 2015.

[24] M. Ouyang, "Review on modeling and simulation of interdependent critical infrastructure systems," *Reliability engineering & System safety*, vol. 121, pp. 43–60, 2014.

[25] E. Galli, "Agent based modeling and simulation for critical and interdependent systems," PhD thesis, PhD Dissertation, Rome: Universita di Roma, 2010.

[26] M. Schläpfer, T. Kessler, and W. Kröger, "Reliability analysis of electric power systems using an object-oriented hybrid modeling approach," *ArXiv preprint arXiv:1201.0552*, 2012.

[27] M. Halappanavar, E. Cotilla-Sanchez, E. Hogan, *et al.*, "A network-of-networks model for electrical infrastructure networks," *ArXiv preprint arXiv:1512.01436*, 2015.

[28] P. D. Hines, S. Blumsack, and M. Schläpfer, "Centralized versus decentralized infrastructure networks," *ArXiv preprint arXiv:1510.08792*, 2015.

[29] P. D. Hines, I. Dobson, and P. Rezaei, "Cascading power outages propagate locally in an influence graph that is not the actual grid topology," *ArXiv preprint arXiv:1508.01775*, 2015.

[30] E. Cotilla-Sanchez, P. D. Hines, C. Barrows, *et al.*, "Multi-attribute partitioning of power networks based on electrical distance," *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 4979–4987, 2013.

[31] E. Cotilla-Sanchez, P. D. Hines, C. Barrows, *et al.*, "Comparing the topological and electrical structure of the North American electric power infrastructure," *IEEE Systems Journal*, vol. 6, no. 4, pp. 616–626, 2012.

[32] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, "Topological models and critical slowing down: Two approaches to power system blackout risk analysis," in *System Sciences (HICSS), 2011 44th Hawaii International Conference on*, IEEE, 2011, pp. 1–10.

[33] P. Hines and S. Blumsack, "A centrality measure for electrical networks," in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, IEEE, 2008, pp. 185–185.

[34] J. Song, E. Cotilla-Sanchez, G. Ghanavati, *et al.*, "Dynamic modeling of cascading failure in power systems," *IEEE Transactions on Power Systems*, vol. 31, no. 3, pp. 2085–2095, 2016.

[35] P. Rezaei, M. J. Eppstein, and P. D. Hines, "Rapid assessment, visualization, and mitigation of cascading failure risk in power systems," in *System Sciences (HICSS), 2015 48th Hawaii International Conference on*, IEEE, 2015, pp. 2748–2758.

[36] M. Korkali, J. G. Veneman, B. F. Tivnan, *et al.*, "Reducing cascading failure risk by increasing infrastructure network interdependency," *ArXiv preprint arXiv:1410.6836*, 2014.

[37] P. Rezaei, P. D. Hines, and M. Eppstein, "Estimating cascading failure risk: Comparing Monte Carlo sampling and random chemistry," in *2014 IEEE PES General Meeting—Conference & Exposition*, IEEE, 2014, pp. 1–5.

[38] P. Rezaei, P. D. Hines, and M. J. Eppstein, "Estimating cascading failure risk with random chemistry," *IEEE Transactions on Power Systems*, vol. 30, no. 5, pp. 2726–2735, 2014.

[39] P. Rezaei and P. D. Hines, "Changes in cascading failure risk with generator dispatch method and system load level," in *2014 IEEE PES T&D Conference and Exposition*, IEEE, 2014, pp. 1–5.

[40] M. J. Eppstein and P. D. Hines, "A 'random chemistry' algorithm for identifying collections of multiple contingencies that initiate cascading failure," *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1698–1705, 2012.

[41] P. D. Hines, B. OHara, and E. Cotilla-Sanchez, "Cascading failures: Extreme properties of large blackouts in the electric grid," *SIAM Math Awareness Month Essay*, 2011.

[42] A. Estebsari, T. Huang, E. Pons, *et al.*, "Infrastructure enhancement for the security of transmission systems against coordinated malicious attack," in *16th IEEE International Conference on Environment and Electrical Engineering*, Jun. 2016.

[43] E. Bompard, A. Estebsari, T. Huang, *et al.*, "A framework for analyzing cascading failure in large interconnected power systems: A post-contingency evolution simulator," *International Journal of Electrical Power & Energy Systems*, vol. 81, pp. 12–21, 2016.

[44] E. Bompard, E. Pons, and D. Wu, "Analysis of the structural vulnerability of the interconnected power grid of continental Europe with the integrated power system and unified power system based on extended topological approach," *International Transactions on Electrical Energy Systems*, vol. 23, no. 5, pp. 620–637, 2013.

