Heavy-Tail Analysis of Network Theory-Based Critical Asset Identification Metrics for Bulk Transmission Power Systems

by

Erick K. Bittenbender

Bachelor of Science in Electrical Engineering, University of Pittsburgh, 2018

Submitted to the Graduate Faculty of the

Swanson School of Engineering in partial fulfillment

of the requirements for the degree of

Master of Science in Electrical and Computer Engineering

University of Pittsburgh

2020

UNIVERSITY OF PITTSBURGH

SWANSON SCHOOL OF ENGINEERING

This thesis was presented

by

Erick K. Bittenbender

It was defended on

March 27, 2020

and approved by

Dr. Gregory F. Reed, Ph.D., Professor,
Department of Electrical and Computer Engineering

Dr. Zhi-Hong Mao, Ph.D., Professor,
Department of Electrical and Computer Engineering

Dr. Robert J. Kerestes, Ph.D., Assistant Professor,
Department of Electrical and Computer Engineering

Thesis Advisor: Dr. Gregory F. Reed, Ph.D., Professor,
Department of Electrical and Computer Engineering

Heavy-Tail Analysis of Network Theory-Based Critical Asset Identification Metrics for Bulk Transmission Power Systems

Erick K. Bittenbender, MS

University of Pittsburgh, 2020

Large-scale blackouts present a significant threat to the reliable delivery of electricity expected of utilities. Often these blackouts are precipitated on a small set of failures, whether through component failures or operator error as a result of insufficient real-time system awareness. In response, a wide array of power system modeling methods has emerged to identify critical assets in electric power systems. This work seeks to study a select grouping of network theory metrics proposed in literature to identify critical power system assets. In total, two standard network theory metrics and eight "extended" complex network betweenness and degree centrality metrics across six synthetic power systems of varying size are examined. These extended complex network representations of power systems account for structural (e.g. system impedance and susceptance) and operational (e.g. power flow and line loss) properties of power systems not readily captured by standard network theory metrics. All ten metrics, evaluated for each of the six networks, are calculated and tested for heavy-tailed, and more specifically power-law tail, distributions to determine potential connections to blackout size distributions. These tests have shown scaling parameters for power-law fits less than two for extended betweenness metrics, closely matching blackout data. System operation metrics more broadly have also shown consistent power-law identification among different network sizes over the various metrics tested. Comprehensive system analysis to determine which metrics are most powerful in identifying mechanisms underlying blackout size distributions is recommended as a primary direction to extend this work.

Table of Contents

List of Tables

List of Figures

1.0 Introduction

Blackouts are a major concern around the globe, especially following the major events in 2003 that cut power to the Northeast United States and parts of neighboring Canada on August 14th, parts of Denmark and Sweden on September 23rd, and Italy on September 28th. While each of these events were surrounded by unique circumstances, some common themes can be seen. In all three, a relatively small subset of system assets failed, resulting in widespread blackouts [1]. In North America, software failures and a lack of situational awareness allowed for a generating unit and a small group of transmission lines to trip. These initial trips led to a cascade, resulting in a blackout affecting large swaths of the Northeast and Ontario [1],[2]. In Denmark and Sweden, maintenance on interconnects to continental Europe and a series of trips at three high power nuclear units resulted in an outage affecting 4 million people [1]. And in Italy, lines with heavy power import tripped due to tree contact and were unable to reclose, adversely affecting the Italian network's synchronization with the rest of Europe and causing a nationwide blackout [1],[3].

Since then, significant discussion and intervention has taken place to mitigate large-scale blackouts. In the US and Canada, a joint task force examined the event and issued a final report. Their findings led to significant systemic changes, including legislation to empower the Federal Energy Regulatory Committee (FERC), to enforce mandatory reliability standards on utilities [2]. FERC tasked the North American Electric Reliability Corporation (NERC) with developing these standards for the bulk power grid [4]. In Europe, the Union for the Coordination of Transmission of Electricity (UCTE) introduced the Operational Handbook to provide recommendations, rules, and standards to help transmission utilities coordinate across national borders [3].

While regulatory agencies recognized the impact of these events and sought to remedy the circumstances that caused them, significant blackout events still occur. As can be seen in [5], [6], and [7], these events are a persistent problem, especially with global electrification. To begin tackling this issue, utilities and transmission system operators (TSOs) need to have greater system awareness in order to identify weaknesses and act quickly to changing conditions.

To help better identify potential causes of blackouts and reduce their impact, different tools have been explored. The focus of this paper will be on critical asset identification metrics founded in network theory principles, due to their familiarity and applicability to a wide array of outage scenarios. A selection of ten network-theory based metrics will be applied to six networks to examine metric distributions across varying network complexity and size. In Section 2.0, a closer examination of blackout data and their impacts will be explored. Section 3.0 will explore network theory and extended complex networks. Section 4.0 will discuss the metrics and networks selected for this analysis in detail, along with a discussion of the process for testing heavy-tailedness. Section 5.0 will present results from distribution calculations and heavy-tail analysis, and Section 6.0 will provide an examination and discussion of these results. Section 7.0 will give suggestions for future potential expansions of this work, and lastly, Section 8.0 will provide some concluding remarks.

2.0 Large-Scale Blackouts

In many large blackout events, a select group of components failed in close temporal proximity, resulting in cascading failures and widespread outages. While some of these outages are in part attributed to broader systemic failures, having asset identification tools to identify these select groups could reduce the impact of similar large-scale blackout events. Beyond SCADA systems, which are largely reactive rather than proactive, performing some form of asset ranking can allow utilities and transmission operators to better prepare for contingencies.

Moreover, large-scale blackouts on the order of 1000 MW of load shed are not uncommon and present higher risk than smaller and more frequent blackouts [8]. As studied in [8] and [9] using NERC data from 1984 to 2006, blackout sizes generally follow a power law distribution, not an exponential distribution. As a result, large blackouts possess a non-negligible probability of occurring. Over the period studied, the authors found no indication that the frequency of large blackouts has decreased. This lends credibility to the idea that better understanding how to mitigate these events is still pertinent today. Taken all together, these studies delineate the exigent problem of large-scale blackouts and the associated ramifications on industry, business, and consumers alike.

In addition to the study of historical blackouts, some investigation into the operating conditions of power systems suggests the power law relationship between blackout probability and size could be due to operation near critical points [10]. Transmission lines and transformers may be operated close enough to overload capacity that reasonably substantial disturbances can result in overloads and cascading blackouts. A similar conclusion was found using Markov chain models

and parametric analysis of power systems. Sensitivity analysis revealed that small changes in operating characteristics were able to markedly reduce the associated cascade probability [11]. While this should be investigated further, the underlying principle remains true; Large-scale blackouts are not uncommon, offer disproportionate risk, and have not significantly decreased over time.

Beyond the technical and economic assessment, large blackouts may also present a risk to the health of those affected. As investigated in a study of the 2003 Northeast blackout, researchers found that mortality rates across age groups and causes of death increased over the first two days of the event in New York City [12]. Other studies of the 2003 blackout have found similar results, and while more observations and data are needed to solidify this relationship, the emerging trend is that blackouts negatively impact health outcomes [13],[14].

3.0 Graph Theory and Networks

Shortly after the 2003 blackouts, network theory modeling approaches were adopted as an early attempt at understanding the mechanisms underlying large-scale blackouts [15]. Network theory remains a popular choice for examining power systems and presents a familiar analog to standard electrical representations of power grids. Put simply, network theory takes graph theory principles and applies them to a system under study. Although approaches have evolved over time, all the tools discussed here utilize some form of complex network (CN) or extended complex network (ECN), with the distinction being how the model chooses to address electrical properties of power systems. Other groups have compiled surveys of CN and ECN approaches to examine electric power systems [16]-[21]. In this work, the focus will be on a select group of ECNs and how they better capture the properties of electric power systems. However, for the sake of completeness, Table 1 summarizes other popular methods. As can be seen in the table, network theory affords some versatility in the failure types that can be analyzed and provides a familiar analog to more widely accepted power system study.

Table 1 Sample of Modeling Methods for Critical Asset Identification

Method	Failure Types	Underlying Theory
Network Theory	Random failures, cascading failures, attacks, n-k contingencies	Mapping power system to graph of nodes & edges
Probabilistic Graph Methods	Random failures, cascading failures (both random and intentional)	System state transitions following failures
Game Theory	Attacks	Strategy formation based on max./min. damage to system
Multi-Attribute Methods	Random failures, attacks	Technical, economic, other factors weighted to assign importance
Deterministic Guidelines	Random failures, attacks	Regulatory guidelines for identifying critical assets

3.1 Network Theory and Topology of Electric Power Systems

When discussing power systems in the context of network theory, it is useful to clarify how power systems are represented. While methods vary, bulk transmission systems are often represented by a graph $G = (V, E)$. Typically, V is the set of vertices, or nodes, corresponding to generation, load, and transmission buses, and E is the set of edges corresponding to transmission lines connecting buses in the system. Representations of this general form can be seen in [15], [22]-[25]. A network representation of the IEEE 300-bus test case can be seen in Figure 1.

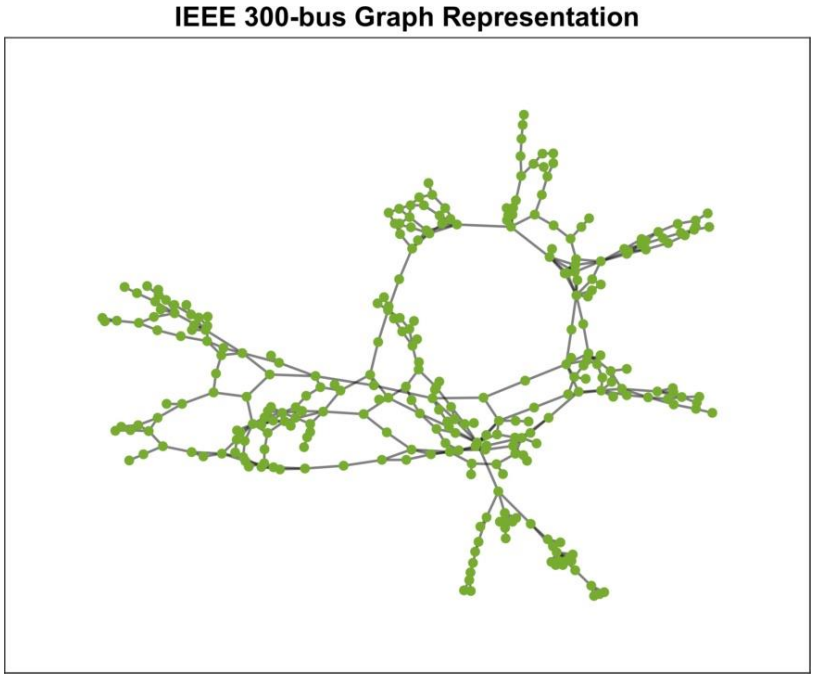


Figure 1 IEEE 300-bus Network Representation

In graph theory, different graph types often have different properties. For example, scale-free graphs are robust to random removal of nodes but are weak to targeted removal of central nodes [15]. With power systems, the network structure is not always easily classified as a single type of network due to the complexity of the system. Therefore, deeper analysis into resulting system behaviors is required (i.e. complex network analysis). However, there are still practical insights to be gained looking at what kinds of networks power systems most closely resemble. As explored in [26], understanding system topology provides insights into what types of failure the system is most vulnerable to, why outage size distributions look the way they do, and what components are most vital to stable system operation. And as explored in [27], the analysis is non-trivial, with different groups yielding different network classifications of the same power grid. While somewhat meticulous, understanding these underlying principles of system identification

can allow for more robust analysis of the system and act as a means of validating conclusions drawn about the system.

3.2 Traditional Network Theory Methods

Building off the identification of the power system's topological model, there are generally two sets of metrics to analyze component importance [28]. The first, topology-based metrics, assigns value to components based on the structure of the network, typically for undirected networks. The second set of metrics, flow-based metrics, assign value to components based on how particles, or in this case power, flows through the network. As a result, these metrics are only applied to directed networks.

Traditional network theory applications to power systems take these general metrics and apply them to the networks depicting physical connections. In [15], a connectivity loss metric is used to quantify how the removal of a generation or transmission bus affects the system's ability to supply a distribution substation in a North American power grid model. In [22], flow robustness is used to analyze lost node pair connections as more nodes and edges are removed in a Polish test case and a Western Interconnect model. This metric was also paired with other topology metrics to determine critical nodes and edges to remove. In [23], network efficiency is used to quantify overall network performance and the impact that potential damages or improvements can have on European transmission systems.

While these methods attempted to describe power systems and identify critical assets, many early approaches are insufficient. Though the metrics are relatively straightforward and easy to compute, they are fundamentally unable to capture the properties of electric power flow. As

explored in [29], strictly topological measures can yield misleading results without properly accounting for power flow properties. Without careful consideration and context, this type of analysis could result in the misallocation of vital outage mitigation resources and fail to fortify against large-scale blackouts. To combat this, several groups have proposed using models and metrics that balance more fully capturing electrical properties and maintaining the ability to inspect emergent features.

3.3 Extended Complex Networks

In order to address some of the challenges associated with traditional network theory metrics, research has been done to examine better ways to represent power systems. For example, one method sought to characterize the Eastern Interconnect by creating similarly sized random, small world, and preferential attachment graphs and comparing various graph measures. From there, the physical topological representation was converted to an electrical topology by using system Y-bus information and converting edges to represent an electrical distance between nodes [26]. Another method sought to utilize information on historical outages to identify common groupings of component failures and seize on the observation that not all cascading outages propagate locally [30]. This led to the creation of an influence graph that can provide a means of measuring the "influence" that one component has on any other component to propagate a failure. In [25], the role that topological structure plays on system vulnerability was highlighted, and suggestions for a new electrically focused representation were proposed. Ultimately, all these methods share the common vein of integrating more information about power system behaviors to produce a more powerful tool with more meaningful conclusions.

With these new network characterizations, familiar concepts and metrics in traditional network theory analysis can be applied to spur new insights. For example, [25] draws new conclusions about which nodes in the network are most central based on the electrical topology of the grid. In [31], a closeness centrality metric is used with influence graphs to determine which groups of components are most vulnerable to initiating a cascading outage. Other methods have utilized power transfer distribution factors (PTDFs) and transmission line capacities to formulate an extended betweenness metric to analyze system vulnerabilities [24].

In this same vein of expressing previously unaccounted electrical characteristics, other methods exist to account for non-technical elements of power system operation. For example, game theory applications offer meaningful insight into attacker and response strategies that extend beyond the ECNs. An in-depth analysis of tools like these are beyond the scope of this paper, but discussion of ECN structures and metrics would be incomplete without alluding to them.

