Efficient Contingency Analysis in Power Systems via Network Trigger Nodes

Anika Tabassum*§ Supriya Chinthavali* Sangkeun Lee* Nils Stenvig* Bill Kay*
Teja Kuruganti* B. Aditya Prakash†

*Oak Ridge National Laboratory
†College of Computing, Georgia Institute of Technology
Email: {tabassuma, chinthavalis, lees4, stenvignm, kaybw, kurugantipv}@ornl.gov, badityap@cc.gatech.edu

***Abstract*— Modeling failure dynamics within a power system is a complex and challenging process due to multiple inter-dependencies and convoluted inter-domain relationships. Subject matter experts (SMEs) are interested in understanding these failure dynamics for reducing the impact from future disasters (i.e., losses or failures of power system components, such as transmission lines). Contingency analysis (CA) tools enable such 'what-if' scenario analyses to evaluate the impacts on the power system. Analyzing all possible contingencies among N system components can be computationally expensive. An important step for performing CA is identifying a set of k 'trigger' components, which when failed initially can significantly impact the overall system by causing multiple failures. Currently SMEs focus on identifying these trigger components by running expensive simulations on all possible subsets, which quickly becomes infeasible. Hence finding a relevant set of trigger components (contingencies) rapidly to enable efficient and useful CA is crucial.**

In a collaboration between computer scientists and power system experts, we propose an efficient method for performing CA by exploiting network inter-dependencies in power system components. First, we construct a network with multiple electric grid infrastructure components and dependencies as connections among them. We reformulate the problem of finding a set of trigger components as a problem of identifying critical nodes in the network, which can cascade power failures through connected nodes and cause significant damage to the network. To guide the practical CA tools, we develop a network-based model with a probabilistic edge-weights setup using intricate domain rules. Then we conduct an empirical study on real power system data in the US for both regional and national levels. Firstly, we use power system datasets for the US to create a national-scale domain-driven model. Secondly, we demonstrate that network-based model outperforms the outputs from a real CA tool and show on average $25\times$ improved selection of contingencies, thereby showcasing practical benefits to the power experts.

I. Introduction

Power systems within the US are highly interconnected and hence vulnerable to multiple failures triggered by extreme events (such as a hurricane or a man-made disaster). Modeling these failure dynamics for domain experts is very challenging, due to the complex relationships and the possibility of multiple contingencies. Contingencies (or unplanned outages) refer to a loss or failure of part of the power system, such as a transmission line, a generator substation etc. Usually domain experts approach contingency analysis (CA) for measuring grid reliability via the so-called 'N-k' analysis. This entails trying out *all possible* combinations of k failures and then subsequently evaluating the resulting impact using multiple metrics (load loss, line loss etc). Clearly, this standard analysis is very expensive, due to the combinatorial nature of the possibilities as well as due to the expensive power simulations which need to be run to evaluate an impact. For instance, even for a very modest size of a power system with $N \approx 1000$ components and $k \leq 4$ leads to over billions of contingency scenarios [1]. Hence, even power experts have proposed several approaches to form an efficient list of contingencies using power-flow simulation tools [1] and scale them using high performance computing approaches [2], the issue is still challenging.

Hence, we aim to develop a complementary pre-analysis tool for the CA by considering the power system from a heterogeneous network perspective. In this network, the system components can be considered as nodes, the interconnections among the components as edges and failure dynamics as cascading failures on the network. Secondly, instead of trying out all possible failures of k components in the network (similar to the $N-k$ analysis), we propose to look for the k 'trigger' or crucial components whose failures can cause the highest impact (largest number of failures) on the network. Once found, these k trigger components allow domain experts to focus on the most critical components, and can then be used as an initial list of contingencies for further analysis with expensive simulation tools [3].

In this paper, we develop a network-based method of finding trigger components to help power system contingency analysis (CA), collaborating between computer scientists and power experts. In contrast to most network approaches which are only structure-based [4], we propose a new domain-inspired method that extracts the trigger nodes by capturing the various

§Most work is done as part of PhD research at Virginia Tech

failure dynamics of a power system efficiently. Our main contributions are:

1) We propose a **D**omain **I**nspired Method in **He**terogeneous **N**etwork (DIHeN) for efficient CA through a heterogeneous network-based model considering dynamics over graphs instead of purely structural analysis.
2) We develop a network failure model with a probabilistic edge-weight setup inspired from complex domain-based mechanisms.
3) We conduct a detailed empirical analysis over nation-scale rich real electric grid infrastructure datasets. We find that our approach can beat the state-of-the-art and also has practical benefits to power experts. Further leveraging an existing power simulation analysis, we also show that our model can find trigger nodes and is beneficial for power-flow simulation tools.

II. DIHeN Methodology

To analyze and prevent unplanned outages, the standard approach of $N-k$ analysis identifies trigger components that cause a maximum impact on the system through multiple failures quantified by metrics, such as line loss, load loss, etc. This procedure of identifying such trigger components becomes exponentially expensive with the high value of k due to the combinatorial nature. Hence, we aim to find a set of trigger components for the SMEs without the help of a simulation tool. We can define our problem for finding trigger components in a power system as:

Problem II.1 (**Trigger Components in CA**). *Given a power system of N components and a value k. Find a set S of k contingencies or trigger components that can cause a maximum impact on the system through failures.*

To address this problem, considering the power system as a heterogeneous network can be advantageous to capture the interconnections among the components, model various dynamics induced by the failures, and quantify the failure impact on the component. Hence, we propose a complementary network-based method DIHeN instead of purely using CA simulation tools, which are accurate but computationally expensive. For DIHeN, we first construct a heterogeneous network modeling the power system inter-dependency, develop a network-based failure cascade model capturing different failure dynamics inspired from the power domain, and finally find trigger components in the heterogeneous network using the failure model.

A. Network Construction

Constructing heterogeneous network from a power system is a crucial task, as every type of system component is available in geospatial format (shapefile). Each component is represented as a geographic object, e.g., point, polygon, line, etc. Since no inter-dependencies or relationships among the components (geographic objects) are addressed explicitly in the data, the researchers need to understand the geographic object and hence define relationships among them. Electric grid infrastructure consists of four types of components (Electric power plants, Transmission Substations, Transmission lines, and Distribution substations) as they have the ability to generate/distribute power [5] and hence are very important for CA. We specifically select these four types of power system components and collect from the publicly available critical infrastructure (CI) data, HIFLD[1] for the US [6]. We consider each component as a node in the network. To capture the inter-dependency (connection) across different types of components, we use the nearest-neighbor based on geographical distance between the components using a distance threshold (25 kilometers) to limit creating dependencies between distant components. To build the network from the geospatial format we use an existing DOE tool by Lee et al. [7]. Table I shows the four components (node) types in the network and their functionalities. For the rest of the paper, we use the terms component and node as interchangeable.