[45] E. Bompard, E. Pons, and D. Wu, "Extended topological metrics for the analysis of power grid vulnerability," *IEEE Systems Journal*, vol. 6, no. 3, pp. 481–487, Sep. 2012.

[46] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, no. 7, pp. 1334–1340, 2011.

[47] E. Bompard, R. Napoli, and F. Xue, "Extended topological approach for the assessment of structural vulnerability in transmission networks," *IET Generation, Transmission Distribution*, vol. 4, no. 6, pp. 716–724, Jun. 2010.

[48] E. Bompard, C. Gao, R. Napoli, *et al.*, "Risk assessment of malicious attacks against power systems," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 39, no. 5, pp. 1074–1085, Sep. 2009.

[49] E. Bompard, R. Napoli, and F. Xue, "Analysis of structural vulnerabilities in power transmission grids," *International Journal of Critical Infrastructure Protection*, vol. 2, no. 1–2, pp. 5–12, 2009.

[50] E. Bompard, M. Masera, R. Napoli, *et al.*, "Assessment of structural vulnerability for power grids by network performance based on complex networks," in *Critical Information Infrastructure Security: Third International Workshop, CRITIS 2008, Rome, Italy, October 13-15, 2008. Revised Papers*, R. Setola and S. Geretshuber, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009, pp. 144–154, ISBN: 978-3-642-03552-4.

[51] E. Bompard, R. Napoli, and F. Xue, "Assessment of information impacts in power system security against malicious attacks in a general framework," *Reliability Engineering & System Safety*, vol. 94, no. 6, pp. 1087–1094, 2009.

[52] E. Bompard, R. Napoli, and F. Xue, "Vulnerability of interconnected power systems to malicious attacks under limited information," *European Transactions on Electrical Power*, vol. 18, no. 8, pp. 820–834, 2008.

[53] X. Wang, Y. Koç, R. E. Kooij, *et al.*, "A network approach for power grid robustness against cascading failures," in *Reliable Networks Design and Modeling (RNDM), 2015 7th International Workshop on*, IEEE, 2015, pp. 208–214.

[54] Y. Koç, M. Warnier, P. Van Mieghem, *et al.*, "A topological investigation of phase transitions of cascading failures in power grids," *Physica A: Statistical Mechanics and its Applications*, vol. 415, pp. 273–284, 2014.

[55] ——, "The impact of the topology on cascading failures in a power grid model," *Physica A: Statistical Mechanics and its Applications*, vol. 402, pp. 169–179, 2014.

[56] Y. Koç, M. Warnier, R. Kooij, *et al.*, "Structural vulnerability assessment of electric power grids," in *Networking, Sensing and Control (ICNSC), 2014 IEEE 11th International Conference on*, IEEE, 2014, pp. 386–391.

[57] Y. Koç, M. Warnier, R. E. Kooij, *et al.*, "An entropy-based metric to quantify the robustness of power grids against cascading failures," *Safety science*, vol. 59, pp. 126–134, 2013.

[58] Y. Koç, T. Verma, N. A. Araujo, *et al.*, "Matcasc: A tool to analyse cascading line outages in power grids," in *Intelligent Energy Systems (IWIES), 2013 IEEE International Workshop on*, IEEE, 2013, pp. 143–148.

[59] Y. Koç, M. Warnier, R. E. Kooij, *et al.*, "A robustness metric for cascading failures by targeted attacks in power networks," in *Networking, Sensing and Control (ICNSC), 2013 10th IEEE International Conference on*, IEEE, 2013, pp. 48–53.

[60] X. Zhang and C. K. Tse, "Assessment of robustness of power systems from a network perspective," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 5, no. 3, pp. 456–464, Sep. 2015.

[61] M. Vaiman, K. Bell, Y. Chen, *et al.*, "Risk assessment of cascading outages: Part i; overview of methodologies," in *2011 IEEE Power and Energy Society General Meeting*, Jul. 2011, pp. 1–10.

[62] R. Baldick, B. Chowdhury, I. Dobson, *et al.*, "Initial review of methods for cascading failure analysis in electric power transmission systems IEEE PES CAMS Task Force on understanding, prediction, mitigation and restoration of cascading failures," in *Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008 IEEE*, Jul. 2008, pp. 1–8.

[63] M. Papic, K. Bell, Y. Chen, *et al.*, "Survey of tools for risk assessment of cascading outages," in *2011 IEEE Power and Energy Society General Meeting*, Jul. 2011, pp. 1–9.

