Evaluation of Cascading Infrastructure Failures and Optimal Recovery from a Network Science Perspective

Mary Warner, Bharat Sharma, Udit Bhatia, and Auroop Ganguly

Abstract This chapter reviews the network science literature in order to create a hypothesis for the recovery of infrastructure systems. We depict the cascade of infrastructure systems through networks and simulate perturbations within a singular topology and discuss how those impact multiple layers of an interconnected network. The simulation compares and contrasts the proposed recovery methods in the literature alongside true-to-life recovery, based upon case studies throughout the United States. We explore the limitations of imposing a recovery algorithm at various points in time during infrastructure failure. This chapter aims to provide resources that account for a quantitative approach to cascading infrastructure failures, as well as accounting for human nature, politics, perceptions, and communication that may prove to be hurdles to optimizing recovery.

Keywords Critical Infrastructure · Infrastructure · Climate Science · Hazards · Resilience · Recovery · Network Science

1 Introduction

Network science has emerged as a way to study networks and better understand the world around us. With the rise of resiliency literature and a transition away from risk-based assessments alone, network science is proving to be a tool that has great potential for understanding resilience. It is uniquely positioned due to the differences that have arisen between traditional risk approaches versus risk coupled with recovery to determine resilience. Although the field of network science

M. Warner · B. Sharma · A. Ganguly (✉)
Civil and Environmental Engineering, Northeastern University, Boston, MA, USA
e-mail: a.ganguly@northeastern.edu; a.ganguly@neu.edu

U. Bhatia
Civil and Environmental Engineering, Northeastern University, Boston, MA, USA

Civil Engineering, Indian Institute of Technology (IIT) Gandhinagar, Gandhinagar, Gujarat, India

F. Ghanbarnejad et al. (eds.), *Dynamics On and Of Complex Networks III*,
Springer Proceedings in Complexity, https://doi.org/10.1007/978-3-030-14683-2_3

is relatively new as compared to many other scientific fields and tools, several approaches have emerged by which network science can be used. Infrastructure and the interdependency that critical infrastructure systems have with one another are critical areas of observation. Many communities heavily rely on critical infrastructure, which makes the resilience of infrastructure vital to their day-to-day functioning. Network science is one tool that can be used to inform decision makers on optimal strategies for increasing the resilience of specific infrastructure as well as infrastructure systems.

2 Risk and Resiliency

2.1 Assessing Risk

Traditionally, engineers and scientists have aimed to mitigate risk, which has led to a variety of approaches and frameworks to both understand and mitigate risk. A traditional approach, often referred to as probabilistic risk analysis (PRA), has been widely used as a tool to quantitatively analyze risk in industry practice and policy. One of the first studies to examine PRA came from Kaplan and Garrick [1], who chose to define risk in the form of triplets. These triplets differ throughout the literature and academic fields. However, they are consistently chosen to be three metrics for which a probability can be assessed; the intersection of these probabilities determines the level of threat [1].

The International Panel on Climate Change (IPCC) has developed a risk framework in which the intersection of three calculable metrics determines the level of threat and the resulting actions to be taken. These actions can be classified into two separate categories: (1) the calculation of risk, which is determined by the combination of vulnerability, exposure, and hazards; and (2) the resulting actions to be taken, which can be classified as adaption and/or mitigation [2]. Although the precise calculations of each input and output may be measured differently depending on the evaluator and the scope of the analysis, there are traditional ways in which these calculations are performed. Hazards are typically measured as the probability of any given hazard occurring, such as the probability of a 500-year flood hitting any given region or the probability of an earthquake of a certain magnitude hitting that same region. Vulnerability is measured in terms of value that could be lost, which may be in the form of the number of human lives lost, ecosystem pricing, or the cost of infrastructure. This particular evaluation metric is one of the most difficult because it is both great in scope but simultaneously often results in assigning a cost value in terms of dollars, which lends itself to some controversy as to whether these value assignments accurately reflect true societal values [3]. Finally, exposure is measured in terms of the probability of damage given a threat. If many exposed assets exist and a hazard event is predicted to come, these assets are not vulnerable if they will not be in the path of the hazard event, nor will they be vulnerable if they are properly secured and reinforced.