The connections among the different components are described in the following, and a pictorial representation of the structure of the network is shown in Fig. 1. We call a node as parent if it supplies power to its connected node, and child if it consumes power from its connected node. The solid line represents corresponding one-one connection among the nodes and a dashed line represents possible one to many connections from parent to its neighboring children.

Component type	Functionality
Electric Power-plant (EP)	Generates power which transmits to transmission substations for power distribution.
Transmission Substations (TS)	Connects two or more transmission lines.
Distribution Substations (DS)	Transform voltage and distributes power to consumers.
Transmission Lines (TL)	Transmits power from TS to TS or TS to DS.

TABLE I: **Description of components of power systems**

Electric Power-plants (EP): An EP generates and distributes generated power to multiple Transmission Substations (TS). We model an EP node to have one or multiple children (TS nodes).

Transmission Substations (TS): TS receives power from one or multiple EPs, and the received power is transmitted to another TS or a distribution substation (DS). Thus, we model a TS to have one or multiple EP nodes as parents and one or multiple TL nodes as children.

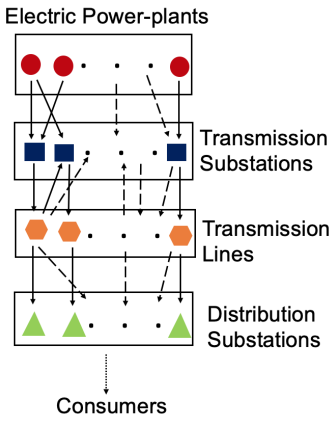


Fig. 1: **Structure of a power system network.**

[1]Homeland Infrastructure Foundation Level Data

Transmission Lines (TL): TL connects TS and TS or TS and DS. Thus, A TL node may have TS nodes as its parents and have DS or TS nodes as children.

Distribution Substations (DS): DS is the terminal component, where it receives power from a TL and distributes received power to multiple consumers within its service area. Note that, we did not include consumer components in our model. Each DS node has one or multiple parent TL nodes.

B. Failure Cascade Model

Modeling failure dynamics through trigger components is difficult due to its complex mechanisms, and no single model can capture all the dynamics [8]. E.g., failure in one component may induce stress to its neighbors due to multiple conditions, such as miscoordination of relays, line tripping, overloading, etc. All these might result in cascading failures to other components [9].

To model such failure, we leverage a network-based independent cascade model that serves as complementary products to the traditional power flow simulation tools to evaluate the impacts of extreme events on power systems.

Independent Cascade (IC) Model: Given a directed weighted network G, consisting of set of N nodes and E edges. F represents set of edge-weights for corresponding edges in E. IC model is a popular information diffusion model [10] where once a node fails, in the next time step it gets one chance to fail its connected child with the probability equal to the connecting edge-weight. The cascade starts with a given set of seed nodes that 'initially' fails and ends when there is no new failed node.

The main challenge in the IC model is to model the edge-weights in the network for the cascade. Each edge-weight represents an impact weight which denotes the probability that a node may fail if its parent node fails. Our goal is to model such probabilities in a realistic way, inspired from real power systems.

C. Impact Weights

Impact Weights F is a set of edge-weights for the edges, where each f_{ij} for the edge e_{ij} denotes the probability of failure of a node n_j if its parent node n_i (node that supplies power to n_j) fails. In the power system, the failure of a parent cannot guarantee failure of its child due to the following properties: **P1.** A node will not fail if it can have a consistent power supply through its other parents due to power redistribution [9]. **P2.** The components in the power system is associated with a protection system (e.g., circuit breakers) which tries to isolate the failed component from the entire network to prevent further damage due to a cascade. These protection systems may break due to an increase of stress induced by some conditions and only then retain the ability to cascade [11], [12]. Considering these properties, we propose two probability models for F.

1) Failure Propagation Probability.: To satisfy **P1**, we make the following assumption: when a node of type t fails, its children (nodes that consume power from it) can gain power from other similar type parents. E.g., if a TS node fails, and its child transmission line (TL) component has another parent which is TS, it still may get power through redistribution and hence this decreases the chance of failure of the TL. Thus, for failure propagation probability we simply assume, a node has less chance to fail if it has high number of parents. In other words, a node with higher number of parents are less vulnerable (see example Fig. 2(a) for computing edge-weights using k_{ij}). Using this assumption, for each node we first identify the type and the number of parents. For each edge e_{ij}, the probability that a node n_i can propagate its failure to node n_j is:

$$k_{ij} = \frac{1}{\sum_{z \in par(v_j)} I(t_i, t_z)} \tag{1}$$

where, $par(v_j)$ are the parents of v_j, t_z is the type of node z and $I(.,.)$ denotes if two nodes are of same type, i.e.,

$$I(t_i, t_j) = \begin{cases} 1 & \text{both nodes are same type, i.e., } t_i == t_j \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

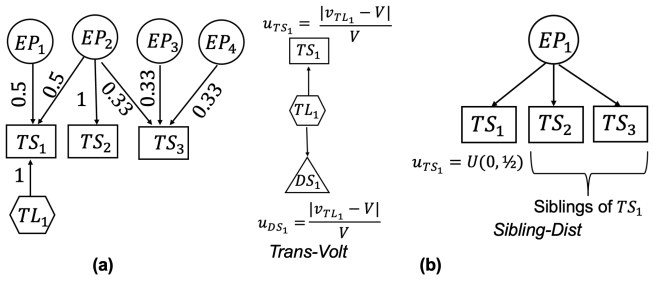


Fig. 2: **Example of (a) Failure Propagation Probability (k_{ij}) (b) Cascade-blocking probability (u_j).**

2) Cascade-blocking Probability.: For satisfying **P2**, we model each node to have a probability to prevent cascading failure to its child. In other words, the node cannot cause any further damage and cascade stops. To capture such blocking probability, we come up with two approaches, one where domain knowledge is involved and provided by the SMEs, the other is based on a realistic assumption but inspired from the scenarios of power simulations. The latter is applicable to the cases where we cannot apply the SME rule.

Trans-Volt: Recommended by the SMEs, for modeling u_{ij} we use the following domain knowledge : Transmission Lines $> 330KV$ are typically deemed critical since they supply more power[2]. Failure of these nodes can highly impact its connected nodes[3]. Based on this knowledge, we come up with the following assumption: The high voltage TL nodes if failed induce more stress on its child to cascade which cause less chance of preventing (blocking) the cascade [13]. Following this assumption, we first collect the associated voltage of

[2]https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf

[3]https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-014-1.pdf

every TL node. We set a threshold value V as maximum voltage of all the TL nodes in a network. For edge e_{ij}, with the connecting nodes n_i and n_j, if n_i is a TL node then $u_{ij} = \frac{|v_i - V|}{V}$, where v_i is the associated voltage of node n_i and V is the threshold voltage value in the network. High voltage TL (v_i) leads to lower $|v_i - V|$, hence decrease the chance of blocking a cascade (u_{ij}).