3.4 Correlation Studies on Standard Network Theory Metrics

A useful exercise in evaluating any of the metrics proposed in this paper is to compare the results of the metrics against each other. In literature, there have been several efforts to analyze how metrics correlate with each other, why they may be correlated, and how this impacts power system network models [28], [32]-[35]. In general, these studies have focused on relationships between metrics, as in [28], [33] and [34]. A major conclusion in [28] found that blackout size measured by the power supply metric was best tracked using a topology-based source-demand efficiency metric. In [33], using Spearman rank correlation between metrics and cascade depth, researchers found that some metrics had a negative correlation, concluding that removing some

nodes may improve system performance. Reference [34] demonstrates that metrics such as degree, eigenvector, and closeness centrality are all poor indicators of asset rankings, while betweenness seemed to track with metrics capturing bus injection responses and line outage distribution factors.

Other studies have found that network structure plays a significant role in determining relationships between metrics. In [34], the authors suggest that a more apt metric would be how different a given network is to a threshold graph, since centrality metric correlations adjust with changing network structure. Ultimately, this study suggested some skepticism about how useful a single metric can be when metrics with competing definitions yield similar rankings. A similar conclusion was drawn in [35], where metric correlation strength varied with the type of network considered. Overall, these studies provide good initial insights into validating the conclusions drawn from modeling power systems as ECNs and applying ECN metrics. That being said, more rigorous analysis could assist in selecting metrics that are computationally cheap yet track well with information that utilities collect, such as outage sizes.

4.0 Analysis of Select Extended Complex Network Metrics

To expand on the network theory analysis of electric power systems, this research will explore methods of investigation like those seen in the study of blackouts in Section 2.0. The primary focus will be on statistical analysis of centrality metric distributions and how information from this analysis may fit into the broader study of bulk transmission power system blackouts. To this aim, the metrics selected for this research will be tested for power-law tails, which convey information about frequency of highly central buses in a system. This testing will aid in analyzing whether these metrics are revealing system behaviors that track with trends seen in large blackout data. Comparison of these metrics will also yield information about the broader task of performing system vulnerability analysis.

In summary, the analysis was conducted as follows. First, system information was gathered and used to calculate the metrics. These calculated values were then ranked and compiled into complementary cumulative probability distribution functions (CCDFs) to illustrate system state. From there, these CCDFs were then tested for fits to parametric distributions and tested for heavy-tailedness. Lastly, the calculated metrics for each system were compared to identify potential relationships between metrics and with blackout size distributions.

To this end, a sample of metrics proposed in the literature will be briefly introduced in Section 4.1, along with the sets of synthetic networks used in the analysis and the justification for their use. Following in Section 4.2, the statistical analysis and tests run on the metrics will be explored.

4.1 Selected Networks and Metrics

4.1.1 Synthetic Networks

In order to examine emergent trends in ECN metric performance, several networks of various sizes are used to account for potential variance in performance. Many test cases, including IEEE test cases, are often used for network theory metric validation. Though the 300-bus test case was used in this analysis, a desire for analogs to real electric power systems led to the incorporation of other test networks. As a result, synthetic networks from Texas A&M University [36] became central to the group of networks used for this work. These synthetic networks approximate transmission infrastructure in the United States using publicly available load and generation data. Since accessing real network data through the Critical Energy Infrastructure Information (CEII) Request process is often cumbersome due to the sensitive nature of the information in question, having synthetic networks that are derived from publicly available data provides an interesting, if not exact, analog to North American electric power systems without the need for managing CEII. In this catalog of networks, the 500-bus South Carolina model, the 2,000-bus Texas Interconnect model, the 10,000-bus Western Electricity Coordination Council (WECC) model, and the 25,000-bus U.S. Northeast model were all selected to provide a diverse range of network sizes. An additional network from the MATPOWER [37] software package, a 6468-bus model of the French VH voltage transmission network, was also used to provide an intermediate sized network to analyze between the 2,000-bus Texas model and the 10,000-bus WECC model.

Table 2 provides for comparison the list of networks used in this analysis and some fundamental characteristics of their respective network structures. The average degree represents the average number of connections a given bus has in a network, and maximum degree represents

the most connections a single bus has. Characteristic path length is the average of all the shortest paths' lengths between pairs of buses in the network, giving insight into sparse or well-connected a network is. Network diameter gives further insight by measuring the longest shortest path, while clustering coefficient gives insight into how well-connected buses and their neighbors are. Lastly, degree assortivity tells how much buses connect with other similarly well-connected buses. For example, negative degree assortivity indicates a given bus will more often than not connect to a bus with fewer total connections.

Table 2 Network Statistics for Selected Networks

	IEEE 300	**French VH Trans**	**Synth. S.C.**	**Synth. T.X.**	**Synth. WECC**	**Synth. U.S. NE**
Nodes	300	6468	500	2000	10000	25000
Edges	409	8065	584	2667	12217	30110
Avg. Degree	2.73	2.49	2.34	2.67	2.44	2.41
Max. Degree	11	15	14	16	17	17
Characteristic Path Length	9.93	14.96	9.49	12.98	22.53	33.45
Network Diameter	24	34	20	30	52	91
Clustering Coefficient	0.11	0.059	0.023	0.0061	0.019	0.026
Degree Assortivity	-0.22	-0.17	-0.25	-0.18	-0.076	-0.091

It should also be mentioned that this focus on synthetic networks, while necessitating an assessment on what types of meaningful information can be obtained from them, does not preclude connections to real networks. In fact, this work can provide a framework for analyzing real power systems and much of the testing discussed can be retooled for testing of existing power systems.

4.1.2 Extended Complex Network Metrics

As mentioned in Section 3.3, ECNs incorporate elements of electric power systems that are not readily captured in more traditional complex network analysis. To facilitate this, a network representation of the power system is constructed based on the element of interest. Ultimately, this network representation will create new connections, new edge weights, or new flows to translate the electric power system phenomenon to network theory. However, different representations often focus on a specific property or set of properties as it pertains to power system behaviors and analysis. For the sake of the analysis presented here, metrics will belong to one of three categories, based on their accompanying ECN and what information the metric is utilizing: metrics examining system structure and metrics examining system operation.

4.1.2.1 System Structure Metrics

Metrics that examine system structure will utilize physical properties of electric infrastructure to construct network representations and formulate extended metrics. Therefore, these metrics should provide insight on the state of the network as a function of how buses and transmission lines are connected and the electrical properties of these components. In this group, two standard metrics and three extended network metrics will investigate the impact of system

structure on system vulnerabilities. A summary of the system structure metrics used in this analysis can be found in Table 3.

Table 3 System Structure Critical Asset Identification Metrics

Metric	Equation	Description of Centrality
Standard Degree	$\deg(v) = \sum_{i \neq j} a_{ij}$	Buses with the most connections
Standard Betweenness	$C_b(v) = \sum_{s \neq t \neq v} \frac{\sigma(s,t\|v)}{\sigma(s,t)}$	Buses appearing most often in shortest paths
Electric Degree	$e_C(v) = \sum_{i \neq j} Z_{ij}$	Buses connected to lowest impedance paths
Electric Betweenness	$e_b(v) = \sum_{s \neq t \neq v} \frac{\sigma^Z(s,t\|v)}{\sigma^Z(s,t)}$	Buses appearing most often in electrical shortest paths
Susceptance Degree	$C_{deg}^B(v) = \frac{\sum_k b_{ik}}{\sum_i \sum_k b_{ik}}$	Buses connected to high susceptance lines

The two metrics standard metrics used in this analysis are node degree centrality and node betweenness centrality. In this analysis, the network calculation for both metrics is conducted under the assumption that the network is undirected and unweighted, which allows for a focus on how buses and lines are connected in the network rather than functional relationships between buses and transmission lines. The first metric, node degree centrality, measures the connectivity of a node to other nodes in the network and can be determined using the adjacency matrix of the network. The following equation is used to calculate node degree centrality:

$$\deg(v) = \sum_{i \neq j} a_{ij} \tag{4-1}$$

where v is in the subset of vertices of G, and a_{ij} is the elements of the adjacency matrix of G. The second, node betweenness centrality, measures how often a node appears as a step in the shortest paths connecting other pairs of nodes, where edge weights are the cost of taking a route. The following equation is used to calculate node betweenness centrality:

$$C_b(v) = \sum_{s \neq t \neq v} \frac{\sigma(s,t|v)}{\sigma(s,t)} \tag{4-2}$$

where $\sigma(s,t|v)$ is the set of shortest paths between node s and node t that include node v, and $\sigma(s,t)$ is the set of all shortest paths between s and t. One of the main reasons for the inclusion of these two standard metrics is establishing and understanding the underlying framework that the other extended metrics are based off and providing a frame of reference for analyzing the extended metrics. Every metric considered in this work is some extension of degree or betweenness centrality.

The three extended metrics in this group are electric node degree centrality, electric node betweenness centrality, and susceptance node degree centrality. Like the standard metrics, all three of these metrics rely on an undirected network representation of the system being studied. However, in contrast, these three use weighted edge connections derived from transmission line impedance data to assign metric importance. Each of the two electric centrality metrics utilize system Z_{bus} information to update the adjacency matrix and construct the network representation, resulting in a fully connected network, or a network where each node has a connection with every other node. This approach seeks to find the strongest electrical connections between buses in a power system, which often are not represented by the physical connections seen in an electrical drawing. The electric node centrality metric is discussed in [25], and is calculated using the following equation:

$$e_C(v) = \sum_{i \neq j} Z_{ij} \tag{4-3}$$

where Z_{ij} represents the impedance connecting nodes i and j. A cursory comparison of Equations (4-1) and (4-3) reveals that $e_C(v)$ mimics the structure of the standard centrality metric, except rather than using the adjacency matrix describing physical connections, the Z_{bus} matrix is being used instead. A similar comparison can be drawn between the standard node betweenness centrality and the electric node betweenness centrality, which is calculated in [30] using the following equation:

$$e_b(v) = \sum_{s \neq t \neq v} \frac{\sigma^Z(s,t|v)}{\sigma^Z(s,t)} \tag{4-4}$$

where $\sigma^Z(s,t|v)$ is the set of shortest electrical paths between nodes s and t that pass through v, and $\sigma^Z(s,t)$ is the set of all shortest electrical paths between nodes s and t. As with the degree centrality metrics, the betweenness centrality metrics differ in what the adjacency matrix and edge weights are set to be.

Last of this group, susceptance node degree centrality utilizes only susceptance information of transmission lines rather than the Z_{bus} information. In approaching the system this way, the same adjacency matrix can be used that describes physical connections, as done so for the standard metrics, however edge weights are assigned based on susceptance of the transmission line in question. In order to maintain the requirements of what constitutes a metric, which is discussed in [26] for a different measure of electric degree centrality, all negative reactances are treated as zero to maintain triangle inequality requirements. Susceptance degree centrality is calculated in [17] using the following equation:

$$C^B_{deg}(v) = \frac{\sum_k b_{ik}}{\sum_i \sum_k b_{ik}} \tag{4-5}$$

where b_{ik} is the line reactance between nodes i and k. Ultimately, this extended degree centrality attempts to provide insight into line reactance relative to total system reactance and potential impacts that may have on voltage angle differences between buses. provides a summary of the system structure metrics used in this analysis.

4.1.2.2 System Operation Metrics

As compared to system structure, system operation instead focuses on how power flows through a network. Though system operation metrics can be affected by some of the same mechanisms as system structure metrics, asset vulnerability measured by system operation metrics can also be impacted by disconnecting loads or generators. Unlike system structure metrics, this provides insight into how day-to-day operation affects system vulnerabilities since system structure is often less volatile than generation profiles for renewables, as an example. In this paper, static loads and generation will be used, though this kind of metric could be reapplied in real-time with updated power flows and sensor data that better reflect system operation at that point in time. A summary of the system operation metrics used in this analysis can be found in Table 4.

Table 4 System Operation Critical Asset Identification Metrics

Metric	Equation	Description of Centrality
Power Flow Degree Centrality	$C_{deg}^{PF}(v) = \sum_{i \neq j} \lvert P_{ij} \rvert$	Buses with the most inflow/outflow of real power
Power Flow Betweenness Centrality	$C_{b}^{PF}(v) = \sum_{s \neq t \neq v} \frac{P_{st}(v)}{P_{st}}$	Buses with high power traffic in shortest power flow paths
Power Flow Edge Betweenness Centrality	$C_{b}^{PF}(e) = \sum_{s \neq t \neq v} \frac{\sigma^{PF}(s,t\lvert e)}{\sigma^{PF}(s,t)}$	Lines appearing most in highest power flow paths
Series Power Loss Degree Centrality	$C_{deg}^{SPL}(v) = \frac{\sum_k \frac{1}{2}(P_{ik} + P_{ki})}{\sum_i \sum_k \frac{1}{2}(P_{ik} + P_{ki})}$	Buses connected to lines with highest real power losses
Modified Susceptance Degree Centrality	$C_{deg}^{B}(v) = \frac{\sum_k b_{ik} \cos(\theta_i - \theta_k)}{\sum_i \sum_k b_{ik} \cos(\theta_i - \theta_k)}$	Buses connected by high susceptance lines causing large "injections" of reactive power

The first metric considered in this category is power flow (PF) node degree centrality. This centrality metric captures information about which buses act as thoroughfares for real power transmission by incorporating load flow data into the network representation. More precisely, a weighted and directed network representation forms the basis for this metric, with edge weights set to real power flow in the corresponding transmission lines and edge directions determined by the direction of real power flow. The metric value is assessed to be the sum of all power inflow and outflow from the bus, or as it is more formally described in [38]:

$$C_{deg}^{PF}(v) = \sum_{i \neq j} \lvert P_{ij} \rvert \tag{4-6}$$

where P_{ij} is the power flow from node i to node j. By taking the absolute value, transmission buses can be properly weighted for their role in both receiving from and delivering to other buses in the network. Constructing the metric this way also ranks similarly sized generation and load buses, which can be useful in examining generation and loads in a uniform manner.

Continuing with power flow analysis, PF node betweenness centrality and PF edge betweenness centrality provide similar valuations for network nodes and edges, respectively. Keeping with earlier betweenness metrics, the PF node betweenness metric analyzes which buses in the network experience large real power flows in high power traffic paths. Much like the earlier betweenness metrics, shortest paths are calculated by finding the combination of edges yielding the lowest cost path. To stay consistent with this, the inverse of real power flow is used, encouraging shortest path tracking to take high traffic routes. Though not perfectly accurate in describing power flow behaviors, this allows for high power flow traffic nodes to be properly identified. As described in [38] and [17], the PF node betweenness centrality of a bus is determined using the equation:

$$C_b^{PF}(v) = \sum_{s \neq t \neq v} \frac{P_{st}(v)}{P_{st}} \tag{4-7}$$

where $P_{st}(v)$ is the highest power inflow or outflow through node v in the path between nodes s and t, and $P_{st}$is the highest power inflow or outflow in the entire path between nodes s and t.