[64] J. Yan, Y. Tang, H. He, *et al.*, "Cascading failure analysis with DC power flow model and transient stability analysis," *IEEE Transactions on Power Systems*, vol. 30, no. 1, pp. 285–297, 2015.

[65] B. P. van Milligen, B. Carreras, and D. Newman, "Constructing criteria to diagnose the likelihood of extreme events in the case of the electric power grid," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 26, no. 3, p. 033 109, 2016.

[66] A. Darvishi and I. Dobson, "Threshold-based monitoring of cascading outages with PMU measurements of area angle," *IEEE Transactions on Power Systems*, vol. 31, no. 3, pp. 2116–2124, 2016.

[67] B. Carreras, D. Newman, I. Dobson, *et al.*, "The impact of local power balance and link reliability on blackout risk in heterogeneous power transmission grids," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, IEEE, 2016, pp. 2584–2593.

[68] B. A. Carreras, D. E. Newman, and I. Dobson, "North American blackout time series statistics and implications for blackout risk," *IEEE Transactions on Power Systems*, 2016.

[69] B. A. Carreras, D. Newman, and I. Dobson, "Does size matter?" *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 24, no. 2, p. 023 104, 2014.

[70] I. Dobson, "Estimating the propagation and extent of cascading line outages from utility data with a branching process," *IEEE Transactions on Power Systems*, vol. 27, no. 4, pp. 2116–2126, 2012.

[71] J. Kim, K. R. Wierzbicki, I. Dobson, *et al.*, "Estimating propagation and distribution of load shed in simulations of cascading blackouts," *IEEE Systems Journal*, vol. 6, no. 3, pp. 548–557, 2012.

[72] B. A. Carreras, D. E. Newman, and I. Dobson, "Determining the vulnerabilities of the power transmission system,"

in *Forty-fifth Hawaii International Conference on System Sciences, Maui, Hawaii*, 2012.

[73] D. E. Newman, B. A. Carreras, V. E. Lynch, *et al.*, "Exploring complex systems aspects of blackout risk and mitigation," *IEEE Transactions on Reliability*, vol. 60, no. 1, pp. 134–143, 2011.

[74] ——, "Evaluating the effect of upgrade, control and development strategies on robustness and failure risk of the power transmission grid," in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*, IEEE, 2008, pp. 182–182.

[75] H. Ren and I. Dobson, "Using transmission line outage data to estimate cascading failure propagation in an electric power system," *Circuits and Systems II: Express Briefs, IEEE Transactions on*, vol. 55, no. 9, pp. 927–931, 2008.

[76] H. Ren, I. Dobson, and B. A. Carreras, "Long-term effect of the N-1 criterion on cascading line outages in an evolving power transmission grid," *IEEE transactions on power systems*, vol. 23, no. 3, pp. 1217–1225, 2008.

[77] I. Dobson, B. A. Carreras, and D. E. Newman, "A loading-dependent model of probabilistic cascading failure," *Probability in the Engineering and Informational Sciences*, vol. 19, no. 1, pp. 15–32, 2005.

[78] B. A. Carreras, D. E. Newman, I. Dobson, *et al.*, "Evidence for self-organized criticality in a time series of electric power system blackouts," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 51, no. 9, pp. 1733–1740, 2004.

[79] Y. Wang and R. Baldick, "Interdiction analysis of electric grids combining cascading outage and medium-term impacts," *IEEE Transactions on Power Systems*, vol. 29, no. 5, pp. 2160–2168, Sep. 2014.

[80] J. Hur, M.-H. Joung, and R. Baldick, "Sequential outage checkers for analyzing cascading outages and preventing large blackouts," *Journal of Electrical Engineering and Technology*, vol. 6, no. 5, pp. 585–594, 2011.

[81] A. Pinar, J. Meza, V. Donde, *et al.*, "Optimization strategies for the vulnerability analysis of the electric power grid," *SIAM Journal on Optimization*, vol. 20, no. 4, pp. 1786–1810, 2010.

[82] D. Bienstock and A. Verma, "The nk problem in power grids: New models, formulations, and numerical experiments," *SIAM Journal on Optimization*, vol. 20, no. 5, pp. 2352–2380, 2010.

[83] V. Donde, V. Lopez, B. Lesieutre, *et al.*, "Severe multiple contingency screening in electric power systems," *IEEE Transactions on Power Systems*, vol. 23, no. 2, pp. 406–417, May 2008.

[84] L. Agudelo, J. M. López-Lezama, and N. Muñoz-Galeano, "Vulnerability assessment of power systems to intentional attacks using a specialized genetic algorithm," *Dyna*, vol. 82, no. 192, pp. 78–84, 2015.