Sibling-Dist: For the edges where above domain knowledge is not applicable, i.e., no TL nodes in the connecting edge, we make the following assumption: the cascade blocking probability of a node n_j is higher if the node has fewer number of siblings (nodes other than n_j which consumes power from the same parent as n_i) [11]. If n_i fails, it impacts on all its children. This induces stress on the protection system on all the siblings of n_j. As a result, few siblings cause less stress on the protection system to deal with, hence more chance to block the cascade. On the other hand, more siblings cause more stress on the protection system to deal with, hence less chance to block the cascade. Based on this assumption, we design u_{ij} of node n_j in edge e_{ij} as the following,

$$u_{ij} = \mathcal{U}(0, b) \tag{3}$$

$$b = \frac{1}{\sum_{z \in Ch(par(n_j))\ n_j} I(t_z, t_j)} \tag{4}$$

where t_j is the type of node n_j, $\mathcal{U}(.)$ is the randomly sample from uniform distribution, $par(n_j)$ gives all the parents of n_j, and $Ch(par(.))$ represents the union of all the child node of all the parents in $par(.)$, i.e., the siblings of the node in $(.)$. Since, there is no specific domain knowledge involved about impact of protection system for a particular number of siblings, we randomly select u_{ij} from a uniform distribution based on the number of siblings the node has. The fewer sibling yields higher values of b, hence the higher expectation of u_{ij} (see example in Fig. 2) (b).

3) Finalizing F.: k_{ij} and u_{ij} are based on two independent properties **P1** and **P2** and f_{ij} is based on the probability of both the events occur simultaneously. Suppose, n_i and n_j are the connecting nodes of e_{ij}. If n_i fails, then probability that it will fail n_j is $f_{ij} = k_{ij}(1 - u_{ij})$, where $1 - u_{ij}$ is the probability that n_j can cascade.

D. Problem Formulation

We formulate Problem II.1 as identifying a set of critical nodes which can cause maximum downstream damage to the network due to cascading failures.

Problem II.2 (Critical Nodes in Network). ***Given****, a heterogeneous power system network G of N components, a set of edge-weights F on G, the IC model M which uses F, and a budget k.*

Find *the best set S^* of k nodes that can cause maximum downstream damage on G using M, i.e.,*

$$\arg\max_{S}\ E[S] = \sum_{n_i \in N - S} P(n_i|S). \tag{5}$$

$P(n_i|S)$ is the probability that a node n_i can fail in the IC, given the initially failed nodes S. N represents all the nodes in G. $E[S]$ represents the expected number of nodes that may fail given S.

E. Finding Critical Nodes S

To find the set of critical nodes as mentioned in the Problem II-D is a well-known Influence Maximization (IM) problem using IC, where $E[S]$ is submodular [10]. To iteratively select k nodes from the network and to solve IM faster on a large network we use the Degree-Discount-IC heuristic [14] over greedy [10], [15]. Our framework for DIHeN is shown in Algorithm 1.

Input: D: Geographic shapefiles of the components of power system,
k: a budget
Result: S: a set of k critical components in D .
1. $S = \{\}$
2. Construct heterogeneous network G from D as mentioned in Sec. II-A
3. Compute Impact weight F in G
foreach $e_{ijk} \in E$ **do**
  Calculate Failure Propagation probability k_{ij} mentioned in Sec. II-C1
  Calculate Cascading-blocking probability u_{ij} mentioned in Sec. II-C2
  Compute $f_{ij} = k_{ij}(1 - u_{ij})$
end
4. Construct the IC model M using F.
5. Select k nodes of S using M solving Problem II.2.
6. **return** S

Algorithm 1: DIHeN Framework.

III. Empirical Study

In this section, we design various experiments to evaluate our results showing DIHeN is able to find critical nodes and has practical benefits to CA tools. All experiments herein were conducted on a 4 Xeon E7-4850 CPU with 512 GB of 1066Mhz main memory. We implement DIHeN using Python. Our analytic code and an anonymized version of data have been released for research purposes [16].

Datasets. We construct both national and regional level heterogeneous networks based on the US power system. We consider different sectors of energy infrastructures, such as Bulk Electricity System (BES). We collect different categories of power system components pertaining to BES. Every component in a category also contains multiple power attributes (such as voltage, load, generated power, etc.). Following, we describe each network in detail.

- *National-level Distance-centric*: We construct the network using the US national level geospatial critical infrastructure (CI) HIFLD [6]. For the edges, we define the inter-dependencies among the components based on the geographical distance between two components with a distance threshold of 25km as described in Sec. II-A.

- *National-level Domain-centric*: For the network, the components and inter-dependencies (edges) are entirely supplied by the SMEs in contrast to using the geographical distance.
- *Regional-level*: The national power system in the US is comprised of three major interconnections of electric grid infrastructures which operate independently from each other, Eastern Interconnection (*EI*), Western Interconnection (*WI*), and Electric Reliability Council of Texas (*ERCOT*) [17]. We construct networks using HIFLD data [6] based on two major interconnections- *EI* (encompasses the eastern region) and *ERCOT* (entire Texas state covers most part of *ERCOT*).

We aim to show that DIHeN is adaptable for both national and regional networks consisting of different interconnection types. The overview of the networks are shown in Table II.

Research Questions. Our goal is to demonstrate that S found through DIHeN provides a good solution to Problem II.2. Specifically we want to address:

Q1. Does S fail large number of nodes to satisfy the goal of maximum downstream damage?

Q2. Does S contains critical nodes useful for contingency analysis?

Q3. How do different modules of F in DIHeN affect the performance on S?

Q4. Does DIHeN enable the nodes to use as trigger components in real power simulations?

Q1, **Q2** are aligned with the goal of the output mentioned in Problem II.1 and Problem II.2. We plan to showcase the performance of DIHeN on multiple power system datasets and compare with different non-trivial models. For **Q3**, we analyze the performance of different variants of F in DIHeN as described in Sec. II-C. With **Q4**, we are interested to retrospect whether DIHeN provides S, that experts can use for the power simulations.

Measures of Success. For evaluating S, we choose the following metrics:

M1. *failure spread*: Motivated from the use of IC (Sec. II-B) for selecting S, we plan to measure in terms of the expected number of nodes failed in the network by S, i.e., *failure spread*$= E[\#n|S]$.