When there is a high probability of a hazard, many valuable assets, and a high probability of damage as a result of the hazard, this results in severe risk [2]. The IPCC has laid out two definitions of risk: key and emergent. This definition is typically been associated with risks related to climate hazards, but it can be broadly interpreted as well. Key risks and emergent risks are distinguished as those that are extremely time sensitive and pressing due to imminent severity (key) as opposed to those that develop over time and gradually pose an increased risk (emergent) [2]. Although time-sensitive and pressing risks are important to immediately tackle, emergent risks pose some of the greater possibilities for action and therefore must not be ignored.

Once risk is determined, actionable items usually take the form of mitigation and/or adaptation. Mitigation includes actions that defer risk or in some way help to reduce risk. Mitigation is usually in the form of deflecting the hazard event from occurring. Adaptation is the action of learning how to change the system so that it can withstand the hazard itself. The IPCC Risk Framework illustrates adaptation and mitigation separately but in conjunction with governance and socioeconomic pathways [2]. Policies and economic incentives are often used to reach the mitigation or adaptive goal, such as through cap and trade programs to reduce extreme climatic change or stricter airport screening policies to reduce manmade terror threats [2].

2.2 Gaps in the Risk Literature

The IPCC Risk Framework focuses primarily on climatic or natural events, with a particular emphasis on climate change, but it has been widely adapted as a standard for many scientists to best quantify inherent risk and response strategies [2]. However, there are still many unresolved problems that come with evaluating risk and creating responses to risk assessments, which include but are not limited to the following: risk is done through a component-wise analysis, risk is threat-specific, and risk is system-specific. Essentially, risk is confined to assessing particular areas and particular activity within those areas and emphasizes pre-event preparation.

Throughout the world in which we live, we can witness the inherent interconnectedness of most of our critical infrastructure systems. The U.S. Department of Homeland Security has identified 16 categories of critical infrastructure, ranging from the transportation sector to the food and agricultural sector, with an attempt to capture all infrastructure on which we rely [4]. When performing a risk analysis as outlined by the IPCC and others, the choice must be made between limiting interconnectedness or including all connections but thus having an overly grandiose scope in which specific implications are difficult to attribute and computational time is high. For this reason, risk analysis has a tendency to require a specific location and specific threat, and the calculations are performed component-wise in the aforementioned style of the triplets [1].

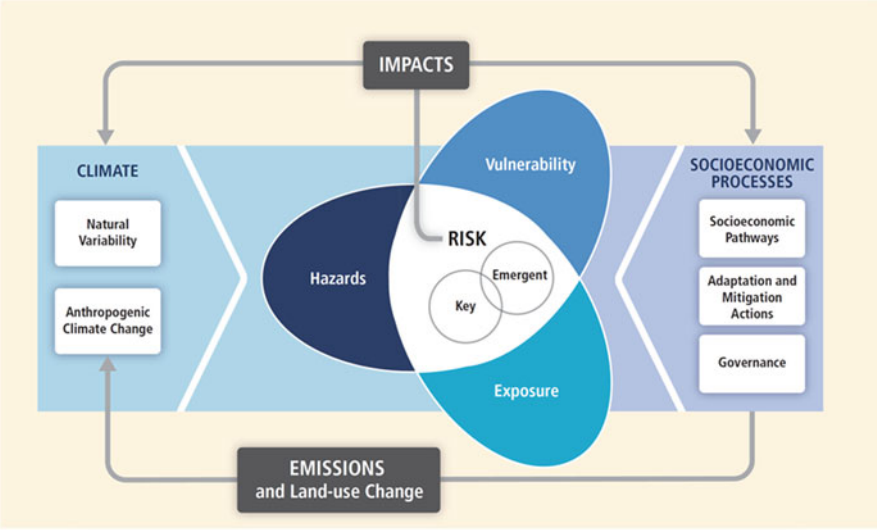

Fig. 1 A risk assessment framework that describes quantifiable ways to determine and calculate the risk of climatic changes [2]