In contrast, PF edge betweenness centrality seeks to assign value to edges in the network. Though somewhat computationally different, the general premise remains the same. This metric ranks highly those edges that appear most often in power flow shortest paths. Using the same edge weights and directions as for PF node betweenness, the network representation used is weighted and directed. More formally, the metric, in part described in [38], is calculated using the following:

$$C_b^{PF}(e) = \sum_{s \neq t \neq v} \frac{\sigma^{PF}(s,t|e)}{\sigma^{PF}(s,t)} \tag{4-8}$$

where $\sigma^{PF}(s,t|e)$ is the set of shortest paths between nodes s and t that include edge e, and $\sigma^{PF}(s,t)$ is the set of all shortest paths between nodes s and t. Though this form more closely follows the form of the standard betweenness metric, the underlying edge weights incorporate the power flow behaviors of the system under study.

The last PF metric in this grouping is series power loss (SPL) node degree centrality. Capturing a slightly different phenomenon, SPL node degree ranks highly those buses that are either connected to high loss transmission lines or many lower loss lines, which can indicate high traffic buses and long-distance lines or highly connected hubs, respectively. SPL degree centrality utilizes the same network representation as PF degree centrality, with edges being weighted according to their real power traffic and directions determined by the direction of real power flow. In [17], SPL node degree centrality is defined as:

$$C_{deg}^{SPL}(v) = \frac{\sum_k \frac{1}{2}(P_{ik} + P_{ki})}{\sum_i \sum_k \frac{1}{2}(P_{ik} + P_{ki})} \tag{4-9}$$

where P_{ik} is the power outflow read from bus i going to bus k, and P_{ki} is the power outflow read from bus k going to bus i. This formulation allows for a less direct and more relaxed approach to finding buses in vital power traffic paths. As an example, this metric would also likely favor buses connected to long-distance lines that service disparate parts of a power system. While the power flow on the line may not excessively large compared to other branches in the system, this metric would be sensitive to the higher power losses associated with this line.

The last metric considered for analysis is the modified susceptance node degree centrality metric. The modified centrality deviates from the original susceptance degree centrality by

integrating information about voltage angle differences between buses into the calculation. Explained in [17], this inclusion of voltage angle information yields metric values based loosely on the concept of reactive power injections into the system. The equation for finding the modified susceptance node degree centrality is:

$$C_{deg}^{B}(v) = \frac{\sum_k b_{ik} \cos(\theta_i - \theta_k)}{\sum_i \sum_k b_{ik} \cos(\theta_i - \theta_k)} \tag{4-10}$$

where b_{ik} is the susceptance between nodes i and k, θ_i is the voltage angle at node i, and θ_k is the voltage angle at node k.In a stable and well-designed system, this metric will likely not differ much from the unmodified version. However, this metric might prove useful when examining systems under heavy load or in situations where multiple failures have occurred. Further investigation into these scenarios should be pursued, however that is outside the scope of this research. System tests will only be considered for steady-state and normal loading conditions.

4.2 Heavy Tail Analysis Methodology

After calculating CCDFs for all the metrics and networks, each metric is tested for a power-law relationship in the tail of the metric value distributions. The primary motivation for focusing on the tail of the CCDFs is to attempt to draw parallels to studies conducted on North American blackout data. In [8] and [9], studies of blackout size distributions found that blackout frequency did not decay exponentially with blackout size. Rather, blackout size distributions demonstrated a power-law tail, indicating that large blackouts occur at relatively significant rates. This

phenomenon is more generally referred to as a heavy tail, meaning that the tail of the distribution decays slower than an exponential, causing larger events to carry greater risk. More specifically, power-law distributions take the following form:

$$P(x) = C(\frac{x}{x_{min}})^{-\alpha} \tag{4-11}$$

where x_{min} is the lower bound of the distribution, α is the scaling parameter, and C is a scalar value. Typical values for α are between 2 and 3, with lower values indicating heavier tails with large events representing more substantial risk. However, in the case of blackout data, the scaling parameters were in the 1 to 2 range, suggesting a greater frequency of large blackout events.

In order to carry out the heavy tail testing, the method presented in [39], which was also used in the study of blackout data, will be used along with its supporting open-access code repository. In summary, this implementation calculates the scaling parameter for a range of lower bound values and determines the best fit from these potential power-law fits. More precisely, the method estimates the scaling parameter for a given lower bound using the maximum likelihood estimator:

$$\hat{\alpha} = 1 + n\left[\sum_{i=1}^{n} ln\frac{x_i}{x_{min}}\right]^{-1} \tag{4-12}$$

where x_i are all the n observations in the sample greater than x_{min}, and x_{min} is the lower bound of the power-law distribution. The resulting model, with the assumed x_{min} and calculated $\hat{\alpha}$, is compared against the empirical data using the Kolmogorov-Smirnov (KS) statistic:

$$D = \max_{x \geq x_{min}} |S(x) - P(x)| \tag{4-13}$$

where $S(x)$ is the empirical CCDF for x greater than or equal to x_{min}, and $P(x)$ is the best fit model for x greater than or equal to x_{min}. Plainly stated, the KS statistic finds the maximum distance between the empirical CCDF data and the power-law model. Once the KS statistic is

calculated for all x_{min} in the range, the x_{min} and subsequent $\hat{\alpha}$ that minimized the KS statistic is chosen as the best power-law fit.

The estimated power-law model is then tested for goodness-of-fit, where a p-value of 0.1 or greater indicates that the model is a plausible fit for the data. It should be noted that this test does not reject or fail to reject a power-law fit in the traditional sense. Rather, the test signifies a potential fit that can be compared against others in a likelihood-ratio test, as an example. The scope of this work will be contained to identifying candidate metrics for deeper comparative analysis. Much like the power-law testing done for blackout data analysis, the testing here seeks to better understand power system structure, operation, and failure. The central tie between these sets of heavy tail testing comes in being able to determine whether highly connected buses or lines are not uncommon, and even constitute a significant portion of system infrastructure. Moreover, if highly central nodes are more common, then random failures have a higher likelihood of components critical to system functionality being taken out of service and severely disrupting electric power systems. While this isn't necessarily suggestive of a causal relationship, it may prove to be a sufficient indicator of system vulnerability.

5.0 Results

Each of the ten metrics were calculated for each of the six networks described in Section 4.1. For graphical and process clarity, metric calculations will be displayed across networks, which will allow for preliminary visual analysis before further examining potential power tail relationships and correlations. As a further breakdown, metrics classified as system structure metrics will be displayed first, followed by system operation metrics. These groupings will also be maintained for the system metric correlation analysis.

5.1 System Structure Metric Distributions

In this class of metrics, standard node degree centrality, standard node betweenness centrality, electric node degree centrality, electric node betweenness centrality, and susceptance node degree centrality have been calculated for the six networks under study. All metrics are normalized based on the maximum metric value for a given network and metric, yielding metric values in the range of 0 to 1. This normalization provides the opportunity to compare metric calculations and distribution shapes across the six networks. Some metric distribution plots are trimmed in order to more easily examine the tails, which will be the focus of Section 5.3. The inclusion of the standard degree and betweenness metrics will also illustrate how ECN metrics provide a finer level of differentiation between buses and lines within a network. This will also provide a point of reference when comparing metrics and performing correlation analysis in Section 0.

The six CCDFs for the first metric in this category, standard node degree centrality, can be found in Figure 2. Lines in the scatter plot are present for graphical clarity only. After compiling the metric values for all six networks, a common trend between the networks is the tight binning of metric values. Due to the discrete nature of the metric, metric values are restricted to integers and result in many nodes taking the same value. This poses a problem for distinguishing between system components and analyzing criticality with a significant level of detail.

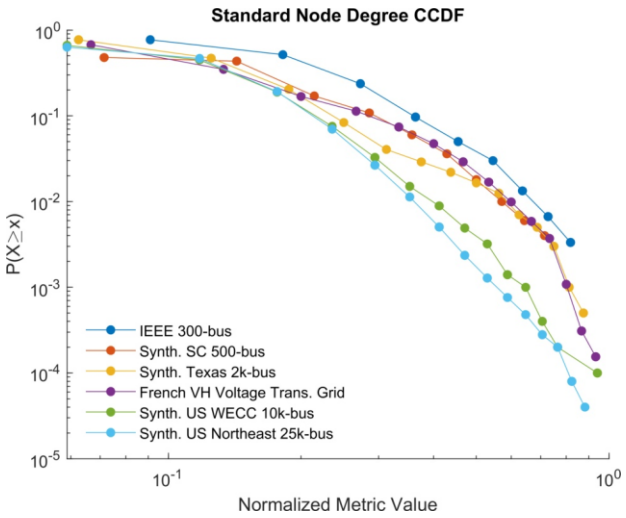
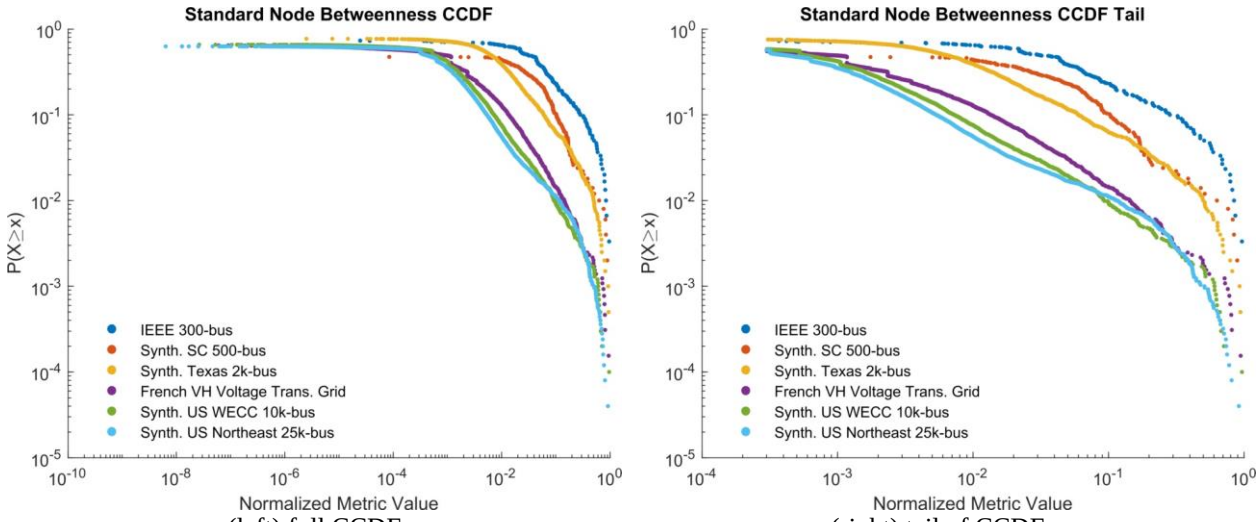


Figure 2 Standard Node Degree Centrality CCDFs

Continuing with standard network theory metrics, Figure 3 shows each of the six CCDFs for the standard node betweenness metric. When comparing the six networks, there appears to be a significant difference between smaller and larger power systems in how these metric values distribute themselves. Most of these systems also appear to have flat power law regions followed

by an exponential drop-off at the end of the tail, though the degree to which that is borne out would need to be further validated.



(left) full CCDFs (right) tail of CCDFs

Figure 3 Standard Node Betweenness Centrality CCDFs

Illustrating the first extended metric, Figure 4 displays each of the six CCDFs for the electric node degree metric. Unlike the previous metrics discussed, the shapes of the distributions appear not to be as strictly scaled based on network size and indicate widely varying network complexity. As an example, the Synthetic South Carolina 500-bus model's CCDF shows a distribution with a tight range of normalized metric values. This suggest a system that is, electrically speaking, uniformly well-connected, with no singular bus or set of buses connecting more disparate sections together. Overall, these varying distributions signify the complexity of power system structures and the variability between them.

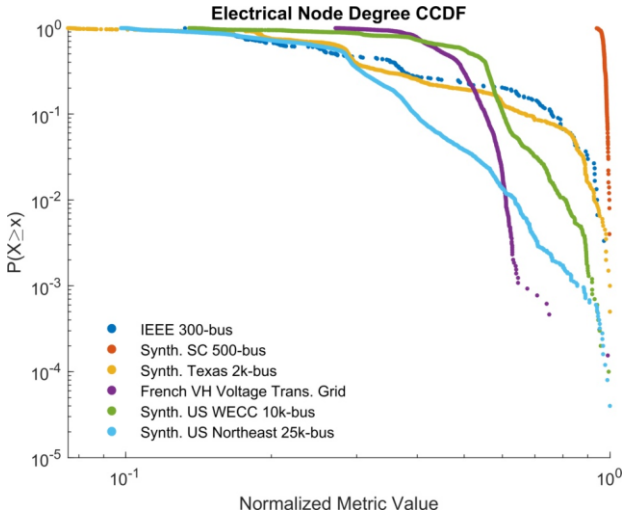
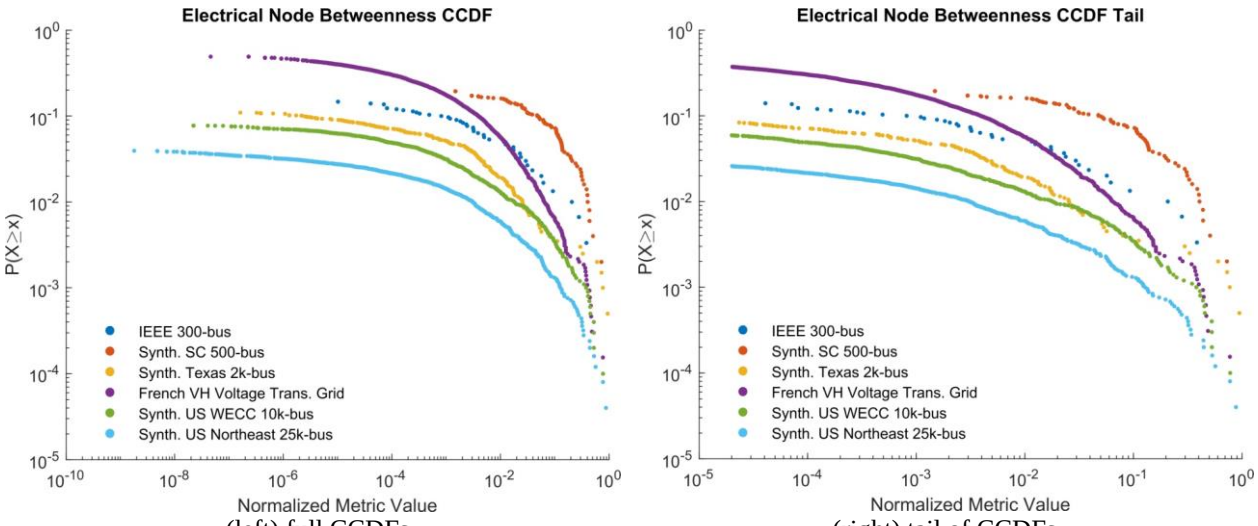