M2. *coverage gain*: To measure that nodes in S are critical, we use the criticality criteria of power components identified by the SMEs [18]. We select these criteria based on availability of the attributes of the HIFLD data. Table III shows the expert identified criteria, description, and networks that used the the corresponding criteria. For each criteria R_x and for each node $n_i \in N$, let $Z(n_i, R_x)$ be 1 if n_i satisfies R_x and 0 otherwise. We define the *coverage gain* for criteria R_x as the ratio of coverage of S for R_x to the expected number of randomly selected k nodes that satisfy R_x:

$$M_{Gain} = \frac{\sum_{s_i \in S} Z(s_i, R_x)/k}{\sum_{n_i \in N} Z(n_i, R_x)/N} \tag{6}$$

Baselines. For baselines, we consider popular network-based model to demonstrate utility of DIHeN. We check the performance of DIHeN against the popular network analysis techniques (1-3) and models with uniform edge-weights (4).

1) *PageRank (PR)*: Compute PageRank scores of nodes using edge-weights as our F. Pick k nodes with highest PageRank scores.
2) *Degree-Centrality (DC)*: Pick k nodes with highest degree.
3) *Critical Score ($CSxy$)*: Model developed to quantify criticality of nodes in US national level critical infrastructure network by computing a weighted average of the PageRank scores and the PageRank scores in the reverse graph (reverse PageRank) of each node [19]. We pick k nodes with the highest $CSxy$ (x, y denotes the weight used for each score).
4) *IC with edge-weight $x \in [0, 1]$ (IC_x)*: Use same edge-weight x for all the edges and select k nodes running the DIHeN framework.

A. Effectiveness (Q1-Q2)

We show that DIHeN is effective in finding S for which (i) the expected number of nodes that will fail given failure of S is large (in terms of **M1**) and (ii) contains critical nodes and can be used for CA (in terms of **M2**).

(i) Evaluation using M1. For **Q1**, the S selected by DIHeN and the baselines, we run our IC model M. Fig. 3 shows *failure spread* (vertical axis) with the increase of k (horizontal axis) on the *Distance-centric* network (we do not show the results for other networks, as the scenario is the same for all other networks). Our model outperforms all the baselines and the difference of failure spread grows as k increases.

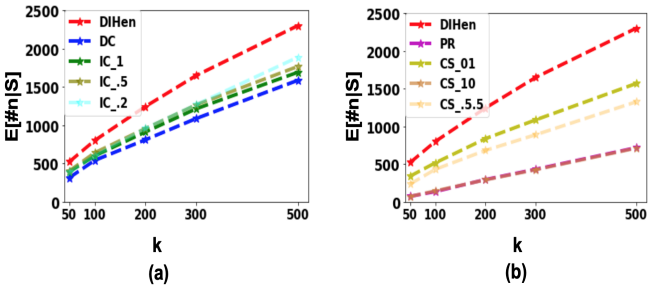


Fig. 3: **Evaluating S in terms of M1 : *failure spread* vs k. High *failure spread* is the better. DIHeN outperforms all the baselines shown in (a) and (b).**

(ii) Evaluation using M2. For **Q2**, similar to the above experiments, we aim to show performance of DIHeN against the baselines as well as varying k on different G. Fig. 4 shows the performance of DIHeN comparing with the baselines using **M2** on all the datasets. The horizontal axis represents the datasets mentioned in Table II and vertical axis represents M_{Gain} for each model. Each bar represents a model. For the space constraints, we only show the performance of IC_x for the best values of M_{Gain}, i.e., $x = 1, 0.5, 0.2$.

Network type	Name of Network	Total Nodes	Total Edges	Components Type	Components Size	Description
National	*Distance-centric*	118956	82750	1. EP 2. TS 3. TL 4. DS	10564 1806 41600 64986	Entire power system of the US.
National	*Domain-centric*	93579	135951	1. EP 2. TS 3. TL 4. DS	10732 3553 51425 27869	Power system of US based on the interconnections taken from SMEs.
Regional	*EI*	77124	51851	1. EP 2. TS 3. TL 4. DS	4138 6705 25610 40671	A major interconnection encompassing most of the area east of US.
Regional	*ERCOT*	9719	6294	1. EP 2. TS 3. TL 4. DS	375 646 3456 5242	Entire TX covers most of *ERCOT*, a very different infrastructure compared to *EI* and *WI* [17].

TABLE II: **Overview of the networks utilized for the study.**

Criteria Name	Criteria	Description	Networks Used
R_1	$V \geq 345KV$	Transmission lines $\geq$ 345KV are deemed critical since they serve $> 1000MVA$ load[2]	*Distance-centric*, *Domain-centric*, *EI*, *ERCOT*
R_2	Near user-defined critical nodes	A power system component that is one hop away from a user-defined arbitrary critical component	*Distance-centric*, *Domain-centric*, *EI*, *ERCOT*
R_3	$V \geq 345KV$ and near user-defined critical node	Components of $\geq$ 345KV which are near a user-defined arbitrary critical component and located within one or two hop away	*Distance-centric*, *Domain-centric*, *EI*, *ERCOT*
R_4	$L \geq 300MW$ &	Components that supply load $\geq$ 300MW are critical	*Domain-centric*
R_5	Near-NG	A power system component that is one hop away from a Natural gas station	*Domain-centric*

