Topological Models and Critical Slowing Down: Two Approaches to Power System Blackout Risk Analysis

Paul Hines  
U. of Vermont  
paul.hines@uvm.edu

Eduardo Cotilla-Sanchez  
U. of Vermont  
jcotilla@uvm.edu

Seth Blumsack  
Pennsylvania State U.  
blumsack@psu.edu

Abstract

This paper describes results from the analysis of two approaches to blackout risk analysis in electric power systems. In the first analysis, we compare two topological (graph-theoretic) methods for finding vulnerable locations in a power grid, to a simple model of cascading outage. This comparison indicates that topological models can lead to misleading conclusions about vulnerability. In the second analysis, we describe preliminary results indicating that both a simple dynamic power system model and frequency data from the August 10, 1996 disturbance in North America show evidence of critical slowing down as the system approaches a failure point. In both examples, autocorrelation in the time-domain signals (frequency and phase angle), significantly increases before reaching the critical point. These results indicate that critical slowing down could be a useful indicator of increased blackout risk.

I. Introduction

Reliable electricity infrastructures are vital to modern societies, but are notably susceptible to large, cascading failures. The disturbances of, for example, 14 August 2003 in North America [1], 4 November 2006 in Europe[2] and 10 November 2009 in South America [3] emphasize the continued risk associated with large cascading outages. Given that large blackouts contribute disproportionately to overall blackout risk [4], [5], and that natural and human exogenous forces will occasionally result in component failures, there is a continuing need for new approaches to the identification of risks in power grids. In this paper we investigate methods for identifying two types of risks: (1) risks associated with components of the power grid that are disproportionately vulnerable to volitional attacks and random failures, and (2) risks associated with operating states that are proximate to points of dynamic instability.

Identifying components that are vulnerable to failure and attack may be useful for prioritizing among risk mitigation investments, such as adding walls around critical components. However it is important that the methods used to identify vulnerabilities are accurate. The use of inappropriate methods could result in the misallocation of scarce resources.

Identifying high-risk operating states may help operators to make better decisions about when or if to implement emergency control policies, such as load shedding or rapid generator set point adjustments. With the growing deployment of synchronized phasor measurement units (PMUs or synchrophasors) operators have increasing access to massive quantities of high-resolution, time-synchronized data. Algorithms that can turn these data into information about operating risk could dramatically increase the value of synchrophasor technology.

With this in mind, this paper describes two approaches to the risk identification problem. Section 2 describes an analysis of topological approaches to vulnerability analysis, stemming from the field of complex network analysis. Section 3 describes a method of using high-resolution time-domain data, such as that which comes from synchronized phasor measurement units, to identify operating points that show evidence of “critical slowing down.”
II. Topological approaches to identifying vulnerable components

Several recent papers have applied complex networks methods [6], [7] to study the structure and function of power grids. Results from these studies differ greatly. Some measure the topology of power grids and report exponential degree distributions [8], [9], [10], whereas others report power-law distributions [11], [12]. Some models of the North American power grid suggest that power grids are more vulnerable to directed attacks than to random failures [9], [13], even though power grids differ from from scale-free networks in topology. Recently, Wang and Rong [14] used a topological model of cascading failure and argue that attacks on nodes (buses) transporting smaller amounts of power can result in disproportionately large failures. Albert et al. [9] draw the opposite conclusion using similar data. In [15], Buldyrev et al. study a topological model of interconnected communications and electricity infrastructure networks and draw broad conclusions about infrastructure vulnerability. Because of the vital importance of infrastructure security to modern society, and heightened concerns about attacks on energy infrastructure, these papers [9], [14] have attracted the attention of government and media (see, e.g., [16]).