However, this approach is problematic for several reasons. First and foremost, limiting location has action implications that may result in disjointed efforts to mitigate or adapt. For example, the probability of a hazard and its degree of impacts to Long Island, New York would also likely have impacts on downtown Manhattan (New York) due to both geographic proximity as well as shared resources and commuters between the two locations. Therefore, conducting a risk analysis and developing unique plans of action should not happen in silos. This location limitation can be scaled to greater or smaller location sizes due to the interconnected nature of all communities. There appears to be no universal solution as to where and how to draw geographic boundaries when disasters extend beyond any one confined area. Additionally, by limiting an analysis to a specific threat or hazard event, it particularly skews the public preparedness and infrastructure reinforcement. A building on the U.S. West Coast might be well-prepared for an earthquake because it is a reoccurring phenomenon, but that does not mean this same building is well-prepared for a fire, hurricane, terror attack, or cyber-attack. Each separate threat must be analyzed and acted upon separately according to a standard risk analysis (Fig. 1).

2.3 Moving Towards Resilience

Due, in part, to the growing recognition of the limitations of risk analysis, the field and concept of building and designing for resiliency has emerged. Resiliency takes the components of risk analysis and couples those results for preventative measures alongside a response to unpredictable, unforeseen, or cascading impacts. Due to the

interconnectedness of our resources, infrastructure, and geographical boundaries, the theory states that it is therefore nearly impossible to accurately predict and appropriately respond to any and all risks.

Resiliency has taken on many different definitions in different contexts and particularly in different fields, with one purported estimate of 70 unique definitions [5]. The consistent underlying message is the ability to be strong and adaptive. Therefore, for the purpose of agreement and consistency, this chapter has adapted and applied resilience theory based on the definition of the National Academy of Sciences: "the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events" [6]. Through this definition, a risk analysis can be determined or conducted prior to an event with the intention of mitigating or adapting, as well as actively recovering when risk analysis fails to be preventative.

Nonetheless, events that have been deemed "black swan" or "grey swan" events will always exist in the literature [7]. Black swan events are extremely unlikely but cannot be said to have no probability of occurring; however, their slim likeliness makes them very unpredictable. Grey swan events are very rare but still somewhat predictable. In both such events, the impact of the hazard would be catastrophic [8]. Take, for example, the terror attacks in the United States on September 11, 2001. This was a devastating event in which little information was known or could be drawn upon to know the exact plans, timing, and approach to catastrophe. The event was essentially unpredictable. Conversely, a 500-year flood—or a series of 500-year floods—is very rare, but data do exist by which we could have some predictable power. In both scenarios, the small likelihood does not negate the large impacts. Conducting a risk analysis and determining there is low risk because of the extremely small probability does not help when such an event does occur. The definition of resilience focuses on this addendum to the standard risk analysis and measures a system or system-of-systems ability to recover once a catastrophic event has occurred. This was best illustrated by Linkov et al. [9], who illustrated perturbation impacts and optimal recovery through a curve in which functionality changes over time (Fig. 2).

A resilient system is one with very limited, or perhaps no, boundaries [9]. When conducting a risk analysis, as previously mentioned, specific areas and threats are studied and the impacts are analyzed for each component, such as a specific industry or specific infrastructure. Resiliency assumes that interconnections and interdependencies are inherent and cannot be removed. Therefore, all must be considered and any given perturbation—whether it be a natural disaster or manmade attack—should have a minimal effect on the system's ability to respond.