Figure 4 Electrical Node Degree Centrality CCDFs

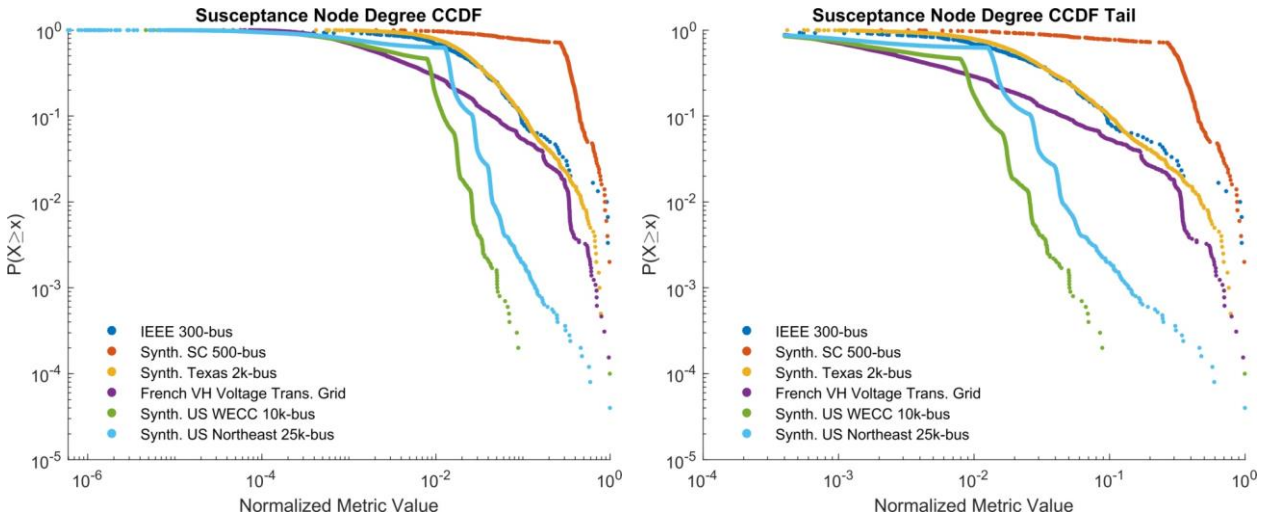
Using the same network structure derived for electric degree centrality, electric node betweenness measures which buses appear most frequently in the shortest electrical paths. In electrical terms, this represents which nodes are electrically central and show up in common low impedance paths. Figure 5 shows each of the six CCDFs for the electric node betweenness metric. While not evident in the figure, because of how the metric is computed, roughly 25% to 35% of buses for a given network are not represented in the plot due to not being passed through in any of the shortest paths (i.e. a metric value of 0). This could potentially be a result of centralized structure of power systems, where edge (or leaf) buses would not necessarily be well-connected to other buses, but central generation and transmission buses would be relatively well-connected to all edge buses. In any case, this does provide a level of asset filtering not seen in degree-based metrics.



(left) full CCDFs (right) tail of CCDFs

Figure 5 Electrical Node Betweenness Centrality CCDFs

The last metric in this grouping, susceptance node degree centrality, focuses more acutely on the susceptance component of impedance for transmission lines in a network. As a result, this metric can potentially yield information about the flow of reactive power in a network and how that impacts rankings for critical power system infrastructure. Figure 6 shows each of the six CCDFs for the susceptance node degree metric. For the South Carolina, WECC, and U.S. Northeast models, there is a pronounced bend in the distributions, indicating cutoff points where the tail of distribution decays quickly. These bends also likely preclude robust power-law relationships in the tail of the distributions.



(left) full CCDFs (right) tail of CCDFs

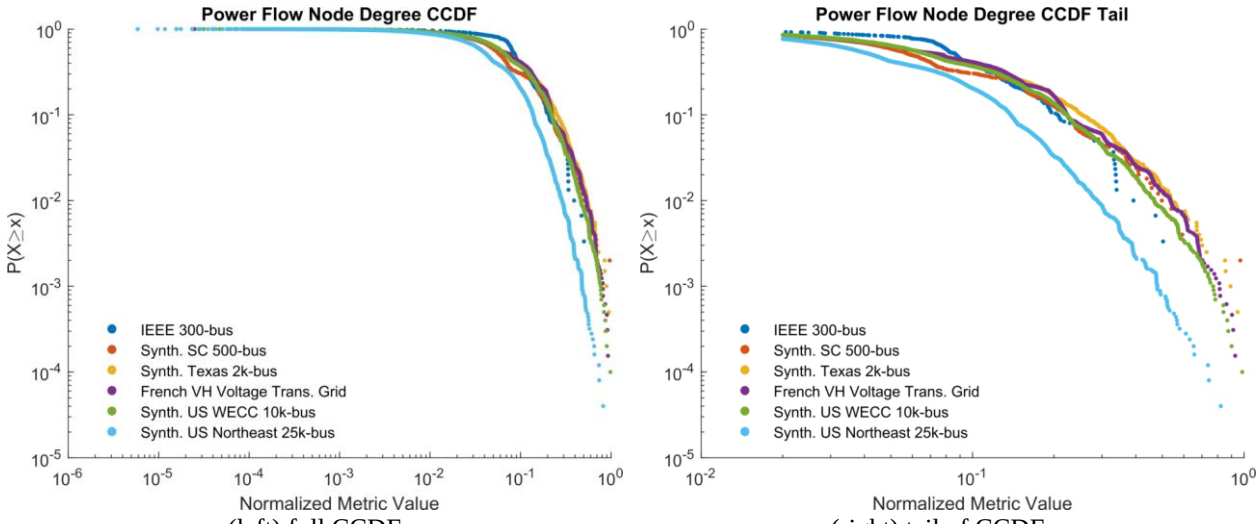
Figure 6 Susceptance Node Degree Centrality CCDFs

5.2 System Operation Metric Distributions

The system operation centrality metrics considered for this study are power flow node degree, power flow node betweenness, power flow edge betweenness, power series losses node degree, and modified susceptance node degree. All metrics are normalized based on the maximum metric value for a given network and metric, yielding metric values in the range of 0 to 1. This normalization provides the opportunity to compare metric calculations and distributions across the six networks. As mentioned previously, these metrics attempt to capture aspects of power system operation that is not otherwise readily captured by network theory metrics, rather than strictly analyzing structural properties of a power system.

First analyzed in this group is the power flow node degree centrality metric, which identifies nodes that act as major thoroughfares for real power flow in the system. All networks

have load flow data simulated using MATPOWER, which utilizes an AC solver based on Newton's method. Figure 7 shows each of the six CCDFs for the power flow node degree metric. The CCDFs in this group all share similarly distributed tails, indicating that there may be consistent applicability across networks of different sizes and configurations. That being said, the Synthetic U.S. Northeast network does show a more exponential tail than the other networks, and broader analysis would need to be conducted, especially for large networks.

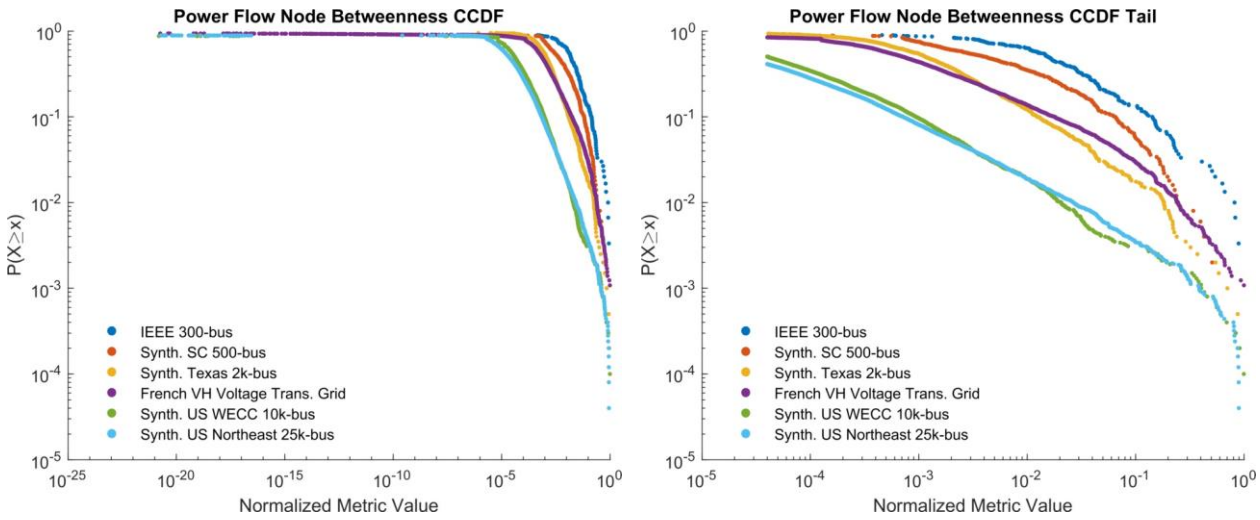


(left) full CCDFs (right) tail of CCDFs

Figure 7 Power Flow Node Degree Centrality CCDFs

Keeping with power flow-based analysis, power flow node betweenness centrality is determined using the same network representation. Figure 8 shows each of the six CCDFs for the power flow node betweenness metric. Much like the other betweenness metrics, roughly 25% to 35% of the buses in each network do not have a significant betweenness value. However, since some lines may carry orders of magnitude less power than other lines in the same path, and directed networks allow for fewer potential paths, the metric value of the lower betweenness buses manifest as approaching zero rather than being zero. Also, as can be seen in the tails of the CCDFs, tail

distribution flatness appears to be dependent on system size with larger networks appearing to have flatter, though not necessarily power-law, tails.



(left) full CCDFs (right) tail of CCDFs

Figure 8 Power Flow Node Betweenness Centrality CCDFs

Taking another approach to investigating the impact of power flow behaviors and system operation in power systems, the power flow edge betweenness metric is investigated next. The power flow edge betweenness metric is calculated using a version of the Floyd-Warshall algorithm for finding all shortest paths for node pairs. The implementation used here can identify one of the shortest paths between a pair of nodes, however if multiple paths exist, they are not distinctly identified. Nonetheless, due to load flows taking real values, it is unlikely that a significant number of shortest paths are omitted so as to impact the general shape of the CCDFs. Figure 9 shows each of the six CCDFs for the power flow node betweenness metric. Based on this figure, the distributions appear to flatten for larger networks in the intermediate connectivity range. Further testing will be conducted to determine if this is a power-law tail, however it the very ends of the tails indicate a power-law tail with exponential cutoff.

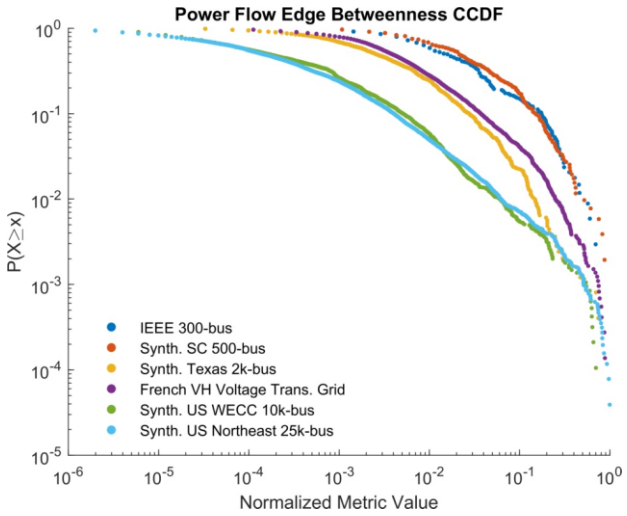
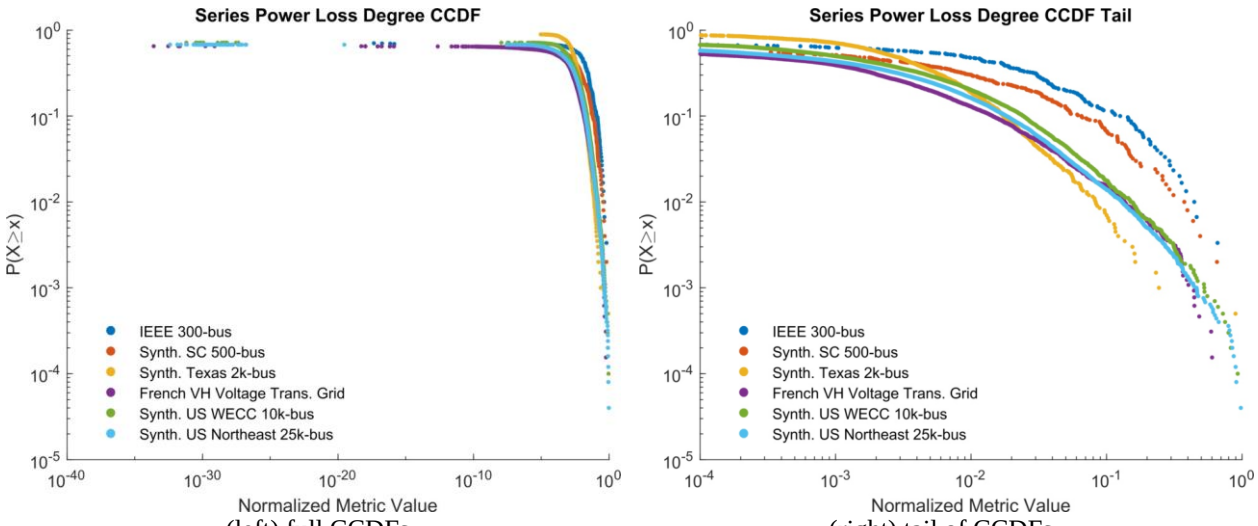


Figure 9 Power Flow Edge Betweenness Centrality CCDFs

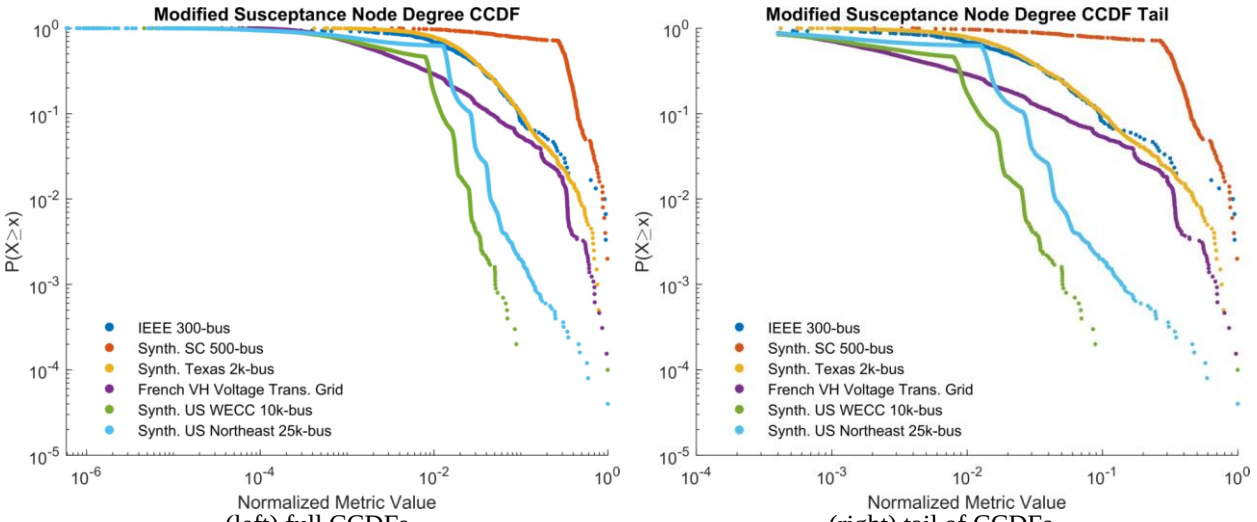
The next metric considered in the system operation group is the SPL node degree metric, with CCDFs found in Figure 10. Along with power flow node degree, series power loss degree also shows relatively similar tails for all the networks. More exhaustive testing of network sizes and complexities should be conducted to see if this pattern holds, though the consistency of distribution shape does provide some initial evidence for a candidate metric in further critical asset and blackout analysis.