The value of purely topological models of power grid failure in assessing actual failure modes in the electricity infrastructure is not well-established. Commodity (electric energy) flows in electricity networks are governed by Ohm's law and Kirchhoff’s laws (among others), which are not captured particularly well in simple topological models (see Fig.1). Some have identified relationships between the physical properties of power grids and topological metrics [17], [18], [10], and find that some metrics do correlate to some measures of power system performance. However, to our knowledge, no existing research has systematically compared the results from a power-flow based cascading failure vulnerability model with those from graph theoretic models of vulnerability. Because cascading failures (and hurricanes) cause the largest blackouts [5] and contribute disproportionately to overall reliability risk [19], models that incorporate the possibility of cascading failure are necessary to provide a sufficiently broad view of power network vulnerability. While there is extensive literature on cascading failure and contagion in abstract networks (see, e.g., Sec. 4 of [7]), and some application of these methods to power networks [20], direct comparisons are needed to draw firm conclusions about the utility of topological methods.

Our primary goal, therefore, is to compare the vulnerability conclusions that result from topological measures of network vulnerability with those that result from a more realistic model of power network failure. Specifically we compare the conclusions that result from two topological measures used to estimate the impact of random failure and directed attacks, and compare these with a simple model of cascading outages in power grids. Note that portions of the material in this section are in press as [21].

A. Vulnerability measures

Our first vulnerability measure is characteristic path length \(0 < L < \infty\), which is the average distance among node pairs in a graph. In [22], path length (network diameter) was suggested as a measure of network vulnerability because as more components in a network fail, nodes\(^1\) in the system become more distant, which may indicate that flows within the network are inhibited.

\(^1\)In this paper we use the terms “node” and “bus” synonymously, while acknowledging that in some power system cases the two have distinct meanings. In this paper “node” means a bus in a power system.
The second measure is connectivity loss ($0 < C < 1$), which was proposed in [9] as a way to incorporate the locations of sources (generators) and sinks (loads) into a measure of network vulnerability. Connectivity loss is defined: $C = 1 - \langle n'_{g}/n_{g} \rangle$, where $n_{g}$ is the number of generators in the network and $n'_{g}$ is the number of generators that can be reached by traveling from node $i$ across non-failed links.

The third measure, which does not appear in the existing network science literature, is blackout sizes as calculated from a model of cascading failure in a power system. While a perfect model of cascading failure would accurately represent the continuous dynamics of rotating machines, the discrete dynamics associated with relays that disconnect stressed components from the network, the non-linear algebraic equations that govern flows in the network, and the social dynamics of operators working to mitigate the effects of system stress, all power system models simplify these dynamics to some extent. Unlike simple topological metrics, our model does capture the effects of Ohm’s and Kirchhoff’s laws, by using linear approximations of the non-linear power flow equations [23]. Similar models have been used to study cascading failure in a number of recent papers [4], [19], [24].

In our model, when a component fails, the “DC power-flow” equations are used to calculate changes in network flow patterns. In the DC approximation the net power injected into a node (generation minus load: $P_{n} = P_{g,i} - P_{d,i}$) is equal to the total amount of power flowing to neighboring nodes through links (transmission lines or transformers): $P_{n} = \sum_{j} (\theta_{i} - \theta_{j})/X_{ij}$, where $\theta_{i}$ is the voltage phase angle at node $i$, and $X_{ij}$ is the series reactance of the link(s) between nodes $i$ and $j$. Each link has a relay that removes it from service if its current exceeds 50% of its rated limit for 5 seconds or more. The trip-time calculations are weighted such that the relays will trip faster given greater overloads. While it is true that over-current relays are not universally deployed in high-voltage power systems, they provide a good approximation of other failure mechanisms that are common, such as lines sagging into underlying vegetation (an important contributor to the August 14, 2003 North American blackout [1]). After a component fails the model recalculates the power flow and advances to the time at which the next component will fail, or quits if no further components are overloaded. If a component failure separates the grid into unconnected sub-grids, the following process is used to re-balance supply and demand. If the imbalance is small, such that generators can adjust their output by not more than 10% and arrive at a new supply/demand balance, this balance is achieved through generator set-point adjustments. If this adjustment is insufficient, the smallest generator in the sub-grid is shut down until there is an excess of load. If there is excess load after these generator adjustments, the simulator curtails enough load to balance supply and demand. This balancing process approximates the process that automatic controls and operators follow to balance supply and demand during extreme events. The size of the blackout $(S)$ is reported at the end of the simulation as the total amount of load curtailed.