3 Network Science as a Tool

Because the definition of resiliency is very broad, there must be a tool to study such a broad subject area. Although many tools do exist and have been proposed, the emergence of network science has provided some of the greatest and far-reaching

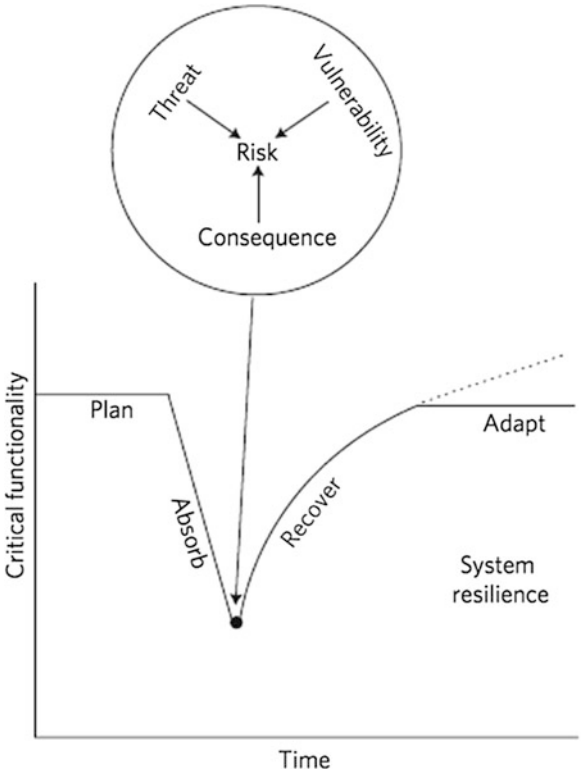

Fig. 2 A visualization of the resilience curve that highlights the loss and gain of functionality over time [9]

effects. Rooted in graph theory and mathematical proofs, network science is a fairly recent area of study [10, 11]. Network science, through the use of nodes and links, takes a more abstract approach to understanding resiliency: a node can have different mathematical attributes; however, to see node failure and cascading failures throughout the network, no granular detail is needed. Details are captured through mathematical applications, such as assigning weights or evaluating fitness. Impacts to any given node, as well as impacts to the system, can be analyzed in this way [10, 12].

The use of nodes and links allow for the theoretical approach to resiliency to be explored. In addition, it provides an opportunity to create multi-layer networks that represent the varying interplays between different systems. For example, although the functionality of a transportation network—such as an airline network—is reliant on the functionality of the infrastructure at each airport, it is also reliant on the communication network and communication towers. If communication were to be disabled, it would not solely impact that network but would cascade to other networks that rely upon on it [13].

Through the use of network science, various disasters can be simulated using real or hypothetical datasets. Nodes can be targeted at random, simulated terror

attacks can occur, or nodes can be targeted for a certain feature. This allows the system to be threat agnostic, and a simulation of its attack can be run. Additionally, a simulation of real-time versus optimal recovery strategies can be run using network science. When system-wide prioritizations are studied and made, optimal recovery is possible because the interactions and dependencies amongst all nodes are considered.

There are also many ways in which network science can be used as a tool to understand the resiliency of critical infrastructure systems. Two common approaches are a structural approach accompanied by a dynamic approach. These two separate approaches rely on network science to evaluate resilience; however, one approach focuses on low-dimensional models to capture a relatively static (non-evolving) network, whereas the other uses system dynamics to define an inherent assigned resiliency for any given complex network. Although each approach is valuable, this chapter analyzes two case studies of seminal papers in each field to highlight, compare, and contrast the approaches [14, 15].

4 Case Studies

4.1 Studying Resilience Curves

These case studies use the methodologies and work as outlined by Bhatia et al. and Gao et al. [14, 15]. These two methodological approaches were selected because they use the theory of network science to analyze similar infrastructure systems; in addition, they serve as foundations for future work. The inherent goal and use of network science for these approaches was to make the infrastructure systems more resilient and analyze their robustness. Similarly, both papers defined resilience such that the networks are able to recover after perturbations, which is in line with the definition selected for the purpose of this chapter [14, 15].