TABLE III: **Criticality criteria for M2.**

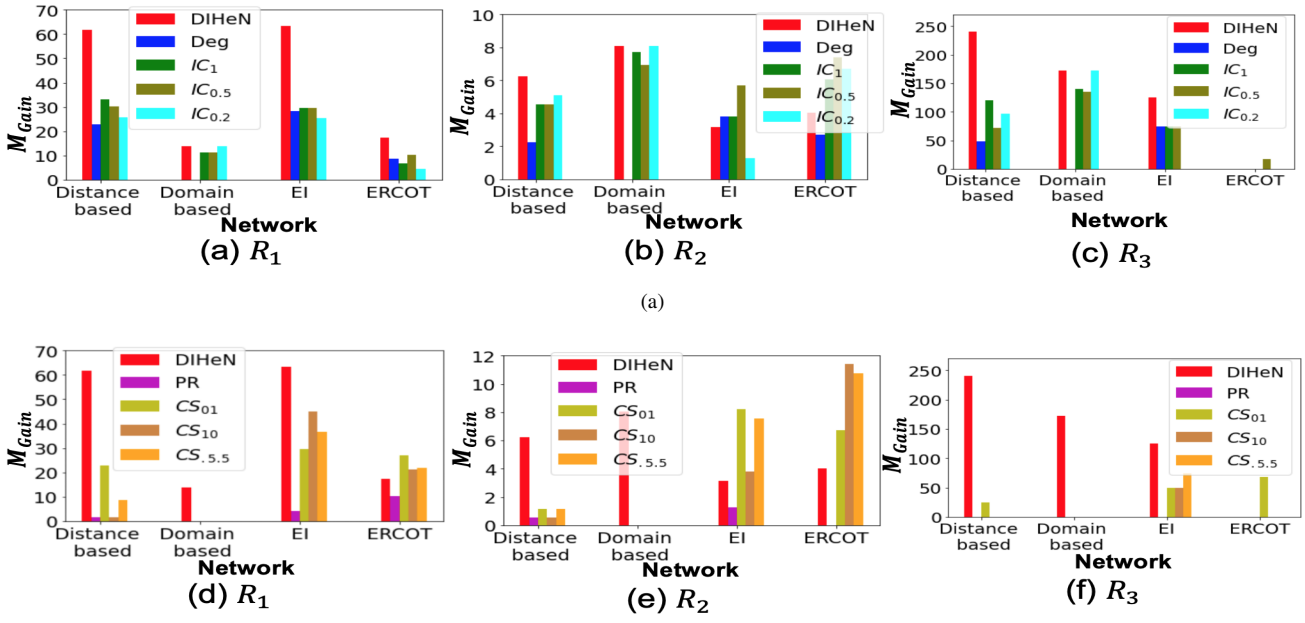


Fig. 4: **Performance of DIHeN comparing with baselines in terms of the criticality criteria R_1-R_3 on different datasets. Fig.(a)-(c) shows the comparison for the baseline models with uniform edge-weights. Fig.(d)-(f) shows comparison against the popular network analysis approaches. Here, we consider $k = 500$ for *Domain-centric* network, and for all other datasets we consider $k = 50$. High M_{Gain} is the better.**

Our model consistently outperforms all the baselines on the national networks for $R_1 - R_3$. Among all the networks, DIHeN best performs $3.5\times$ in R_1, $2.75\times$ in R_2, and $5x$ in R_3[4]. For R_3, DIHeN is very high and around $240\times$ *coverage gain* (in the *Distance-centric* network) which no other baselines can perform. For $R_4 - R_5$, DIHeN also outperforms the other baselines on *Domain-centric* network (see Fig. 5). The *Distance-centric* national network and the regional networks *EI* and *ERCOT* do not contain the necessary attributes to evaluate R_4, R_5. Fig. 4 (a)-(c) also indicates that for the baseline IC_1, when failure of initial nodes cause every connected nodes in the cascade to fail, (i.e., a large spread of failure) this can not guarantee critical nodes useful for CA.

For *EI*, we outperform all the baselines in R_1, R_3. For R_2, our M_{Gain} are comparable in 5 out of 8 baselines. On average ratio of our M_{Gain} with respect to other baselines is $1.95\times$ in R_1, $1.18\times$ in R_2, and $1.67\times$ in R_3.

For *ERCOT*, DIHeN consistently outperforms the baselines in R_1 (5 out of 8 baselines). M_{Gain} for all the baseline models and DIHeN is 0 in R_3 due to the presence of very sparse data (only 11 nodes in the network satisfy R_3). In R_2 DIHeN provides consistent M_{Gain} on all the network based models (performs best in 2 out 8 baselines). Overall, mean ratio of our model gain to the baseline is $3.45\times$ in R_1 and $.83\times$ in R_2.

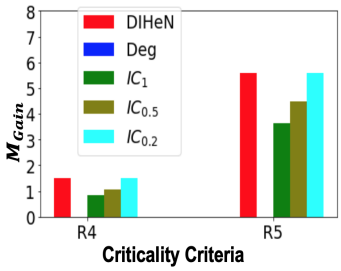


Fig. 5: ***Domain-centric* network for $R_4 - R_5$.**

Fig. 6(a)- 6(c) shows the performance of our model on different G varying k, for R_1-R_3 (Table III). Each bar represents a power system network. The horizontal axis represents size of k and vertical axis represents M_{Gain} for each R_x. The higher M_{Gain}, the better the performance of DIHeN.

DIHeN consistently provides good set of critical nodes for both national and regional networks and average M_{Gain} across all the networks is $39.3\times$ better than cherry picking the nodes for R_1, $4.87\times$ for R_2, and $108\times$ for R_3. For R_1, the results show decrease of M_{Gain} with the increase of k, although the number of nodes in S satisfy R_1 increases with k. This indicates that we can get a good set of S satisfying R_1, even for small value of k. For R_3, M_{Gain} for DIHeN is low in *ERCOT* (0 for $k < 200$), since number of nodes satisfy R_3 in *ERCOT* is very scarce (only 11 nodes out of 9500 satisfy R_3).

B. Ablation Studies (Q3)

To evaluate the impact of different variants of F, we describe the models based on each of these variants (Sec. II-C). Note that, we only set the edge-weights using each of the following model and select the top k nodes using our framework.

1. *Failure-propagating (FP)*: Set the edge-weights, $f_{ij} = k_{ij}$ using Failure Propagation probability to check satisfying **P1** is not enough.
2. *Cascade-blocking (CB)*: Set edge-weights, $f_{ij} = (1-u_{ij})$ using Cascade-blocking probability (Sec. II-C) to check satisfying **P2** is not enough.
3. *No expert rule (NER)*: Assign the edge-weights $f_{ij} = k_{ij} * (1-u_j)$ using Eq. 3 for all the edges to check effect of using only model Sibling-Dist (sec. II-C2).
4. *Random Gaussian (RG)*: Select edge-weights randomly from the Gaussian distribution $N(\mu, \sigma)$, where μ is the mean of DIHeN F and σ is the variance obtained from DIHeN F. We intend to compare our domain inspired meaningful method of edge selection (F) over random selection of edge-weights.

Using **M2**, in Fig. 7, we compare performance of DIHeN against the models consists of different variants of F on all the national and regional datasets.

Our model outperforms all other models in the national network and shows competitive performance on the regional network for criticality criteria R_1-R_3. For checking the consistency of our performance, we run the DIHeN framework for each model 1000 times. From Fig. 7(a)-(c), the low deviation f M_{Gain} (black vertical lines on each model) shows M_{Gain} of all the models are consistent. In the regional networks *EI* and *ERCOT*, DIHeN performs almost similar comparing with CB. This might be due to sparse graph unlike *Distance-centric* and *Domain-centric* national network, where most components have only one parent, hence $k_{ij} = 1$. Hence, edge-weights F of DIHeN is similar weights as model CB (u_{ij}).