**B. Attack vectors**

In order to measure power network vulnerability, we test the response of 41 electricity networks to a variety of exogenous disturbance vectors (attacks or random failures). In each case we measure the relationship between disturbance (attack or random failure) size and disturbance cost using the three vulnerability measures described above. To compare our results with prior research five disturbance vectors are simulated. These are described as follows.

The first vector is random failure, in which nodes (buses) are selected for removal by random selection, with an equal failure probability for each node. This approach simulates failure resulting from natural causes (e.g., storms) or an unintelligent attack. For each network, we test its response to 20 unique sets of random failures, with 10 nodes in each set. These sets are initially selected from a uniform distribution, and then applied incrementally (one node, then two nodes, etc.).

The second vector is degree attack, in which nodes are removed incrementally, starting with the highest degree (connectivity) nodes. This strategy represents an intelligent attack, in which the attacker chooses to disable nodes with a large number of neighboring nodes.

The third vector is a maximum-traffic attack, in which nodes are removed incrementally, starting with those that transport the highest amounts of power. We use the term “traffic” to differentiate this measure from “load,” which frequently describes the quantity of power being consumed at a node. Thus traffic $(T)$ is similar to the measures described as load in [9], [14]. The following measure of node-loading is used to select maximum-traffic nodes: $T_{i} = |P_{n}| + \sum_{j} |(\theta_{i} - \theta_{j})/X_{ij}|$.

The fourth vector is minimum-traffic attack, which is the inverse of the max-traffic attack. This vector is used for comparison with the conclusions in [14], which argues that failures at low-traffic (load) nodes lead to larger blackouts than failures at high-traffic nodes.

The fifth vector is betweenness attack, in which
nodes are removed incrementally, starting with those that have the highest betweenness centrality (the number of shortest paths that pass through a node [7]). This vector was used in [9] to approximate an attack on high traffic (load) nodes, and was reported to result in disproportionately large failures.

C. Results

To compare the vulnerability measures we report results from the simulation of random failures and directed attacks for a common test system (IEEE 300 bus test case) and 40 of 136 control areas from within the North American Eastern Interconnect (EI). The EI data come from a North American Electric Reliability Corporation power-flow planning case, to which the authors have been granted access for the purpose of this research. The 40 control areas analyzed were selected because of their proximate sizes (336-1473 nodes). Together they represent 29,261 of 49,907 nodes (buses) in the Eastern Interconnect data. We initialized the simulations to provide an initial balance between supply and demand by decreasing either load or generation, whichever was initially greater. In a few areas the base-case power flows exceeded the rated flow limits. In these cases we increased the line limits until all power flows were 10% below the flow limits. Actual locations have been deleted from our data set, such that these results are not linked to physical locations in the US electricity infrastructure.

The upper panels of Figs. 2 and 3 show how path lengths ($L$) change as nodes are removed from the test networks. In both the IEEE 300 bus network and the EI areas path lengths resulting from degree-based, max-traffic, and betweenness attacks is greater than the average $L$ from random failures. Min-traffic attacks do not substantially differ from random failures in this measure.

The middle panels of Figs. 2 and 3 illustrate the difference between the connectivity losses ($C$) from directed attacks and $C$ from random failure. From this semi-topological perspective, power grids are notably more vulnerable to directed attacks than to random failure, and are thus similar to scale-free networks (see [9] for a similar result).

The blackout size results (lower panels of Figs. 2 and 3) also indicate that power networks are notably more vulnerable to directed (degree-based, max-traffic-and betweenness-based) attack than they are to random failure. Max-traffic attacks on 10 nodes produce blackouts with an average size of 72%. Random failure of 10 nodes results in an average blackout size of 20%, and min-traffic attacks produced much smaller blackouts (5% average). From these results it appears that the prediction in [14] that attacks on low-traffic nodes lead to large failures is not accurate. Note that the measure of traffic (load) used [14] is different than ours, but it would be incorrect to conclude that failures at low power-flow nodes contribute substantially to system vulnerability.