The methodology and results from each study are described and compared using open-source data. Although neither approach in itself is uniquely superior to the other, each comes with its own caveats and contentions. As a result, we suggest different applications and uses for each approach depending upon the desired results, computational time, and data availability.

4.2 Data

For the purpose of comparison, the same data and network were used for each approach to resilience. The data for this case study were gathered from the University of Washington's "IEEE 118 Bus Test Case," which represents a portion of the American Electric Power System in the Midwestern United States per records

dated December 1962. The data were saved in the IEEE Common Data Format by Rich Christie at the University of Washington in 1993. Figure 3 shows a diagram of the IEEE 118 Bus Test Case.

4.3 Limitations of the Data

As outlined by Kinney et al. [16], there are limitations to studying a power grid from a complex network analytical perspective due to the simplification of a nodes-link network in which not all essential nodes serve the same function. If all nodes necessary for functionality in the power grid are considered, then the network would have to be able to distinguish between various node functions, such as the distinction between substations and generators. In addition, the supply and flow of electricity through the system constantly varies depending on user demand and the generator from which the electricity is derived.

There are additional considerations, such as underground and above-ground systems in which unique vulnerabilities exist. The network itself is functionally and conceptually similar; however, an in-depth understanding of each node and each classification and vulnerability incurred by a node must be considered. Therefore, these data and the following model serve as a simplified proof-of-concept in order to depict the general schema of the network [16].

4.4 Network Analysis of IEEE Bus Test Case

For this analysis, it was assumed that the nodes are independent of each other and that each node serves the same function as the others. This assumption is a simplification of the network topology, but nonetheless provides general insights into the interconnectedness and interdependencies at play within the system. Figure 3 shows the network graph of the IEEE Bus Test Case [19]. The analysis was done using the NetworkX library for Python.[1] The graph has a total of 118 nodes and 179 links or edges, with the nodes representing the busses and the links representing the connections and reliance amongst them. The average degree of the graph is 3.03. The diameter—or the maximum number of link lengths from one bus to another—of the graph is 14.

Figure 4 shows a histogram of the degrees of nodes. The important insight here is that the maximum degree of the graph is 8, but the network as a whole is largely dominated by nodes of degree 2, which results in the average degree of the nodes being 3.03. This also indicates that the nodes with 7 or 8 degrees are much more

[1] https://networkx.github.io/.