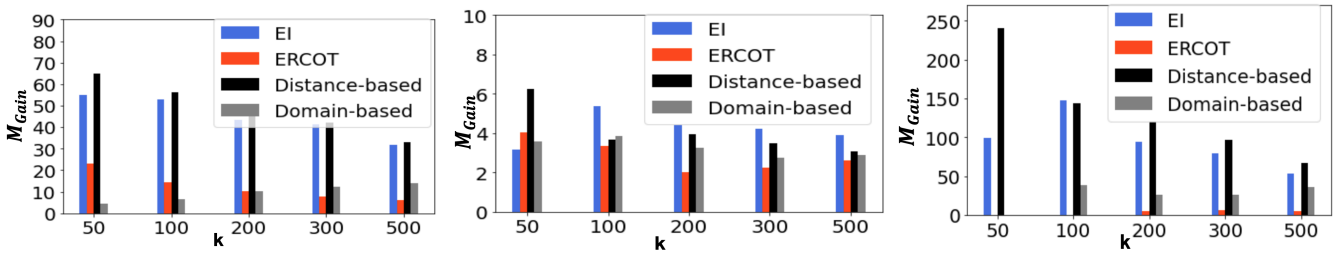
Remark: Note that, if we only consider the nodes which apply to criticality criteria $R_1 - R_5$, the total number of components is 7000 in the *Domain-centric* national network. Analyzing combination of 7000 nodes for CA is also exponential. On the other hand, if we choose nodes randomly from 7000 nodes, it can not guarantee the failure of a large number of nodes downstream. Hence, our goal behind using M_{Gain} is to provide the SMEs sufficient reason to filter the nodes that maybe important for CA.

C. Qualitative Case-study: Power-flow Analysis (Q4)

In this section, we show that the selected nodes using DIHeN can be used for real CA simulations by leveraging high fidelity simulation analysis on the power system of *ERCOT* conducted through an in-depth study by the SMEs. Due to privacy concern we cannot share the reported results.

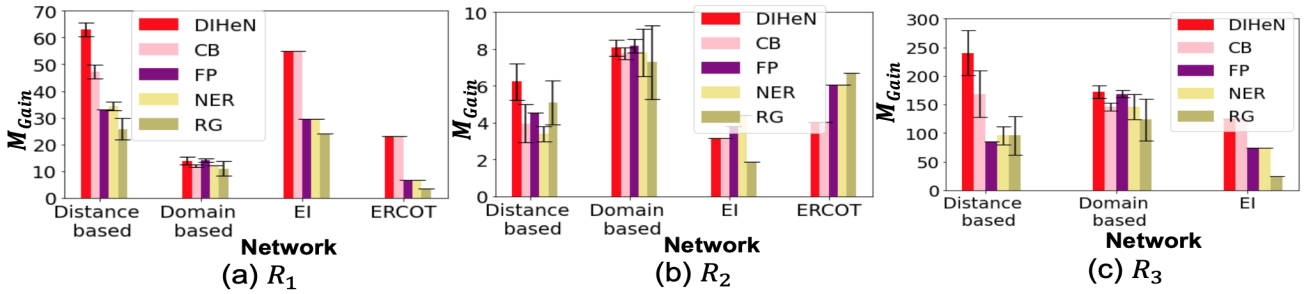
Power-flow analysis. For the analysis, the SMEs choose 81 high voltage transmission lines ($= 345KV$). They first conduct a *base case* analysis, i.e., ideal scenario when no components are removed (i.e., nothing has failed). From the analysis, several parameters are recorded, e.g., the total load due to power flow, number of voltage violation (rise of drop of voltage), the convergence of the simulation, etc.). Next, multiple simulation scenarios are created, each time removing a different subset of transmission lines. The parameters are compared with the *base case* scenario (amount of load loss,

[4]The values are found considering the maximum value of ratio of M_{Gain} of DIHeN and M_{Gain} of a baseline model, i.e., $\max \frac{M_{gain}^{\text{DIHeN}}}{M_{gain}^{\text{baseline}}}$, $M_{gain}^{\text{baseline}} \neq 0$



(a) R_1 (b) R_2 (c) R_3

Fig. 6: **Performance of DIHeN for the criticality criteria R_1-R_3 mentioned in Table III using M2 on different networks in terms of M_{Gain} vs size of k for each R_x. High M_{Gain} is the better.**



(a) R_1 (b) R_2 (c) R_3

Fig. 7: **Ablation study on different variants of F on national and regional network for criticality criteria $R_1 - R_3$. For each model, the black vertical bars show standard deviation of M_{Gain} running DIHeN framework 1000 iterations. In *ERCOT*, for R_3, $M_{gain} = 0$** for all the models, hence not present in Fig. (c)

number and nature of components which cause voltage violation, the simulation is convergent, etc.). Based on the above comparisons, the experts rank each transmission line. DS components that give the worst number of voltage violations are also identified. If a simulation does not converge, the SMEs consider such scenario as highly critical.

Our goal is to check the nodes in S with the expert provided components in *ERCOT*. However, due to privacy concerns we are unable to collect the exact *ERCOT* components used by the utility company. Hence, we plan to use our *ERCOT* power system data as mentioned in the Table II. Due to the difference of these two datasets, we cannot compare top k nodes in S using DIHeN with the SMEs provided rank of transmission lines. Instead, we aim to qualitatively evaluate S in terms of the available attributes of the nodes as provided by HIFLD [6]. We also record the attributes of the components reported by the SMEs in the scenario analysis. Table IV shows these attributes, its descriptions, and *coverage gain* (M_{Gain}) for each of the following attributes R.

Analyzing detected nodes. Table. IV shows performance of DIHeN using **M2** for $R_6 - R_8$. Note, all the nodes detected by DIHeN are transmission lines (TL) which the SMEs selected to use for their analysis (removing different sets of TL). For R_7, we analyze voltage of the DS connected with our selected TL which failed due to S. Among all the nodes failed due to cascade by S, 35% of them are DS nodes with high voltage $\geq 138KV$. In all the attributes $R_6 - R_8$, DIHeN gain on average is 25.3 (mean M_{Gain} based on the results shown in Table IV). For R_8, which is a potential attribute for a simulation to not converge, *coverage gain* of DIHeN is 21.2×. This indicates that selected nodes through DIHeN are suitable as trigger nodes for contingency analysis.

Name	Attributes	Rationale	M_{Gain}
R_6	TL $= 345KV$	The transmission lines ranked by DEs are of $345KV$.	17.44×
R_7	DS $\geq 138KV$	In most analysis DS $\geq 138KV$ cause worse voltage violations.	37.28×
R_8	DS $\geq 138KV$& TL $= 345KV$	Using combination of $345KV$ TLs results to fail its associated $DS \geq 138KV$ and results simulation to not converge.	21.15×

TABLE IV: **Attributes for case-study and DIHeN performance.**

D. Scalability Experiment

We record the run-times (in seconds) varying size of the network (G) and number of seeds (k). To perform the experiments on larger network than the datasets we use (Table II), we create synthetic networks using multiple layers of consumer node types using HIFLD dataset [6]. To ensure similar topology as power system, we use the connections as supplied by the SMEs at Oak Ridge National Laboratory. Table V(a) shows runtime of DIHeN in seconds varying size of G ($N + |F|$) keeping constant $k = 50$. We observe on a large network ($N + |F| > 2M$), DIHeN finish in approx. 13 mins and for $k = 500$ in 35 mins.