While trends in the path length, connectivity loss and blackout size measures are similar after averaging over many simulations, the correlation between measures for individual simulations is poor. Because connectivity loss does not directly account for cascading failure, it roughly predicts only the minimum size of the resulting blackout (see Fig. 4). Once triggered, the complex interactions among network components during a cascading event can result in a blackout of almost any size. Many disturbances with small connectivity loss ($<$10%) produced very large blackouts.

Another notable difference among the model results is that one would draw different conclusions about the most dangerous attack vectors, depending on the vulnerability measure used. From path lengths, betweenness attacks have the greatest impact. From connectivity loss, degree-based attacks look most dangerous. From the blackout model, max-traffic attacks appear to contribute most to vulnerability.

D. Implications of topological analysis results

Together these results indicate that while topological measures can provide some indication of general vulnerability trends, they can also be misleading when used in isolation. In some cases, overly-abstracted topological models can result in erroneous conclusions, which could lead to mis-allocation of scarce risk-mitigation resources. Vulnerability measures that properly account for network behavior as well as the arrangement of sources and sinks produce substantially different results; we argue that these results are more realistic and more useful for infrastructure risk assessment. If the results described here are similar to what one would obtain from an ideal model of cascading failure, the implication for electricity infrastructure protection is that the defense of high-traffic, high-degree, and high-betweenness substations from attack is likely to be a cost-effective risk mitigation strategy.

\footnote{The North American power grid data used in this paper are available from the US Federal Energy Regulatory Commission, through the Critical Energy Infrastructure Information request process (http://www.ferc.gov/legal/ceii-foia/ceii.asp).}
III. “Critical slowing down” as an indicator of blackout risk

In this section we investigate a method for identifying statistical properties in high-resolution time-series data that appear to signal “critical slowing down,” which is frequently an early warning sign for critical phenomena. Building on substantial literature on critical slowing down, Scheffer et al. [25] describe methods for detecting proximity to transition in a variety of complex dynamical systems through the use of autoregression models. Here we apply the method described in [25], [26] to a two bus power system model and data from the August 10, 1996 blackout Western Interconnect. Both cases show evidence of critical slowing down as the point of critical transition (blackout) approaches.
Figure 4. The correlation between blackout sizes and connectivity loss (C) for 40 areas within the EI network. The correlation coefficients corresponding to each attack vector are as follows: $\rho = 0.210$ (random failure), $\rho = 0.621$ (degree attack), $\rho = 0.551$ (max-traffic attack), $\rho = 0.288$ (min-traffic attack), $\rho = 0.138$ (betweenness attack), and $\rho = 0.477$ (all simulations).

A. Background

It is well known that the trajectory of eigenvalues (poles) in a power system, or in any dynamical system, can be used to predict critical transitions such as voltage collapse or dynamic instability. References [27], [28], [29], [30] (among others) describe the use of this property for stability analysis in power systems. However, the accurate measurement of eigenvalue trajectories in a large system requires accurate models and large quantities of sensor data. Power system failures sometimes progress across the boundaries of balancing authorities, where sensor data are aggregated, through Energy Management (EMS) and SCADA systems. Across these boundaries models are often less useful. Furthermore, even within a balancing authority, cascading failures can progress more quickly than the communications and computational processes from which eigenvalues are calculated. Therefore there is a need for tools that can identify emerging risks without detailed, highly accurate, network models.

With the growing deployment of phasor-measurement (synchrophasor) units (PMUs) in power systems, there is a rapidly growing quantity of high-resolution time-synchronized sensor data available to system operators. Information in these data that could signal a critical transition such as voltage collapse or dynamic instability could be valuable to system operators who need to make timely, and costly, decisions to avert large blackouts. This section provides preliminary evidence that time-series data alone, without intricate network models, may be useful as an indicator of proximity to critical transition in power systems.

The concept of critical slowing down comes from statistical physics. The concept was first observed in ferromagnetic systems (random-field Ising systems [31]), in which it was observed that as the system approached a critical point (e.g., a bifurcation) the time required for it to recover from a perturbation (the relaxation time) increased rapidly. Scheffer et al. [25], argue that critical slowing down can be observed before critical transitions occur in time domain data from high-order, complex systems such as climate models [26], models of species extinction [25], and the human body before an epileptic attack [35]. Specifically, as noisy, high-order, systems are driven toward a critical point time-series data from those systems show a variety of statistical properties including increased signal variance as a result of “flicker” between or among alternative stable operating points and an increase in signal auto-correlation, which comes from the slow deviations that proceed from the increased relaxation time.