(left) full CCDFs (right) tail of CCDFs

Figure 10 Series Power Loss Degree Centrality CCDFs

The last metric analyzed is the modified susceptance node degree centrality. Compared to the system structure metric version of susceptance degree, the modified distributions take very similar shapes. This is due to the stable power flows of each of the networks, resulting in no significant angle differences between buses. Without many significant angle differences, the original and the modified susceptance node degree CCDFs are superficially similar with limited differences in metric values between the two. Investigation of real-time metric calculations, especially during high-stress operation such as peak load, may yield more significant differences and warrant inclusion of bus angle differences in the metric calculation. The CCDFs for the six networks studied can be found in Figure 11.



(left) full CCDFs (right) tail of CCDFs

Figure 11 Modified Susceptance Degree Centrality CCDFs

5.3 Complementary Cumulative Distribution Heavy-Tail Testing

With the CCDFs of all ten metrics across each of the six networks compiled, more rigorous testing of the shape of these distributions can be conducted. As described in Section 4.2, heavy-tail tests were applied to all CCDFs to identify candidate metrics and assist in explaining blackout size distributions. In order to recognize significant fits, two criteria were followed. The first set a threshold value for α at 3 or less. This allowed for recognition of true heavy-tail relationships that fell within the bounds of typical power-law distributions and remained close to the shape of blackout size distributions. The second criterion was the p-value discussed for testing goodness-of-fit for the power-law distribution. Since, according to [39], a p-value of 0.1 or greater provides meaningful insight without being overly inclusive, this threshold is maintained in this work. The final p-value calculations can be found in Table 5, with the corresponding α values in Table 6. All significant relationships have their values in bold in the tables.

Table 5 Power Law Tail Significance Testing (p-values)

	ECN Metrics									
	Structural					Operational				
Network	**Standard Degree**	**Standard Bet.**	**Electric Degree**	**Electric Bet.**	**Sus. Degree**	**Power Degree**	**Power Bet.**	**Power Edge Bet.**	**Power Loss Degree**	**Modified Sus. Degree**
IEEE	0.512	0.048	0	**0.613**	**0.182**	0.034	0.024	0.074	**0.770**	**0.191**
Synth. SC	0.163	**0.662**	0.074	0.024	0.073	0.498	**0.149**	**0.345**	**0.406**	0.071
Synth. TX	0	0.002	0.001	**0.508**	0.023	0.102	0.011	0.058	**0.903**	0.037
French HV	0	0	0	0.032	0	0.011	0	0	0	0
Synth. WECC	0.012	0.082	0	0	0	0	**0.187**	**0.516**	0	0
Synth. US NE	0.095	0	0	0.077	**0.959**	0.01	0.023	**0.903**	0.002	**0.967**

Table 6 Power Law Tail Significance Testing (α values)

	ECN Metrics									
	Structural					Operational				
Network	**Standard Degree**	**Standard Bet.**	**Electric Degree**	**Electric Bet.**	**Sus. Degree**	**Power Degree**	**Power Bet.**	**Power Edge Bet.**	**Power Loss Degree**	**Modified Sus. Degree**
IEEE	10.17	1.861	2.297	**1.645**	**2.182**	2.794	1.900	2.078	**2.919**	**2.180**
Synth. SC	6.056	**2.419**	186.3	2.426	5.197	3.479	**2.458**	**2.813**	**2.617**	5.199
Synth. TX	6.892	1.824	22.87	**1.613**	2.338	4.236	1.739	2.191	**2.473**	2.336
French HV	2.404	2.015	12.39	1.964	1.829	5.540	1.571	1.839	2.070	1.829
Synth. WECC	9.402	1.896	13.37	1.453	4.311	3.897	**1.727**	**1.985**	2.199	4.312
Synth. US NE	12.05	1.849	6.059	2.026	**2.722**	4.695	1.628	**1.919**	2.303	**2.722**

The following figures illustrate the power-law fits for those metrics that satisfied the two criteria, separated by network. Though not formalized, lower bounds will also be discussed briefly for those metrics with substantial relationships. Because power-law tails should constitute a meaningful segment of the distribution and provide a sufficient number of samples to draw a reasonable conclusion about the nature of the distribution tail, x_{min} values and the percentage of buses with values greater than x_{min} are also provided. For graphical clarity and to be able to examine distribution tails more closely, all fifteen figures use their corresponding trimmed CCDF bounds seen in Sections 5.1 and 5.2, where applicable. The trimmed bounds, in conjunction with the reported percentage of buses greater than x_{min}, should provide adequate context for the CCDFs and their fits.

The first power-law fit for the Synthetic South Carolina 500-bus model can be seen in Figure 12. Across the six networks, only this standard network theory metric CCDF suggested potential for a power-law distributed tail, with an α value of 2.419 and roughly 20% of buses with a centrality score greater than or equal to x_{min}. While this represents one of the stronger power-tail fits, it is not reproduced in any of the other networks and the relatively small set of nodes in the power-law region suggest a need for examining these results on larger networks with similar structure and network complexity.

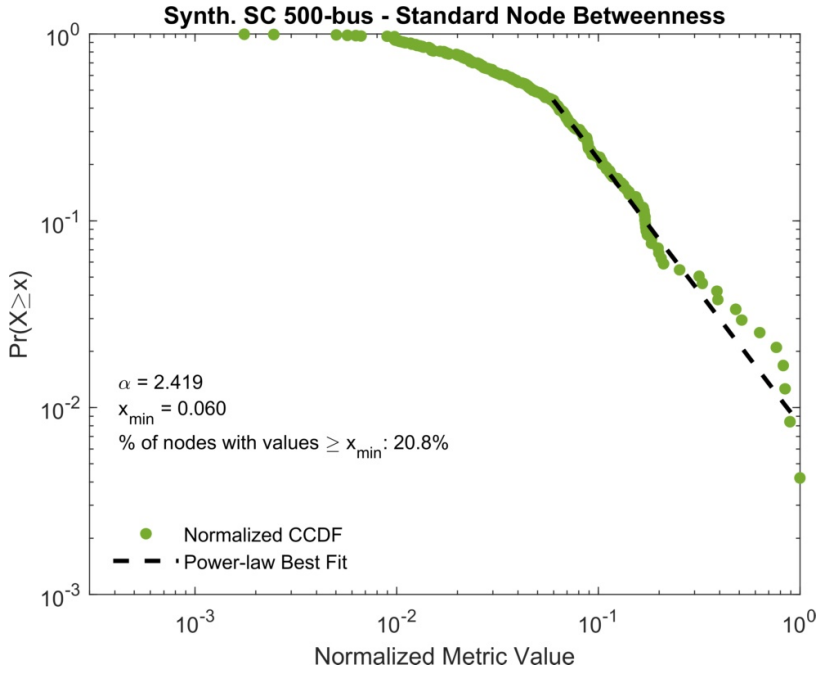


Figure 12 Synthetic South Carolina 500-bus Standard Betweenness Power-law Best Fit

Moving to extended network metrics, the electric betweenness power-law fits can be seen for the IEEE 300-bus case in Figure 13 and for the Synthetic Texas 2k-bus model in Figure 14. Across all fifteen qualifying CCDFs, the power-law best fits for these two CCDFs, with α values of 1.645 and 1.613, respectively, most closely matched the scaling parameter of blackout size distributions. While this does provide interesting insight and contributes to the broader trend seen with extended betweenness metrics, only two of the six networks exhibited CCDFs with potential power-law tail fits. This may indicate limited application of the metric as a tool for identifying critical system assets. Additionally, the power-law fit only applies for roughly 5% and 4% of nodes in the networks, which constitutes a diminishing portion of the network. At percentages this small, it is questionable whether the relationship is substantial enough relative to the entire CCDF to gain any insight into system behavior.

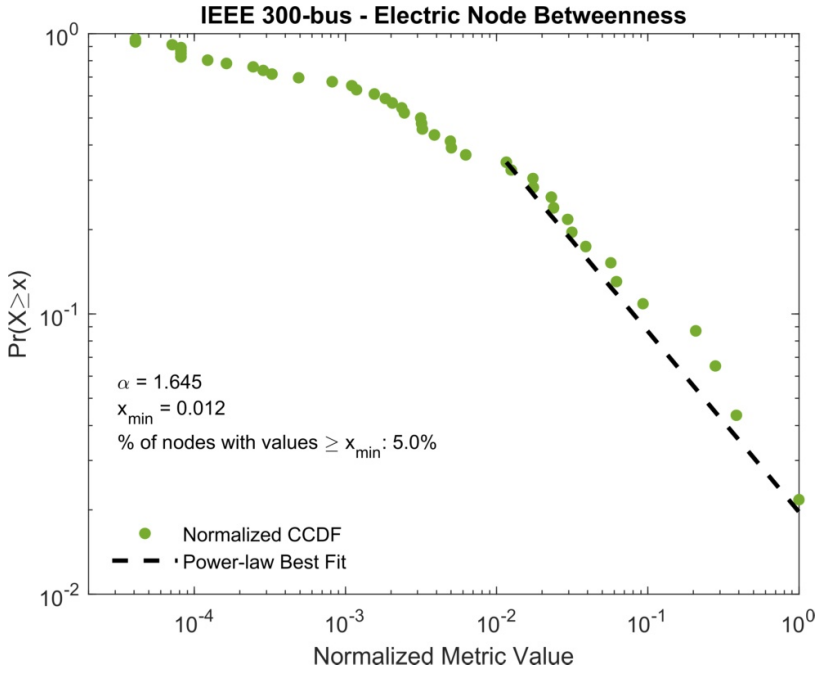


Figure 13 IEEE 300-bus Electric Betweenness Power-law Best Fit

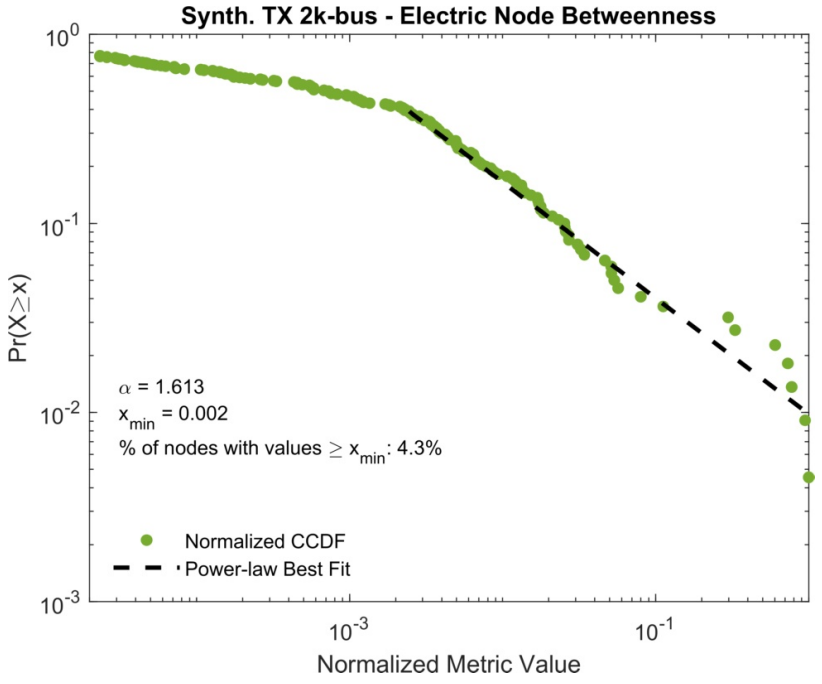


Figure 14 Synthetic Texas 2k-bus Electric Betweenness Power-law Best Fit

Continuing with structural metric power-law tails, the susceptance node degree centrality CCDFs and best fits can be seen in Figure 15 and Figure 16 for the IEEE case and the Synthetic US Northeast case, respectively. Due to the similar shape of the modified susceptance CCDFs, the IEEE and US Northeast cases also exhibited potential power-law fits for the modified metric and are displayed here in Figure 17Figure 17 and Figure 18. Upon close examination of the IEEE 300-bus distributions, the associated fits appear to be substantial, with 36.7% of buses fit with an α of 2.182 for the susceptance metric and with 36.7% of buses fit with an α of 2.180 for the modified version. This also represents the strongest fit across the extended degree centrality measures. In contrast, the US Northeast distributions were both fit with a scaling parameter value of 2.722 over 0.4% of the buses in the network, indicating a very narrow application of the fit. These weaker fits combined with the fact that the metric only identified a strong fit in one network indicates that a weak candidate for widespread application.