E. User interface

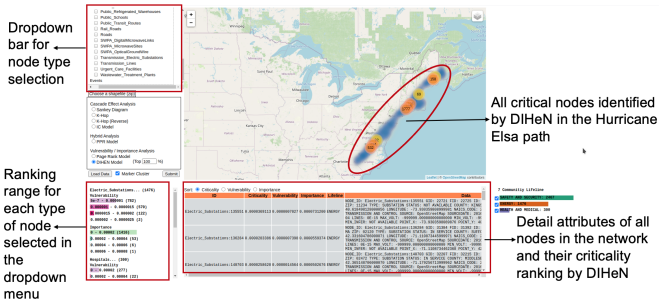


Fig. 8: **Snapshot of our UI (shows critical nodes that fall in the trajectory path of Hurricane Elsa)**

To guide the real CA simulations and improve usability we design a web-based user interface (UI) that integrates our proposed method DIHeN, all the baselines. Fig. 8 shows a snippet of the UI. We can view the network on a geography map. The blue trajectory in the map shows a hurricane shape where the number of critical nodes at different locations is shown in a circle. The top left corner in Fig. provides users to select different components they want to consider for the network construction. The bottom left corner shows the ranking range of the selected components. The table below the geography map shows the criticality rank and description of each node in the network.

IV. Related Work

Power system Models: Several literature have been proposed to facilitate vulnerability analysis in power systems through network-based models [20], [21], [22]. Hunag et al. [23] presented a visual analytic tool for decision support system through network-based operations. Flueck et al. [24] conducted a study on the state-of-the-art models to capture the interaction of relays and protection with dynamics of cascading failures. To facilitate vulnerability analysis in transmission network, Yang et al. proposed to construct cascading fault graph viewing it from network-science perspective [25]. To speed up contingency analysis approach Gorton et al. proposed a hybrid computing approach using HPC [26]. Recently, various centrality measures have been proposed to serve CA through a direct and fast pre-analysis tool by looking at the structural graph analysis [27], [28]. To the best of our knowledge all the literature are restricted to one type of component of power system instead considering a heterogeneous network on large scale national level power system. Besides, no methods have been proposed to identify critical components for CA through fine tuning the edge-weights through domain rules.

Critical Infrastructure (CI) Networks: Several literature have been proposed to quantify importance of nodes in CI network using well-known network-based centrality measures [19], [29], [30]. Tabassum et al. conducted a study on the state-of-the-art research and tools to address computational challenges in CIs using machine learning techniques [31]. Dzangier et al. developed a framework to address the recovery coupling in a multilayered CI collecting recovery time of millions of power grid failures [32]. Lee et al. first proposed how to construct a CIs network from geographic shapefiles and discussed how to compute importance of nodes using CI network reachability score [7]. Chen et al. proposed a new path-based cascade model in CI to find critical transmission lines using path-based cascade model [33]. However, their path-based model not efficient to use in large-scale power network. Recently Oliva et al. proposed an approach to measure criticality indices of CI nodes by aggregating different centrality metrics through *Logarithmic Least Squares* method [34]. However, their model finds critical nodes through structural graph analysis in contrast to our dynamic model.

TABLE V: **Scalability Experiment varying size of G.**

Nodes (N)	Edges ($\|F\|$)	Time (sec.)
179218	500746	151.57
231359	572216	192.33
234586	578255	178.63
269547	698866	1207.15
565084	1849856	804.54

TABLE VI: **Scalability Experiment varying k**

k	Run-Time (sec.)
50	164.42
100	422.33
200	821.47
300	1358.69
500	2124.19

V. Conclusion and Discussions

We proposed a complementary network-based framework DIHeN for power system CA to identify a set of contingencies ('trigger nodes') using a heterogeneous network. For the first time, we provide a capability within power system inter-dependency analysis that identifies critical nodes within an inter-dependent network not using network connectivity (similar to baseline model IC_1), instead use the knowledge provided by the subject matter experts. We first construct a heterogeneous network using large-scale real power system US data for national and regional levels. DIHeN provides a good set of nodes that cause significant failures in the network and are critical for CA. We consistently outperform the baselines in both national and regional level networks. Qualitatively, we find a set of trigger nodes ($25.38\times$ coverage gain) that has similar attributes as the experts used for their CA simulations. Our results contain 21% components (number of components among all the selected nodes by DIHeN) that have the similar attributes ($R_6 - R_8$ in Table IV) which the SMEs consider as a potential contributor to a highly critical scenario. DIHeN is based on carefully designed variants inspired from the real CA simulation tools. Our model is very fast, and all the experiments (except computing error bars) finish within 5-15 minutes. The speed and applicability of results are promising towards real-time use of DIHeN in evaluating geographically expansive threats, where large failures are expected but cannot be predicted/assessed in reasonable time frames nor with any expectation of solution convergence using traditional CA tools.

There are several interesting directions to further study and guide CA through DIHeN. First, the network construction may play an important role in DIHeN performance. E.g., while our

performance was promising in all the datasets, the gain of our model in *ERCOT* was not as high as the others. This might be due to the sparsity of the network across critical components (e.g., fewer high voltage nodes). Investigating this aspect across regional grids more in detail would be interesting. Next, although we use multiple criticality criteria for evaluating S, there are several user-defined and domain-specific criteria that can be incorporated to tailor the methodology to specific analysis needs. Using such new criticality criteria can be more beneficial for selective CA and hence is an interesting direction of study. As a part of future work, we plan to analyze DIHeN quantitatively with the ground-truth trigger components collected by real CA simulations.

Acknowledgements: This paper is based on work partially supported by NSF (Expeditions CCF-1918770, CAREER IIS-2028586, RAPID IIS-2027862, Medium IIS-1955883, Medium IIS-2106961, CCF-2115126, NRT DGE-1545362), CDC MInD program, ORNL, faculty award from Facebook, and funds/computing resources from Georgia Tech. We thank Nikhil Muralidhar for his thoughtful comments during initial time of the research.

REFERENCES

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

[2] Z. Huang, Y. Chen, and J. Nieplocha, "Massive contingency analysis with high performance computing," in *2009 IEEE power & energy society general meeting*. IEEE, 2009, pp. 1–8.