Given that critical slowing down is evident in other complex systems (or models of complex systems), the goal of this section is to test the following hypothesis:

**H1** High resolution time domain phase angle data show measurable evidence of “critical slowing down” during times of elevated blackout risk.

Subsection III-B describes the testing of this hypothesis for a simple 2-bus power system model and Subsection III-C describes the testing of H1 for data from the August 10, 1996 blackout in Western North America.

B. Two-bus model and results

To initially test H1 we use a single machine, infinite bus power system model in which the machine gradually increases its real power output toward the maximum power transfer limit for the system. The generator at Bus 1, with voltage $V_1$, is modeled as a classical round rotor, lossless generator [32]. It has a constant field (open circuit) voltage magnitude ($|E_f|$) behind a synchronous reactance ($X_s = 0.1$). The machine has a damping constant of $D = 1.5$ p.u. and an inertia constant of $M = 3$ p.u. The generator is initially driven by $P_m(t = 0) = 1.0$ p.u. of mechanical power. After accounting for damping losses (see below), all of this power is injected into Bus 1 as electrical power. Bus 1 is connected to the infinite bus
(Bus 2) via a single transmission line with impedance: 
\[ Z_{12} = 0 + j0.1 \text{ p.u.} \]
The voltage at the infinite bus \( V_2 \) is a random variable drawn from a normal distribution with a mean of \( V_2 \) and a standard deviation of \( \sigma = 0.001 \text{ p.u.} \). Thus the two-bus model represents a small generator connected to a large power grid over a transmission line. The grid end of the line is a bus with a small amount of exogenous noise. This noise serves to perturb the generator slightly from its steady-state operating condition.

The rotor dynamics are governed solely by the classical swing equation:

\[
P_m(t) = P_e(\delta(t)) + D\omega(t) + M\dot{\omega}(t)
\]

where \( \delta \) is the machine rotor angle, relative to the phase angle of the infinite bus, and \( \omega = d\delta/dt \) (thus \( \omega = 0 \) indicates nominal rotational velocity). The trajectory of \( \delta \) and \( \omega \) are calculated using forward Euler integration with a fixed time step of \( \Delta t = 0.1 \text{ seconds} \). At each time step the standard physical relationships facilitate the calculation of the electrical state variables:

\[
P_e(\delta(t)) = \Re(V_1(t)I_1^*) = \Re(E_f e^{j\delta} I^*)
\]
\[
E_f e^{j\delta} I^* = E_f e^{j\delta} (E_f e^{j\delta} - V_2)^*
\]
\[
= \frac{E_f^2 - E_f V_2 e^{-j\delta}}{Z_{12}^*}
\]

In steady state \( P_e = P_m \) since we assume that \( P_m \) is measured after accounting for the damping losses at normal rotational frequency. \( E_f \) is the open-circuit voltage that results from the rotor field current.

As defined here the system has a theoretical maximum power transfer from Bus 1 to Bus 2 of

\[
P_{\text{max}} = \frac{|E_f||V_2|}{X_{12} + X_s}
\]

Since the initial open circuit voltage \( (E_f) \) is \( \approx 1.02 \) per unit, the maximum power transfer is

\[
P_{\text{max}} = \frac{1.02 \cdot 1.0}{0.2} = 5.1 \text{ p.u.}
\]

To test for critical slowing down, we follow the procedure defined in [26], which describes the use of autocorrelation (or autoregression) to test for criticality in global climate models. The following summarizes this procedure:

1) Choose a window size within which to measure autocorrelation. This window should be large enough to capture enough data to minimize the impact of spurious changes. Here we use a 2-minute window size.

2) Filter the data in each window to remove slow trends that are not the result of critical slowing down. In this two bus example the slow increase in the phase angle at Bus 1 would be removed by this filter. Following the method in [26] we use a high-pass filter based on a Gaussian Kernel Smoothing function to remove trends slower than 0.1 Hz.