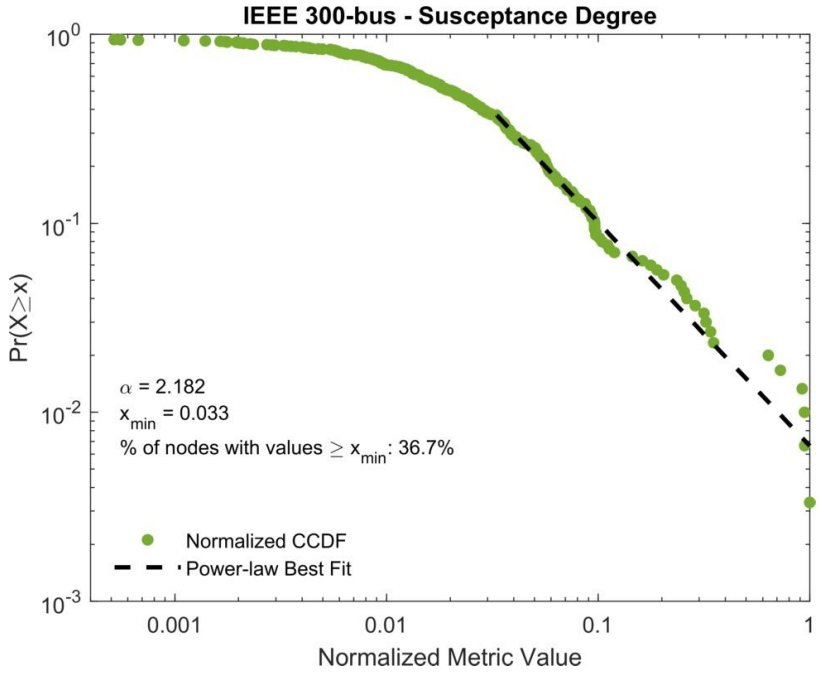


Figure 15 IEEE 300-bus Susceptance Degree Power-law Best Fit

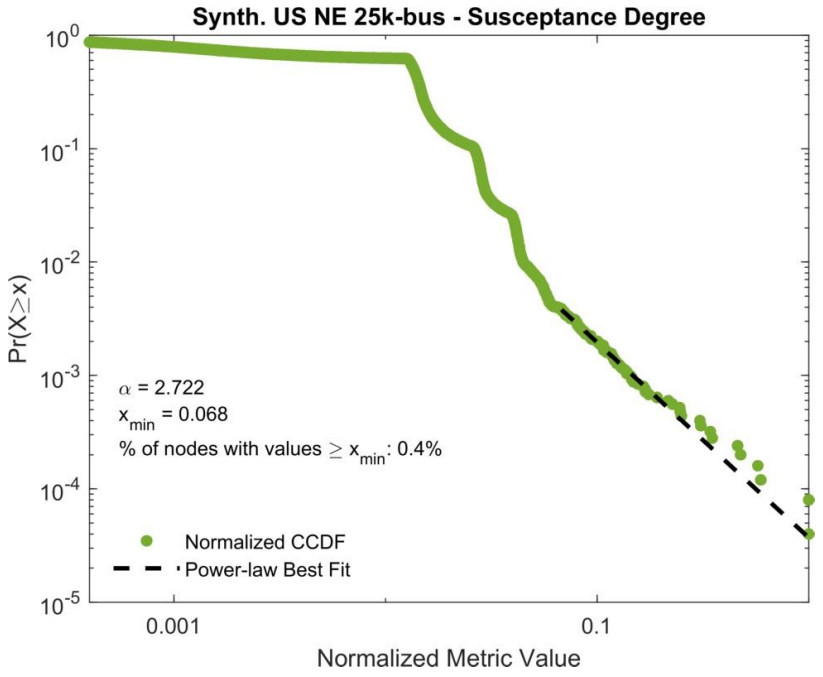


Figure 16 Synthetic US Northeast 25k-bus Susceptance Degree Power-law Best Fit

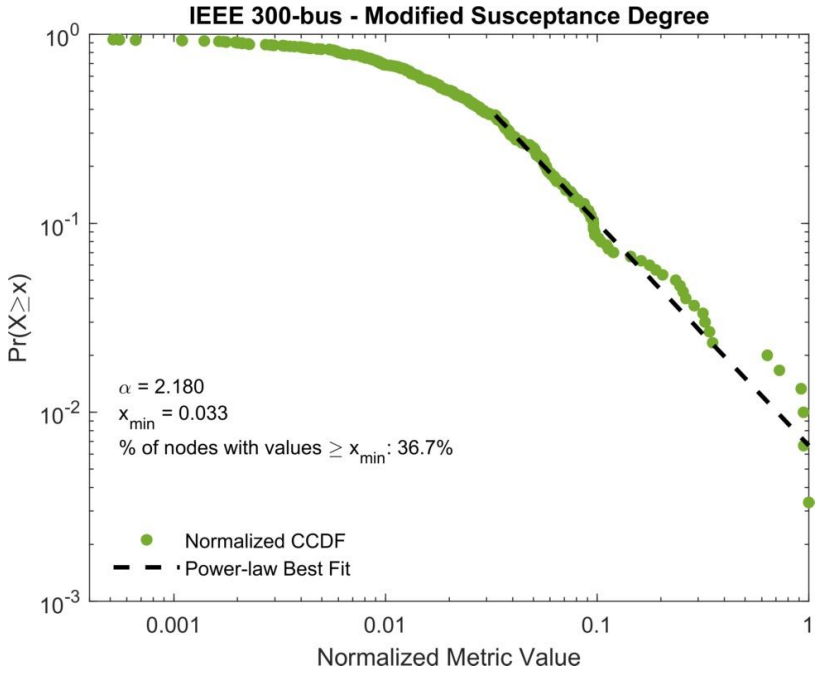


Figure 17 IEEE 300-bus Modified Susceptance Degree Power-law Best Fit

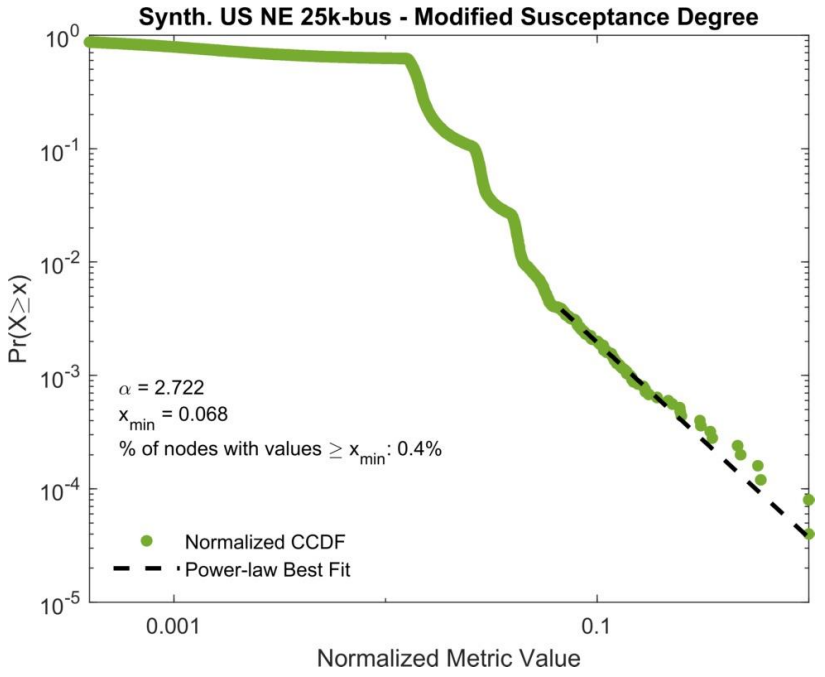


Figure 18 Synthetic US NE 25k-bus Modified Susceptance Degree Power-law Best Fit

Moving into system operational metrics, two power flow node betweenness CCDFs exhibited potential power-law distribution tails. The Synthetic South Carolina best fit can be found in Figure 19, along with the Synthetic WECC best fit in Figure 20. With α values of 1.727 and 2.458, respectively, both of these distributions show relatively heavy tails compared to blackout size distributions. Additionally, 13.2% and 10.0% of buses fall within the power-law region for each network, which yields more evidence in support of power flow node betweenness for identifying critical system assets. However, as with many of the other metrics in this study, only two networks of six exhibited potential for a power-law fit.

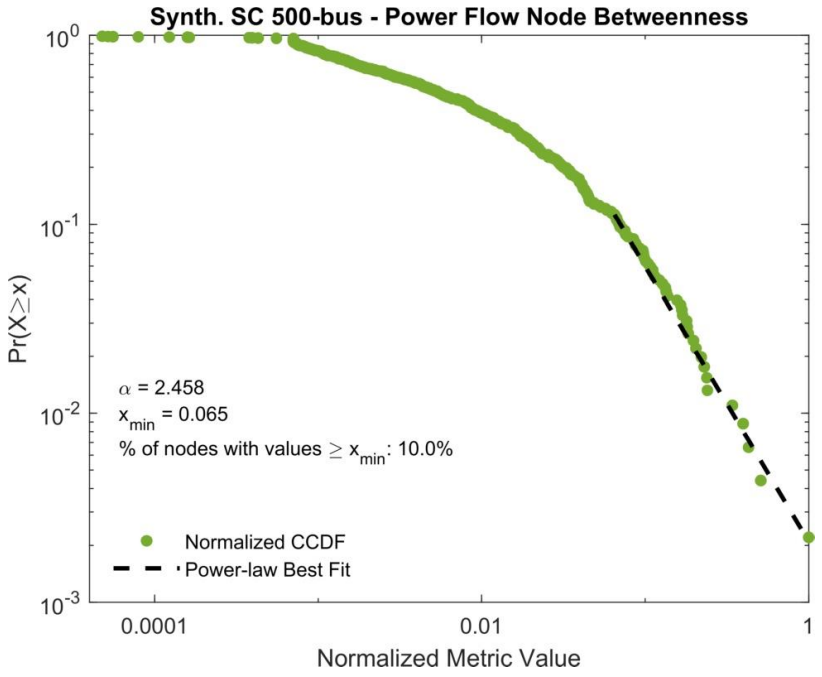


Figure 19 Synth. S.C. 500-bus Power Flow Node Betweenness Degree Power-law Best Fit

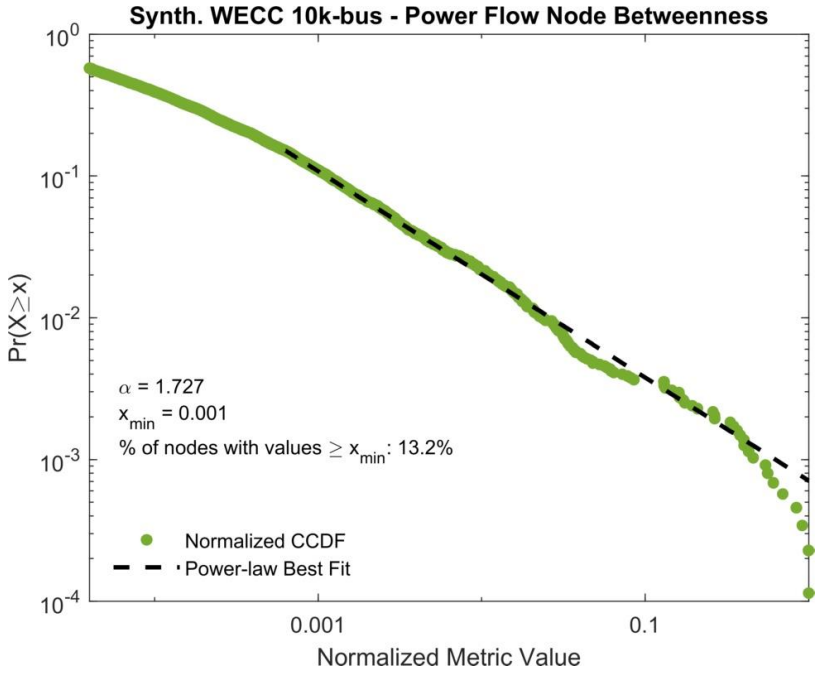


Figure 20 Synthetic WECC 10k-bus Power Flow Node Betweenness Power-law Best Fit

The last two remaining metrics, PF edge betweenness and SPL node degree, demonstrated a more consistent ability to identify power-law tail relationships across the six networks, with each identifying three. The PF edge betweenness metric best fits for the Synthetic South Carolina, Synthetic WECC, and Synthetic US Northeast can be seen in Figure 21, Figure 22, and Figure 23. Across the three CCDFs, the best power-law fits appear to be relatively consistent in terms of scaling parameter and percentage of buses described by the fit, with the exception being the scaling parameter for the Synthetic South Carolina case at 2.813 compared to 1.985 for the WECC case and 1.919 for the US Northeast case. Taken together, the PF edge betweenness metric exhibits some of the heaviest power-law fits observed in this analysis.