[3] "Psse – transmission planning and analysis psse power system simulation and modeling software." [Online]. Available: https://new.siemens.com/global/en/products/energy/energy-automation-and-smart-grid/pss-software/pss-e.html

[4] J. Banerjee, A. Das, and A. Sen, "A survey of interdependency models for critical infrastructure networks," *arXiv preprint arXiv:1702.05407*, 2017.

[5] S. M. Kaplan, "Electric power transmission: background and policy issues." Library of Congress, Congressional Research Service, 2009.

[6] "Homeland Infrastructure Foundation-Level Data (HIFLD)." [Online]. Available: https://hifld-geoplatform.opendata.arcgis.com/

[7] S. Lee, L. Chen, S. Duan, S. Chinthavali, M. Shankar, and B. A. Prakash, "Urban-net: A network-based infrastructure monitoring and analysis system for emergency management and public safety," in *2016 IEEE International Conference on Big Data (Big Data)*. IEEE, 2016, pp. 2600–2609.

[8] J. Song, E. Cotilla-Sanchez, G. Ghanavati, and P. D. Hines, "Dynamic modeling of cascading failure in power systems," *IEEE Transactions on Power Systems*, vol. 31, no. 3, pp. 2085–2095, 2015.

[9] H. Guo, C. Zheng, H. H.-C. Iu, and T. Fernando, "A critical review of cascading failure analysis and modeling of power system," *Renewable and Sustainable Energy Reviews*, vol. 80, pp. 9–22, 2017.

[10] D. Kempe, J. Kleinberg, and É. Tardos, "Maximizing the spread of influence through a social network," in *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*, 2003, pp. 137–146.

[11] M. Jazaeri, M. Farzinfar, and F. Razavi, "Evaluation of the impacts of relay coordination on power system reliability," *International Transactions on Electrical Energy Systems*, vol. 25, no. 12, pp. 3408–3421, 2015.

[12] D. C. Elizondo, J. de La Ree, A. G. Phadke, and S. Horowitz, "Hidden failures in protection systems and their impact on wide-area disturbances," in *2001 IEEE Power Engineering Society Winter Meeting. Conference Proceedings (Cat. No. 01CH37194)*, vol. 2. IEEE, 2001, pp. 710–714.

[13] "Addressing security and reliability concerns of large power transformers." [Online]. Available: https://www.energy.gov/oe/addressing-security-and-reliability-concerns-large-power-transformers

[14] W. Chen, Y. Wang, and S. Yang, "Efficient influence maximization in social networks," in *Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2009, pp. 199–208.

[15] J. Leskovec, A. Krause, C. Guestrin, C. Faloutsos, J. VanBriesen, and N. Glance, "Cost-effective outbreak detection in networks," in *Proceedings of the 13th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2007, pp. 420–429.

[16] "Code repository," 2021. [Online]. Available: https://github.com/AdityaLab/DIHEN

[17] "U.S. electric system is made up of interconnections and balancing authorities - Today in Energy - U.S. Energy Information Administration (EIA)." [Online]. Available: https://www.eia.gov/todayinenergy/detail.php?id=27152

[18] "Bes cyber system categorization." [Online]. Available: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf

[19] P. Devineni, B. Kay, H. Lu, A. Tabassum, S. Chintavali, and S. M. Lee, "Toward quantifying vulnerabilities in critical infrastructure systems," in *2020 IEEE International Conference on Big Data (Big Data)*. IEEE, 2020, pp. 2884–2890.

[20] M. Bao, Y. Ding, C. Shao, Y. Yang, and P. Wang, "Nodal reliability evaluation of interdependent gas and power systems considering cascading effects," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 4090–4104, 2020.

[21] I. B. Sperstad, E. H. Solvang, and S. H. Jakobsen, "A graph-based modelling framework for vulnerability analysis of critical sequences of events in power systems," *International Journal of Electrical Power & Energy Systems*, vol. 125, p. 106408, 2021.

[22] R. S. Biswas, A. Pal, T. Werho, and V. Vittal, "A graph theoretic approach to power system vulnerability identification," *IEEE Transactions on Power Systems*, vol. 36, no. 2, pp. 923–935, 2020.

[23] Z. Huang, P. C. Wong, P. Mackey, Y. Chen, J. Ma, K. P. Schneider, and F. L. Greitzer, "Managing complex network operation with predictive analytics." in *AAAI Spring Symposium: Technosocial Predictive Analytics*, 2009, pp. 59–65.

[24] A. J. Flueck, I. Dobson, Z. Huang, N. E. Wu, R. Yao, and G. Zweigle, "Dynamics and protection in cascading outages," in *2020 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2020, pp. 1–5.

[25] S. Yang, W. Chen, X. Zhang, C. Liang, H. Wang, and W. Cui, "A graph-based model for transmission network vulnerability analysis," *IEEE Systems Journal*, vol. 14, no. 1, pp. 1447–1456, 2019.

[26] I. Gorton, Z. Huang, Y. Chen, B. Kalahar, S. Jin, D. Chavarría-Miranda, D. Baxter, and J. Feo, "A high-performance hybrid computing approach to massive contingency analysis in the power grid," in *2009 Fifth IEEE International Conference on e-Science*. IEEE, 2009, pp. 277–283.

[27] E. P. R. Coelho, M. H. M. Paiva, M. E. V. Segatto, and G. Caporossi, "A new approach for contingency analysis based on centrality measures," *IEEE Systems Journal*, vol. 13, no. 2, pp. 1915–1923, 2018.

[28] M. R. Narimani, H. Huang, A. Umunnakwe, Z. Mao, A. Sahu, S. Zonouz, and K. Davis, "Generalized contingency analysis based on graph theory and line outage distribution factor," *arXiv preprint arXiv:2007.07009*, 2020.

[29] H. Yang and S. An, "Critical nodes identification in complex networks," *Symmetry*, vol. 12, no. 1, p. 123, 2020.

[30] 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.

[31] A. Tabassum, S. Chinthavali, L. Chen, and A. Prakash, "Data mining critical infrastructure systems: Models and tools," *IEEE Intelligent Informatics Bulletin*, vol. 19, no. 2, 2018.

[32] M. M. Danziger and A.-L. Barabási, "Recovery coupling in multilayer networks," *arXiv preprint arXiv:2011.04623*, 2020.

[33] L. Chen, X. Xu, S. Lee, S. Duan, A. G. Tarditi, S. Chinthavali, and B. A. Prakash, "Hotspots: Failure cascades on heterogeneous critical infrastructure networks," in *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*, 2017, pp. 1599–1607.

[34] G. Oliva, A. E. Amideo, S. Starita, R. Setola, and M. P. Scaparra, "Aggregating centrality rankings: A novel approach to detect critical infrastructure vulnerabilities," in *International Conference on Critical Information Infrastructures Security*. Springer, 2019, pp. 57–68.