[85] J. M. Arroyo and F. J. Fernandez, "A genetic algorithm approach for the analysis of electric grid interdiction with line switching," in *Intelligent System Applications to Power Systems, 2009. ISAP '09. 15th International Conference on*, Nov. 2009, pp. 1–6.

[86] J. M. Arroyo and F. J. Fernandez, "Application of a genetic algorithm to N-K power system security assessment," *International Journal of Electrical Power & Energy Systems*, vol. 49, pp. 114–121, 2013.

[87] N. Romero, N. Xu, L. K. Nozick, *et al.*, "Investment planning for electric power systems under terrorist threat," *IEEE Transactions on Power Systems*, vol. 27, no. 1, pp. 108–116, Feb. 2012.

[88] N. Romero, N. Xu, L. K. Nozick, *et al.*, "Investment planning for electric power systems under terrorist threat," *Power Systems, IEEE Transactions on*, vol. 1, no. 99, pp. 108–116, 2012.

[89] Y. Wang, J. Zhao, F. Zhang, *et al.*, "Study on structural vulnerabilities of power grids based on the electrical distance," in *IEEE PES Innovative Smart Grid Technologies*, IEEE, 2012, pp. 1–5.

[90] E. Zio and R. Piccinelli, "Randomized flow model and centrality measure for electrical power transmission network analysis," *Reliability Engineering & System Safety*, vol. 95, no. 4, pp. 379–385, 2010.

[91] E. I. Bilis, W. Kröger, and C. Nan, "Performance of electric power systems under physical malicious attacks," *IEEE Systems Journal*, vol. 7, no. 4, pp. 854–865, 2013.

[92] T. A. Ernster and A. K. Srivastava, "Power system vulnerability analysis-towards validation of centrality measures," in *Transmission and Distribution Conference and Exposition (T&D), 2012 IEEE PES*, IEEE, 2012, pp. 1–6.

[93] J. Salmeron, K. Wood, and R. Baldick, "Analysis of electric grid security under terrorist threat," *IEEE Transactions on Power Systems*, vol. 19, no. 2, pp. 905–912, May 2004, ISSN: 0885-8950. DOI: 10.1109/TPWRS.2004.825888.

[94] J. Salmeron, K. Wood, and R. Baldick, "Optimizing electric grid design under asymmetric threat (ii)," Naval Postgraduate School Monterey CA Dept. Of Operations Research, Tech. Rep., 2004.

[95] J. M. Arroyo and F. D. Galiana, "On the solution of the bilevel programming formulation of the terrorist threat problem," *IEEE Transactions on Power Systems*, vol. 20, no. 2, pp. 789–797, 2005.

[96] J. M. Arroyo, "Bilevel programming applied to power system vulnerability analysis under multiple contingencies," *IET Generation, Transmission Distribution*, vol. 4, no. 2, pp. 178–190, Feb. 2010.

[97] A. Delgadillo, J. M. Arroyo, and N. Alguacil, "Analysis of electric grid interdiction with line switching," *IEEE Transactions on Power Systems*, vol. 25, no. 2, pp. 633–641, May 2010.

[98] A. L. Motto, J. M. Arroyo, and F. D. Galiana, "A mixed-integer lp procedure for the analysis of electric grid security under disruptive threat," *IEEE Transactions on Power Systems*, vol. 20, no. 3, pp. 1357–1365, 2005.

[99] N. Alguacil, A. Delgadillo, and J. M. Arroyo, "A trilevel programming approach for electric grid defense planning," *Computers & Operations Research*, vol. 41, pp. 282–290, 2014.

[100] J. Salmeron, K. Wood, and R. Baldick, "Worst-case interdiction analysis of large-scale electric power grids," *IEEE Transactions on Power Systems*, vol. 24, no. 1, pp. 96–104, Feb. 2009.

[101] L. Zhao and B. Zeng, "Vulnerability analysis of power grids with line switching," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 2727–2736, Aug. 2013.

[102] M. P. Scaparra and R. L. Church, "A bilevel mixed-integer program for critical infrastructure protection planning," *Computers & Operations Research*, vol. 35, no. 6, pp. 1905–1923, 2008.

[103] Y. Yao, T. Edmunds, D. Papageorgiou, *et al.*, "Trilevel optimization in power network defense," *IEEE Transactions*

on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 37, no. 4, pp. 712–718, Jul. 2007.

[104] W. Yuan, L. Zhao, and B. Zeng, "Optimal power grid protection through a defender–attacker–defender model," *Reliability Engineering & System Safety*, vol. 121, pp. 83–89, 2014.