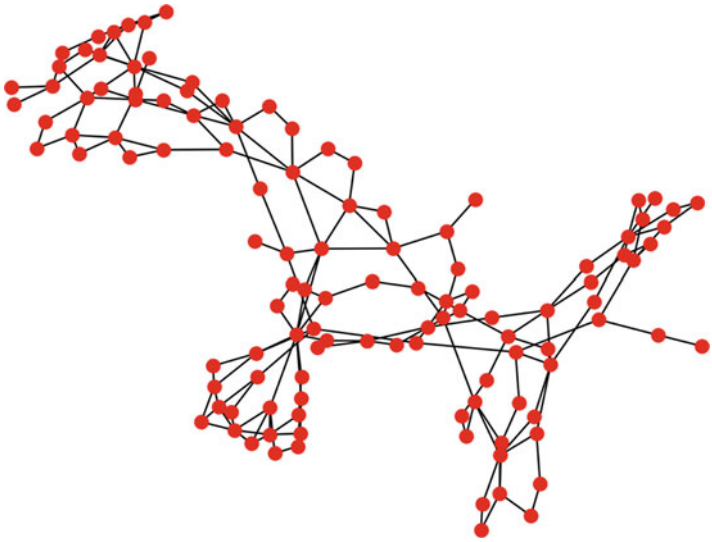

Fig. 3 The network graph

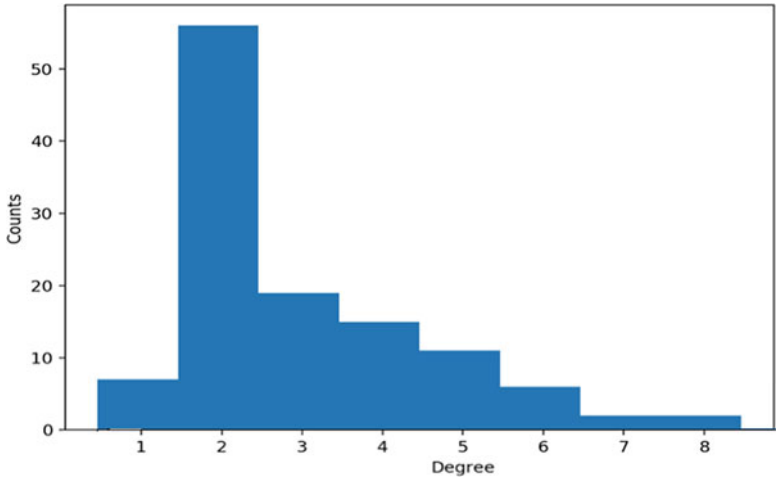

Fig. 4 Histogram of degrees

connected and potentially important to the system as a whole. This hypothesis is tested through network robustness and recovery.

4.5 Network Robustness

To check the robustness of the network, the different centralities were calculated. The centrality of the network is a measure of the importance of the nodes, such as how popular you are and/or how many people you know. Each node is assigned a centrality metric for which robustness can be determined, such that targeted or non-targeted attacks can be simulated. For example, see the following table from Newman [17]:

Centralities	Formula	Importance
Degree centrality, C^D	$C^D(i) = \frac{k_i}{N-1}$	– How popular you are – How many people you know
Betweenness centrality, C^B	$C^B(i) = \sum_{j<k} \frac{d_{jk}(i)}{d_{jk}}$	– Ability to be broken between groups – Likelihood that information originating anywhere in the network reaches you
Closeness centrality, C^C	$C^C(i) = \left[\sum_{j=1}^{N} d(i,j)\right]^{-1}$	– Being close to all nodes

Here, N is the total number of nodes, k_i is the degree of ith node, d_{jk} is the number of shortest paths between j and k, $d_{jk}(i)$ is the number of shortest paths between j and k that go through i, and $d(i,j)$ is the distance between i and j.

Based on the different measures of centrality, the nodes were removed in the decreasing order of importance to simulate a targeted attack. This is based on the assumption that a targeted attack would aim to disable the network as quickly and effectively as possible while gaining the most attention. For example, a terror attack that targets a node that is isolated or of very little importance will not gain much attention, nor will it have a great impact on the network as a whole. The random removal of a node, therefore, represents a non-targeted attack or one in which a natural disaster or an unintentional failure occurred [18].

At every time step after a node was removed, the number of nodes in the largest connected component (referred as the giant component) was measured. For example, after the first targeted attack, everything connected to the removed node would split off into several different large interconnected components. The new giant component is the one in which the most number of nodes are still connected [18].

From the graph depicted in Fig. 5, it is clear that removal of the first few important nodes (under a targeted attack) impacts the robustness of the graph substantially.