3) Choose a sample time-lag that will be used for the autocorrelation calculation. Setting this time lag to 1 second Eq. 1 gives the autocorrelation coefficient for a window ending at time \( t \).

\[
\rho_k = \frac{\sum_{\tau=t-120}^{t} x(\tau)x(\tau-1)}{\sigma_x^2}
\]

where \( \rho_k \) is the autocorrelation coefficient at time \( t_k \) and \( \sigma_x^2 \) is the variance in the signal within the window.

Figure 5 shows the results that emerge from this two bus model. Providing evidence in support of H1, the autocorrelation in the phase angle data at Bus 1 increases notably about 30 seconds before the system hits the point of maximum power transfer.

C. Western interconnect data and results

Shortly before 16:00 in the afternoon on August 10, 1996 a power line near Portland, Oregon sagged into underlying vegetation. This triggered a second line-trip on a neighboring line, which subsequently resulted in the loss of a small generator, which triggered a long sequence of events ending in the separation of the North America Western Interconnection into five sub-grids and the interruption of electric service to 7.5 million customers. Reference [33] describes the sequence of events leading up to the blackout, and [34] provides some detailed analysis of the power system dynamics during the event. In Reference [33], the WSCC (now WECC) disturbance study committee provided about 10 minutes of frequency data from the Bonneville Power Administration territory (See Figure 6).

In order to test for critical slowing down in these data, the printed frequency charts were scanned and translated into a numerical time series. The statistical test described above was repeated, with the only difference being that we used a two-second (rather than one second) time lag for the autocorrelation test. The rationale for this is that the autocorrelation is fairly high in the first portion of the signal (greater than 0.3) with a one second time lag, which would make it difficult to note a change in \( \rho_k \), if one were there. Figure 6 shows the results of the autocorrelation tests for the August 1996 data. As was found with the two-bus model, autocorrelation in the frequency signal increases notably as the critical transition approaches (See Figure 6).
Figure 5. Evidence of critical slowing down in a two-bus (single machine infinite bus) power grid model being driven toward the point of maximum power transfer. The black line shows the autocorrelation in the generator bus voltage phase angle. About 1 minute before the transition occurs the autocorrelation in the signal increases notably.

Figure 6. Evidence of critical slowing down in the frequency as measured at the Bonneville Power Administration, immediately before the blackout of August 10, 1996. The top figure shows the raw Bonneville Power Administration frequency data (merged from 4 pages of [33]). These data were tested for critical slowing down using the autocorrelation method described here, with a rolling 2 minute sample window and a 2-second time lag within each window.
D. Discussion of critical slowing down results

Given that critical slowing down has been observed in other large complex systems approaching points of critical transition, such as climate models nearing points of catastrophic climate change [26, 26], ecological systems [25] approaching population collapse, and the human body immediately before an epileptic seizure [35], it seems reasonable to believe that power systems show similar early warning signs. The results provided in this section do indeed indicate that critical slowing down could be useful in identifying operating states with unusually high dynamic risk. However, further research is needed to reliably identify critical slowing down. In future work we will investigate methods to integrate data from multiple PMUs to form a more reliable risk indicator, building on the concept of critical slowing down.

IV. Conclusions

This paper provides results from two different approaches to identifying blackout risks in power systems. In the first analysis we investigate a number of topological (graph theoretic) methods that are currently popular in the complex networks literature. While these approaches may have some utility in certain contexts, perhaps in combination with actual power grid data and/or physics-based models, the results described here indicate that when used in isolation from physical models, topological approaches can lead to very misleading conclusions. It is important therefore that risk-mitigation decisions not be based solely on topological models. In the second analysis we describe a method for testing for “critical slowing down” and argue that this measure could (given further development) lead to a measure that would be useful to operators in quickly deciding whether the current operating point is near a point of dynamic instability. The statistical approach described uses only high-resolution time data and could therefore be useful even if SCADA/EMS systems fail, so long as the operator has access to time synchronized phasor data.

References