[105] B. A. Carreras, V. E. Lynch, I. Dobson, *et al.*, "Critical points and transitions in an electric power transmission model for cascading failure blackouts," *Chaos: An interdisciplinary journal of nonlinear science*, vol. 12, no. 4, pp. 985–994, 2002.

[106] C. Nan, I. Eusgeld, and W. Kröger, "Analyzing vulnerabilities between SCADA system and SUC due to interdependencies," *Reliability Engineering & System Safety*, vol. 113, pp. 76–93, 2013.

[107] V. M. Bier, E. R. Gratz, N. J. Haphuriwat, *et al.*, "Methodology for identifying near-optimal interdiction strategies for a power transmission system," *Reliability Engineering & System Safety*, vol. 92, no. 9, pp. 1155–1161, 2007, Critical Infrastructures.

[108] J.-W. Wang and L.-L. Rong, "Robustness of the western United States power grid under edge attack strategies due to cascading failures," *Safety Science*, vol. 49, no. 6, pp. 807–812, 2011.

[109] K. Wang, B.-h. Zhang, Z. Zhang, *et al.*, "An electrical betweenness approach for vulnerability assessment of power grids considering the capacity of generators and load," *Physica A: Statistical Mechanics and its Applications*, vol. 390, no. 23–24, pp. 4692–4701, 2011.

[110] W. Y. Ng, "Generalized generation distribution factors for power system security evaluations," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-100, no. 3, pp. 1001–1005, Mar. 1981.

[111] U. Brandes, "A faster algorithm for betweenness centrality," *Journal of mathematical sociology*, vol. 25, no. 2, pp. 163–177, 2001.

[112] O. Sporns, "Graph theory methods for the analysis of neural connectivity patterns," in *Neuroscience databases*, Springer, 2003, pp. 171–185.

[113] J. Lofberg. (2016). Big-m and convex hulls, [Online]. Available: https://yalmip.github.io/tutorial/bigmandconvexhulls/ (visited on 11/17/2016).

[114] C. Coffrin, D. Gordon, and P. Scott, "NESTA, the NICTA energy system test case archive," *ArXiv preprint arXiv:1411.0359*, 2014.

[115] J. Bialek, E. Ciapessoni, D. Cirio, *et al.*, "Benchmarking and validation of cascading failure analysis tools," *IEEE Transactions on Power Systems*, vol. PP, no. 99, pp. 1–14, 2016.

[116] C. Grigg, P. Wong, P. Albrecht, *et al.*, "The IEEE Reliability Test System-1996. a report prepared by the Reliability Test System Task Force of the Application of Probability Methods Subcommittee," *IEEE Transactions on Power Systems*, vol. 14, no. 3, pp. 1010–1020, Aug. 1999.

[117] H. Wan, J. D. McCalley, and V. Vittal, "Increasing thermal rating by risk analysis," *IEEE Transactions on Power Systems*, vol. 14, no. 3, pp. 815–828, Aug. 1999.

[118] S. D. Foss, S. H. Lin, and R. A. Fernandes, "Dynamic thermal line ratings part i dynamic ampacity rating algorithm," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-102, no. 6, pp. 1858–1864, Jun. 1983.

[119] P. Cuffe and A. Keane, "Visualizing the electrical structure of power systems," *IEEE Systems Journal*, vol. PP, no. 99, pp. 1–12, 2015.

[120] J. Lofberg, "YALMIP : A toolbox for modeling and optimization in MATLAB," in *Computer Aided Control Systems Design, 2004 IEEE International Symposium on*, Sep. 2004, pp. 284–289.

[121] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on power systems*, vol. 26, no. 1, pp. 12–19, 2011.

[122] MATLAB, *Version 9.0.0.341360 (R2016a)*. Natick, Massachusetts: The MathWorks Inc., 2016.

[123] I. Gurobi Optimization, *Gurobi optimizer reference manual*, 2015.

[124] MATLAB, *Global Optimization Toolbox User's Guide (R2016a)*. Natick, Massachusetts: The MathWorks Inc., 2016.

[125] P. Cuffe, "Raw data from "a comparison of malicious interdiction strategies against electrical networks"," May 2017. DOI: 10 . 6084 / m9 . figshare . 4970804 . v1. [Online]. Available: https : / / figshare . com / articles / Raw_data_from_A_Comparison_of_Malicious_Interdiction_Strategies_Against_Electrical_Networks_/4970804.

[126] I. Dobson and D. E. Newman, "Cascading blackout overall structure and some implications for sampling and mitigation," *International Journal of Electrical Power & Energy Systems*, vol. 86, pp. 29–32, 2017.