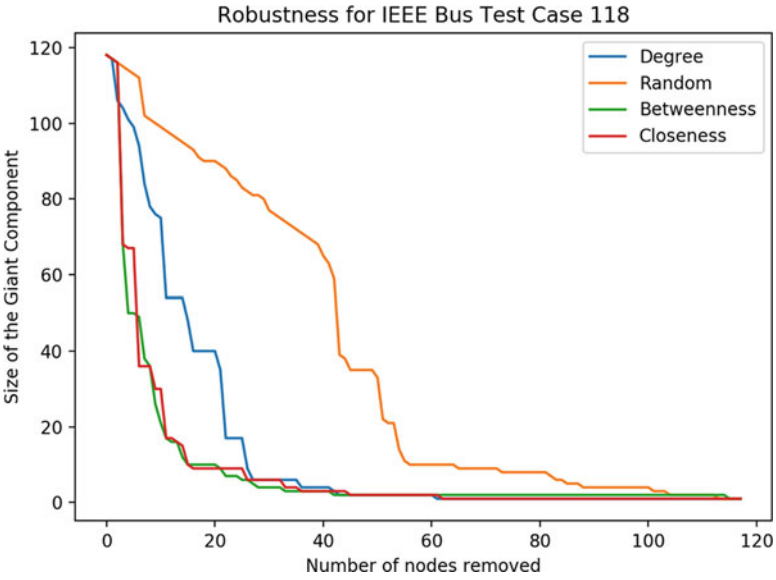

Fig. 5 Robustness graph for the IEEE Bus Test Case 118

It can be seen that an attack based on the betweenness centrality and closeness centrality affects the network the most; in this case, the targeting of the most connected node (highest degree) has slightly less impact. This procedure helps to identify the most critical nodes and how their removal affects the functionality of the network. Additionally, this process serves as a way in which decision makers can aim to strengthen the resilience of the system as a whole by knowing which nodes are of greatest threat to disabling the system.

4.6 Network Recovery

After any attack, whether it be targeted or random, it is of critical importance to restore the functionality of the system. Figure 6 shows a case of the random failure (left) that results in a complete loss of system functionality, followed by the recovery path (right) to restore the network's functionality after failure. To generate the resilience profile of the IEEE Bus Test case, the recovery algorithms from the Recovery-Master git repository[2] were used [14].

This approach has been outlined and proposed elsewhere [14]. It assumes that the network remains relatively static and the dynamics of the network do not change throughout the analysis. This assumption can be challenged, but it is also

[2]https://github.com/udit1408/Recovery_algorithm.

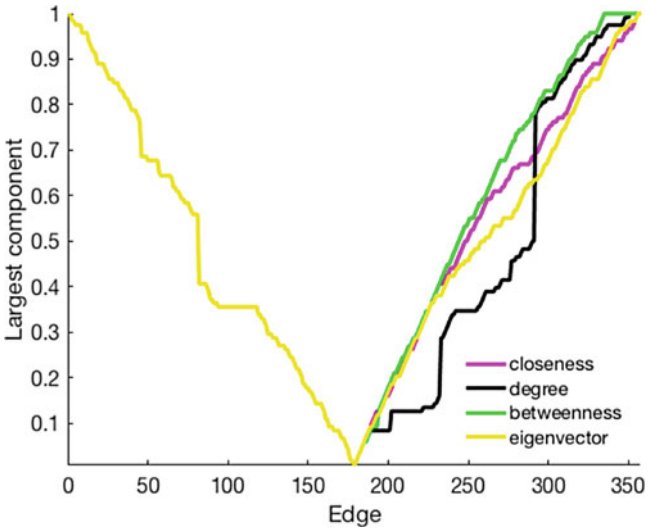

Fig. 6 IEEE Bus Test Case resilience curves

important to consider the time period over which loss of functionality occurs. Loss of functionality in the electricity grid network during an unprecedented storm may be very swift, with little action that is able to be taken until the storm passes. However, if the same analysis was conducted for the loss of biodiversity over the course of hundreds of years, then there is ample time for the structure of the network to change and adapt. For the purpose of this failure and recovery system, it remains logical to maintain the underlying assumptions.

Additionally, the conclusions from this methodology indicate to decision makers the best way in which to respond to the failure of a system. When all nodes are disjointed, no longer connected, and therefore no longer able to provide any functionality, the way in which the system recovers is important in order to return it most efficiently to full functionality. If many different operators attempt to return each individual node in the network to functionality without a targeted plan for resource allocation, then more time will be wasted. In this scenario, as outlined in Fig. 6, it is optimal to prioritize and allocate resources first towards nodes with the highest betweenness centrality, because this results in the quickest return to functionality.