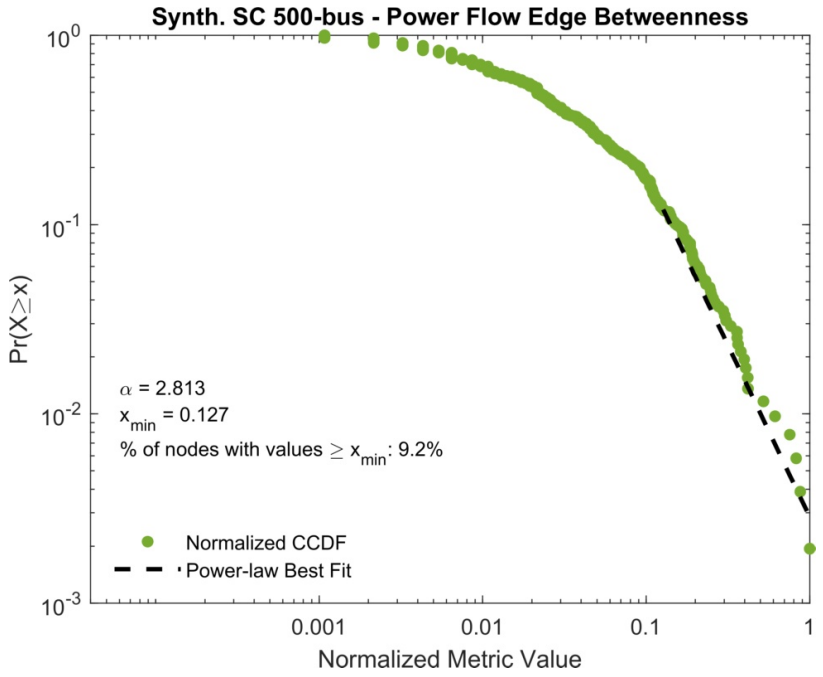


Figure 21 Synthetic S.C. 500-bus Power Flow Edge Betweenness Power-law Best Fit

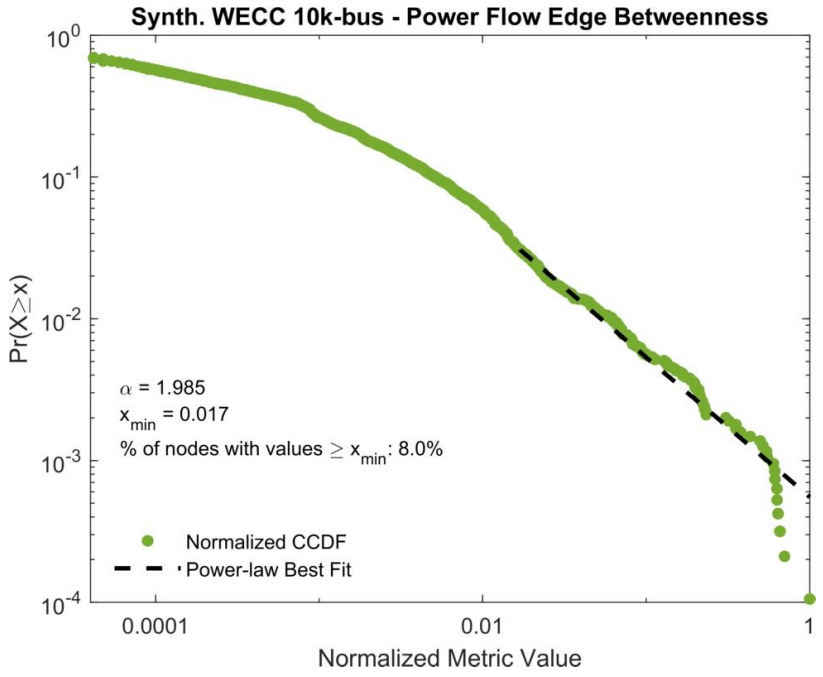


Figure 22 Synthetic WECC 10k-bus Power Flow Edge Betweenness Power-law Best Fit

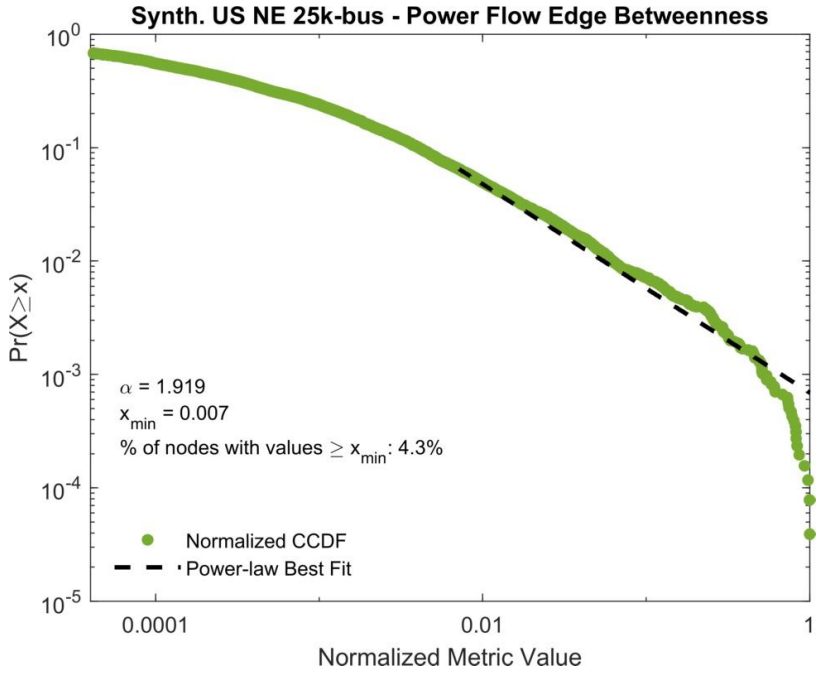


Figure 23 Synthetic US NE 25k-bus Power Flow Edge Betweenness Power-law Best Fit

The SPL metric best fits can be seen in Figure 24, Figure 25, and Figure 26 for the IEEE, South Carolina, and Texas cases. Of all the metrics tested, SPL degree proved to be most consistent when significant power-law tails were identified, though only about 10% of buses were described by the relationship for each network. Compared to other metrics, however, the α values were on the upper edge of passing, indicating a less heavy tail. Overall, these two metrics provide some of the more compelling frames of reference from which further investigation should be conducted.

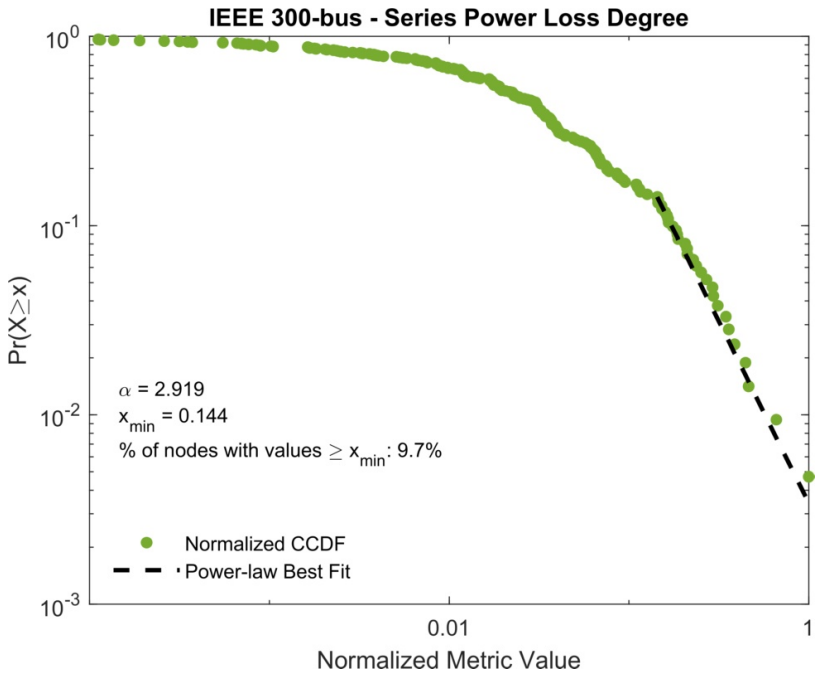


Figure 24 IEEE 300-bus Series Power Loss Degree Power-law Best Fit

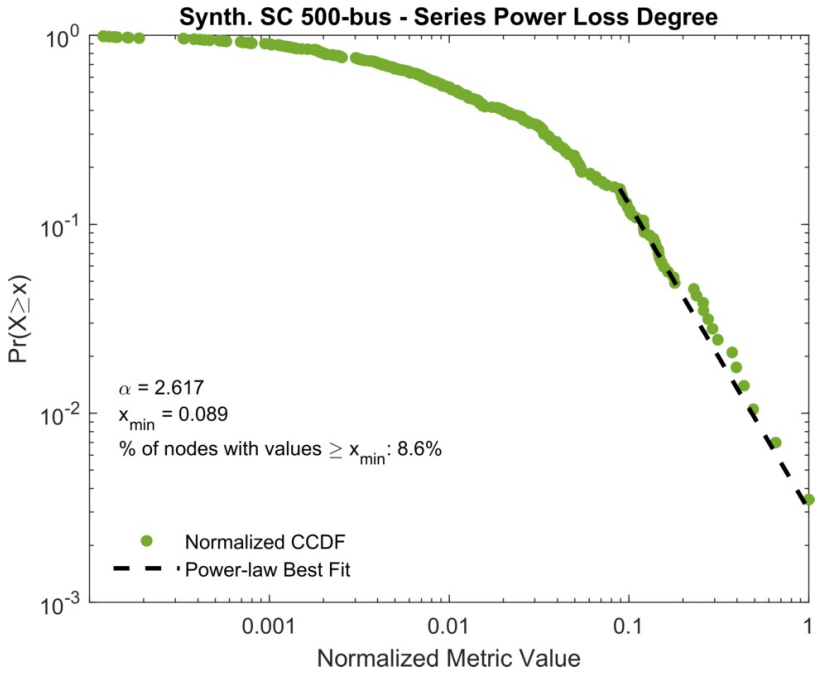


Figure 25 Synthetic S. Carolina 500-bus Series Power Loss Node Power-law Best Fit

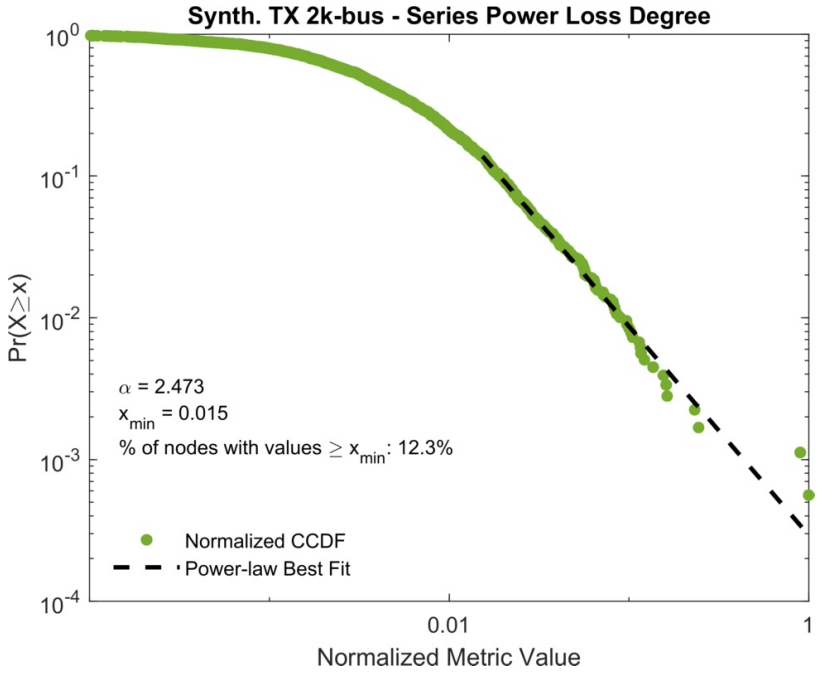


Figure 26 Synthetic Texas 2k-bus Series Power Loss Degree Power-law Best Fit

6.0 Discussion

6.1.1 General Trends in Network Theory Metrics

Overall, these results indicate a connecting thread between macro level power system behaviors and how they manifest in critical asset identification metrics. One of the critical challenges in identifying future metrics will be capturing those macro interactions in a sophisticated manner without necessitating overly complex calculations or data requirements. While the metrics tested are by no means exhaustive, this work does help narrow the scope and provide compelling evidence for further examination of system operation metrics generally, extended betweenness metrics specifically, and expansion into system outage metrics.

6.1.2 CCDF Heavy-Tail Results

Based off the heavy-tail test results, three conclusions can be drawn. First, extended betweenness metrics generally displayed the heaviest tails, suggesting the greatest potential connection to blackout mechanisms. Though only seven of the fifteen significant power-law relationships were extended betweenness metrics, the four with α less than 2 were extended betweenness metrics. These results indicate that macro interactions and relationships between components, rather than local phenomena captured by degree metrics, more closely track the observed distribution of blackout data. It is also worth noting that significant betweenness metric distributions were not consistent across networks but were consistent within networks. For the six networks tested, those that showed structural betweenness metric power-law tails did not also show

operational betweenness metric power-law tails, and vice versa. Further research into whether this extends to other structural and operational metrics should be pursued.

Another conclusion drawn from these results is that operational metrics, generally speaking, have a much better ability to consistently observe power-law tail relationships. With ten consequential relationships, five of which belonging to degree centrality metrics and five to betweenness metrics, the overall indication is that capturing power flow behaviors may yield substantive insight into power system outage patterns. This also partly falls in line with the first conclusion, suggesting further evidence that capturing how components interact in the larger system rather than in their immediate neighborhood is most important for identifying significant critical asset rankings.

And lastly, no single metrics was able to consistently produce a heavy-tailed valuation of system assets, suggesting instead that a slate of metrics is needed to meaningfully describe and diagnose power system behavior. Though SPL degree centrality consistently produced power-law tails for smaller networks and produced the most significant relationships, it showed no indication of doing so for larger networks. And in addition to this, none of the metrics tested showed a power-law tail for the French transmission grid model. While more metrics should be tested in this fashion, networks like the French grid may pose problems for conducting any kind of robust system analysis. However, based on the results from extended betweenness metrics and system operation metrics, further exploration of metrics like these or metrics that expand on their underlying principles could yield a more comprehensive set of testing metrics.

6.1.3 How Results Relate to Blackout Observations

As one of the primary goals of this research, trying to find possible connections between the distribution of blackout sizes and some electrical properties of power systems has proven to require a holistic approach and deeper understanding of network theory analysis. In this work, ten metrics were examined across six power systems of varying size and complexity. From this, it has already reaffirmed some prevailing notions about how to best understand blackout data.

First among these prevailing notions is the substantial impact that power system complexity has on applying network theory-based metrics and extracting meaningful results. As discussed in [34], metric rankings can be highly dependent on network structure, to the point that metrics capturing similar information about a network yield vastly different component rankings. This result can clearly be seen across each of the six networks, both when examining rankings across networks and examining significant power-law tail distributions. No single metric yielded consistent distributions across network size, nor did any single metric appear to consistently demonstrate a power-law tail in the CCDF. While this does not necessarily preclude these metrics from contributing to observations drawn from blackout data, it does confirm another prevailing notion that no single metric or method of analysis is sufficient to explain blackout size and frequency distributions.

In keeping with the complex nature of power systems and their structure and operation, a set of metrics would likely be needed to come to noteworthy conclusions on emergent power system behaviors. As can be seen from Section 5.3, with the associated caveats from this analysis, six of the ten metrics exhibited significant possibilities of power law tail behavior across multiple networks. This range of metrics portends a need for a more holistic methodology when implementing network theory criticality analysis, which could resemble a blood panel doctor's use

to diagnose the health of a patient. In keeping with this analogy, it appears most likely that the general un-wellness of a network is a confluence of different structural and operational vulnerabilities that manifest as significant blackout events. In order to more fully characterize network vulnerabilities, the types of metrics and the types of information they capture should be expanded from this work.

The final prevailing notion reaffirmed in this work is the need to expand the toolset of power system analysis. More pointedly, conventional load flow analysis and risk assessment methodologies are insufficient to understand deeper system vulnerabilities and creating more reliable and resilient electric power systems. As evidenced by this work, which employed metrics encompassing traditional power system structural and operational characteristics, there appears to be an opportunity to expand this type of work beyond traditional power system properties. As power system structure evolves with higher penetration of distributed generation resources and senor technologies, renewable generation sources, and electric vehicles and other energy storage systems, the way these systems are analyzed will also need to expand in order to better understand emergent behaviors.

As a final note, though this work has served to reaffirm some notions about the broader context that it fits in, it has also exhibited the value that can come from conducting significant analysis on ECNs. While this work is not all-inclusive, seeing as dozens of ECN metrics exist in the literature, there is promise in using extended betweenness metrics and system operation metrics. Further expanding on these types of metrics can lead to a substantive and actionable method of identifying specific critical system assets in a wide array of networks. This research has laid out a process to begin that identification process.

7.0 Future Work

There are multiple avenues for expansion of this research. Namely, the inclusion of system outage metrics would provide a good opportunity to capture less apparent technical aspects of power systems. As discussed in Section 4.1.2.2, system outage metrics utilize information about interactions between system components and how failures impact system operation. While significantly more complex and computationally intensive than analyzing system structure or operation exclusively, system outage metrics are more intimately associated with the phenomenon that result in large-scale blackouts. Performing heavy-tail tests and correlation analysis could provide insight into how outage patterns, responses, and locations track with established trends and fit into a broader holistic analysis of power systems.

Another opportunity to expand would be through the addition of actual system data. Though many of the metrics discussed have been tested using data from FERC or other regulatory bodies, no overall analysis has been conducted with access to power system structural data or blackout data. In many cases, these metrics are only scrutinized using relatively small test networks, such as the IEEE 30-bus model or the IEEE 300-bus model. While this provides a consistent and reproducible model from which initial testing can be conducted, this can be limiting in terms of application beyond hypothetical models. Incorporating this data would provide a method of validating results and giving additional weight to conclusions drawn from the ECN analysis, heavy-tail testing, and correlation analysis.

A final avenue to improve upon this work would be the integration of interconnected infrastructure analysis. Because critical infrastructures often rely on other systems to operate (e.g. water infrastructure relying on electric pumps, or electric generators relying on a steady supply of

natural gas), fully diagnosing system vulnerabilities likely requires a sophisticated understanding of how different systems interact. Though this would require depth of knowledge in a variety of different sectors and could potentially be overly abstract or computationally costly, further investigating these relationships can provide a more expansive view of what assets are deemed critical. Several attempts with varying degrees of complexity have been made to account for and model interconnected behaviors involving electric power transmission [40]-[43]. Across all of these models, the tradeoff between model complexity and useful simulation results appears repeatedly as one of the biggest challenges. That being said, this holistic approach could be thoughtfully developed to inform a comprehensive disaster response strategy, detecting interrelated failures and bringing critical infrastructure back online faster.

8.0 Conclusion

As times goes on, the modern world is increasingly more reliant on electric power systems, with potential for ruinous impacts on quality of life should these systems become unavailable. Without significant measures being taken to address large-scale blackouts, industries and businesses grind to a halt and the lives of individuals are adversely affected. While many approaches are being developed to handle these events, network theory methods provide a familiar analysis that can prove vital in minimizing the risk associated with large-scale blackouts.

By being able to categorize metrics that track blackout behaviors and the associated vulnerable infrastructure, system planners can get ahead of outages, harden infrastructure, and craft mindful strategies for more robust and resilient power systems. But that process comes with a need for deep understanding of system architecture and the role that critical asset identification metrics can play in system preparedness. While network complexity can affect analysis, continued testing of systems and their structure, operation, and failure patterns will be indispensable in the pursuit of modernizing power grids to meet the rising expectations associated with them.

The research presented here offers the initial steps to identifying system vulnerabilities in a consistent and reproducible manner. Though more metrics and networks can, and should, always be tested, the results discussed should narrow the scope of future analysis and provide a framework for analyzing system features responsible for the size and frequency of large-scale blackouts. Using heavy-tail testing to scrutinize metrics and relationships between useful metrics has shown promise as a useful filter. By continuing along these lines, a collection of pointed metrics can provide useful information on power system vulnerabilities and assist in building more reliable and resilient electric power infrastructure.

Bibliography

[1] G. Andersson et al, “Causes of the 2003 Major Grid Blackouts in North America and Europe, and recommended Means to Improve System Dynamic Performance,” *IEEE Trans. on Power Systems*, vol. 20, no. 4, Nov. 2005. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed Oct. 29, 2019].

[2] U.S.-Canada Power System Outage Task Force, “Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations,” Washington, DC, 2004. [Online]. Available: www.epa.gov. [Accessed Oct. 23, 2019].

[3] Union for the Coordination of Transmission of Electricity, “Final Report of the Investigation Committee on the 28 September 2003 Blackout in Italy,” Paris, France, 2004. [Online]. Available: http://www.rae.gr/old/cases/C13/italy/UCTE_rept.pdf. [Accessed Oct. 23, 2019].

[4] Federal Energy Regulatory Commission, Order Certifying North American Electric Reliability Corporation as the Electric Reliability Organization and Ordering Compliance Filing. Washington, DC: FERC Headquarters, July 20, 2006. [Online]. Available: http://www.nerc.com/. [Accessed Oct. 29, 2019].

[5] O. P. Veloza and F. Santamaria, “Analysis of major blackouts from 2003 to 2015: Classification of incidents and review of main causes,” *The Electricity Journal*, vol. 29, no. 7, pp. 42-49, Sept. 2016. [Online]. Available: http://www.sciencedirect.com/. [Accessed Oct. 29, 2019].

[6] G. F. Reed, “Expect more blackouts unless we invest in our energy grid,” *The Hill*, Aug. 10, 2019. [Online], Available: www.thehill.com. [Accessed Oct. 23, 2019].

[7] J. Barron and M. Zaveri, “Power Restored to Manhattan’s West Side After Major Blackout,” *The New York Times*, July 13, 2019. [Online], Available: www.nytimes.com. [Accessed Oct. 23, 2019].

[8] B. A. Carreras, D. E. Newman and I. Dobson, "North American Blackout Time Series Statistics and Implications for Blackout Risk," *IEEE Trans. Power Systems*, vol. 31, no. 6, pp. 4406-4414, Nov. 2016. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed Oct. 29, 2019].

[9] P. Hines, J. Apt, and S. Talukdar, “Large blackouts in North America: Historical trends and policy implications,” *Energy Policy*, vol. 37, no. 12, pp. 5249-5259, Dec. 2009. [Online]. Available: http://www.sciencedirect.com/. [Accessed Oct. 29, 2019].

[10] B. A. Carreras, V. E. Lynch, I. Dobson, and D. E. Newman, “Critical points and transitions in an electric power transmission model for cascading failure blackouts,” *Chaos*, vol. 12,

no. 4, pp. 985-994, Dec. 2002. [Online]. Available: https://aip.scitation.org/. [Accessed Oct. 29, 2019].

[11] M. Rahnamay-Naeini and M. M. Hayat, "Impacts of operating characteristics on sensitivity of power grids to cascading failures," in *2016 IEEE Power and Energy Society Gen. Meeting*, July 17-21, 2016, Boston, MA, USA [Online]. Available: https://ieeexplore.ieee.org/. [Accessed Oct. 29, 2019].

[12] G. B. Anderson and M. L. Bell, "Lights out: Impact of the August 2003 power outage on mortality in New York, NY," *Epidemiology*, vol. 23, no. 2, March 2012. [Online]. Available: NCBI https://www.ncbi.nlm.nih.gov/pmc/. [Accessed Oct. 14, 2019].

[13] S. Lin, B. A. Fletcher, M. Luo, R. Chinery, and S. Hwang, "Health Impact in New York City during the Northeastern Blackout of 2003," *Public Health Reports*, vol. 126, no. 3, pp. 384-393, May 2011. [Online]. Available: http://journals.sagepub.com/. [Accessed Oct. 29, 2019].

[14] C. Dominianni, K. Lane, S. Johnson, K. Ito, and T. Matte, "Health Impacts of Citywide and Localized Power Outages in New York City," *Environmental Health Perspectives*, vol. 126, no. 6, June 2018. [Online]. Available: https://ehp.niehs.nih.gov/. [Accessed Oct. 29, 2019].

[15] R. Albert, I. Albert, and G. L. Nakarado, "Structural vulnerability of the North American power grid," *Phys. Rev. E*, vol. 69, no. 2, pp. 1-4, Feb. 2004. [Online]. Available: https://journals.asp.org/. [Accessed Oct. 31, 2019].

[16] M. Ouyang, "Review on modeling and simulation of interdependent critical infrastructure systems," *Reliability Engineering & System Safety*, vol. 121, pp 43-60, Jan. 2014. [Online]. Available: http://www.sciencedirect.com/. [Accessed Oct. 29, 2019].

[17] P. Chopade and M. Bikdash, "New centrality measures for assessing smart grid vulnerabilities and predicting brownouts and blackouts," *Int. Journal of Critical Infrastructure Prot.*, vol. 12, pp. 29-45, March 2016. [Online]. Available: http://www.sciencedirect.com/. [Accessed Oct. 29, 2019].

[18] G. A. Pagani and M. Aiello, "The Power Grid as a complex network: A survey," *Phys. A: Statistical Mechanics and its Applications*, vol. 392, no. 11, pp. 2688-2700, June 1, 2013. [Online]. Available: http://www.sciencedirect.com/. [Accessed Oct. 29, 2019].

[19] A. Abedi, L. Gaudard, and F. Romerio, "Review of major approaches to analyze vulnerability in power system," *Reliability Eng. & System Safety*, vol. 183, pp. 153-172, March 2019. [Online]. Available: http://www.sciencedirect.com/. [Accessed Oct. 29, 2019].

[20] H. Guo, C. Zheng, H. H. 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, Dec. 2017. [Online]. Available: http://www.sciencedirect.com/. [Accessed Oct. 29, 2019].

[21] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-Fernández, and Z. W. Geem, "A Critical Review of Robustness in Power Grids Using Complex Network Concepts," *Energies*, vol. 8, no. 9, pp. 9211-65, Aug. 2015. [Online]. Available: http://www.mdpi.com/. [Accessed Oct. 31, 2019].

[22] A. S. Bhave, M. L. Crow, and E. K. Çetinkaya, "Robustness of Power Grid Topologies Against Centrality-Based Attacks," in *2016 Resilience Week*, Chicago, IL, USA. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed Nov. 1, 2019].

[23] P. Crucitti, V. Latora, and M. Marchiori, "Locating Critical Lines in High-Voltage Electrical Power Grids," *Fluctuation and Noise Letters*, vol. 5, no. 2, pp. L201-L208, 2005. [Online] Available: http://www.worldscientific.com/. [Accessed Nov. 1, 2019].

[24] E. Bompard, D. Wu, and F. Xue, "Structural vulnerability of power systems: A topological approach," *Electric Power Systems Research*, vol. 81, no. 7, pp. 1334-40, July 2011. [Online]. Available: http://www.sciencedirect.com/. [Accessed Nov. 1, 2019].

[25] P. Hines, S. Blumsack, E. Cotilla Sanchez, and C. Barrows, "The Topological and Electrical Structure of Power Grids," in *2010 43rd Hawaii Int. Conf. on Systems Science*, Honolulu, HI, USA. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed Nov. 1, 2019].

[26] E. Cotilla-Sanchez, P. Hines, C. Barrows, and S. Blumsack, "Comparing the Topological and Electrical Structure of the North American Electric Power Infrastructure," *IEEE Systems Journal*, vol. 6, no. 4, pp. 616-626, Dec. 2012. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed Nov. 1, 2019].

[27] M. Ouyang, Z. Pan, L. Hong, and L. Zhao, "Correlation analysis of different vulnerability metrics on power grids," *Physica A: Statistical Mechanics and its Applications*, vol. 396, pp. 204-211, Feb. 15, 2014. [Online]. Available: http://www.sciencedirect.com/. [Accessed Nov. 1, 2019].

[28] P. Hines, E. Cotilla-Sanchez, and S. Blumsack, "Do topological models provide good information about electricity infrastructure vulnerability," *Chaos*, vol. 20, no. 3, Aug. 2010. [Online]. Available: https://aip.scitation.org/. [Accessed Nov. 1, 2019].

[29] P. Hines, I. Dobson, and P. Rezaei, "Cascading Power Outages Propagate Locally in an Influence Graph That is Not the Actual Grid Topology," *IEEE Trans. Power Systems*, vol. 32, no. 2, pp. 958-967, March 2017. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed Nov. 1, 2019].

[30] P. Hines and S. Blumsack, "A Centrality Measure for Electrical Networks," in *Proc. 41st Ann. Hawaii Int. Conf. on System Sciences*, Jan. 2008, Waikoloa, HI, USA. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed Nov. 1, 2019].

[31] U. Nakarmi and M. Rahnamay-Naeini, "Analyzing Power Grids' Cascading Failures and Critical Components using Interaction Graphs," in *2018 IEEE Power & Energy Society*

Gen. Meeting, Portland, OR, USA. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed Nov. 1, 2019].

[32] R. Ghanbari, M. Jalili, and X. Yu, "Correlation of cascade failures and centrality measures in complex networks," *Future Generation Computer Systems*, vol. 83, pp. 390-400, June 2018. [Online]. Available: http://www.sciencedirect.com/. [Accessed Nov. 1, 2019].

[33] T. A. Ernster and A. K. Srivastava, "Power System Vulnerability Analysis – Towards Validation of Centrality Measures," in *PES T&D 2012*, Orlando, FL, USA. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed Nov. 1, 2019].

[34] D. Schoch, T. Valente, and U. Brandes, "Correlations among centrality indices and a class of uniquely ranked graphs," *Social Networks*, vol. 50, pp. 46-54, July 2017. [Online]. Available: http://www.sciencedirect.com/. [Accessed Nov. 1, 2019].

[35] N. Meghanathan, "Correlation Coefficient Analysis of Centrality Metrics for Complex Network Graphs," in *Computer Science On-line Conf.*, 2015. [Online]. Available: http://link.springer.com/. [Accessed Nov. 1, 2019].

[36] A. B. Birchfield, T. Xu, K. M. Gegner, K. S. Shetye, and T. J. Overbye, "Grid Structural Characteristics as Validation Criteria for Synthetic Networks," in *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3258-3265, July 2017. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed March 12, 2020].

[37] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: Steady-State Operations, Planning and Analysis Tools for Power Systems Research and Education," *Power Systems, IEEE Transactions on*, vol. 26, no. 1, pp. 12–19, Feb. 2011. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed March 12, 2020].

[38] E. P. R. Coelho, J. C. Thomazelli, M. H. M. Paiva and M. E. V. Segatto, "A complex network analysis of the Brazilian Power Test System," *2015 IEEE PES Innovative Smart Grid Technologies Latin America (ISGT LATAM)*, Montevideo, 2015, pp. 113-118. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed March 12, 2020].

[39] A. Clauset, C. R. Shalizi, and M. E. J. Newman, "Power-Law Distributions in Empirical Data," *SIAM Review*, vol. 51, no. 4, pp. 661-703, 2009. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed March 12, 2020].

[40] S. Breor, "Assessing Critical Infrastructure Dependencies and Interdependencies," in *2018 Winter Simulation Conf.*, Gothenburg, Sweden. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed Oct. 29, 2019].

[41] K. Grolinger, M. A. M. Capretz, A. Shypanski, and G. S. Gill, "Federated Critical Infrastructure Simulators: Towards Ontologies for Support of Collaboration," in *2011 24th Canadian Conf. on Electrical and Computer Eng.*, Niagara Falls, ON, Canada. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed Oct. 29, 2019].

[42] P. Capodieci et al, “Improving Resilience of Interdependent Critical Infrastructures via an On-line Alerting System,” in *2010 Complexity in Eng.*, Rome, Italy. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed Oct. 29, 2019].

[43] S. M. Rinaldi, “Modeling and Simulating Critical Infrastructures and Their Interdependencies,” in *Proc. Ann. Hawaii Int. Conf. on System Sciences*, Big Island, HI, USA, Jan. 2004. [Online]. Available: https://ieeexplore.ieee.org/. [Accessed Oct. 29, 2019].