4.7 Universal Resilience Curves [15]

The research done by Gao et al. [15] is unique from that of Bhatia et al. [14] in two major ways. First and foremost, Gao et al. [15] had a goal of determining how resilient any given network is, whereas the purpose of the research from Bhatia

et al. [14] was to determine how best to recover a system after failure. Both studies lend insights to one another and are not mutually exclusive from one another. Additionally, the inputs and results from Gao et al. [15] take the dynamics of the system into consideration, as opposed to performing an analysis primarily on the basis of a singular topology. This requires more inputs, such as various equations regarding how to calculate the resilience, as well as a thorough understanding of the way in which the observed network acts, changes, and adapts.

The following research was conducted through the Gao et al. [15] study on measuring universal resilience; the processes and a brief understanding of the inputs are described. The authors were able to provide several equations and dynamics of the data, which produced results that demonstrated how any given network could respond to perturbation. These equations are highlighted and described as follows:

- Transmission lines have a characteristic admittance, Y. To calculate current (I) through each bus using Y and voltage at bus, V:

$$I_i = Y_{ii} V_i - \sum_{\substack{k=1 \\ k \neq i}}^{N} Y_{ik} V_k, \tag{1}$$

- To calculate load at each bus, S:

$$S_i^* = V_i^* I_i, \tag{2}$$

- To obtain a measure of system resilience, substitute Eq. (1) into Eq. (2), then multiply both sides of equation by the complex conjugate and the quadratic equation for voltage on each bus:

$$|V_i|^4 - \left(\frac{2\,\mathrm{Re}\,(S_i Y_{ii})}{|Y_{ii}|^2} + \left| \frac{1}{Y_{ii}} \sum_{\substack{k=1 \\ k \neq i}} Y_{ik} V_k \right|^2 \right) |V_i|^2 + \frac{|S_i|^2}{|Y_{ii}|^2} = 0 \tag{3}$$

Therefore, Gao et al. [15] concluded that if there is a real solution for Vi_2, the system is functioning. If not, then the only possible outcome is blackout state with zero voltage and zero load. A nonzero solution exists if the discriminant is greater than zero:

$$\sqrt{\frac{|Y_{ii}|^2}{|S_i|\,|Y_{ii}| - \mathrm{Re}\,(S_i Y_{ii})}} \left| \frac{1}{Y_{ii}} \sum_{\substack{k=1 \\ k \neq i}} Y_{ik} V_k \right| - \sqrt{2} > 0, \tag{4}$$

To obtain the simulations of the IEEE Bus Test Case, the network has to satisfy Eq. (4), then apply perturbation (λ) at a single node (m), such that load at node m is increased:

$$S_m \rightarrow (1 + \lambda)\, S_m .$$

Then, new activity is calculated at each node. λ is increased iteratively until the system fails at the critical perturbation, λ_c.

The simulation output is as follows:

1. For each load bus, a $5 \times M$ matrix is used, with M being the number of steps to λ_c.
2. Variables returned are voltage amplitude, β effective, lambda, x effective, and gamma.

The variable β was defined by Gao et al. [15] as representing the changing environmental conditions and x effective represents the most effective state of the system. Therefore, β effective is the conditions under which we create x effective.

In power systems, λ_c is highly dependent on the selection of the perturbed node m. For some nodes, a load increase of $\lambda \sim 1$ leads to collapse, whereas for others the system maintains its resilience even up to $\lambda \sim 10^2$—a discrepancy of two orders of magnitude. This diversity exposes the difficulty in predicting a power system breakdown [15].

Figures 7 and 8 were derived from running the data, equations, and code provided by the study via open source documentation. Figure 7 shows the performance of the power supply network under increasing demand. λ was increased until the system reached collapse. λ_c is highly unpredictable. Figure 8 shows that mapping to β-space led to much more predictable behavior, exposing the universality in power system resilience and showing that β effective captures the natural control parameter also for power supply systems. Both of the figures were created using the NuRsE git repository.[3]

[3] https://github.com/jianxigao/NuRsE.

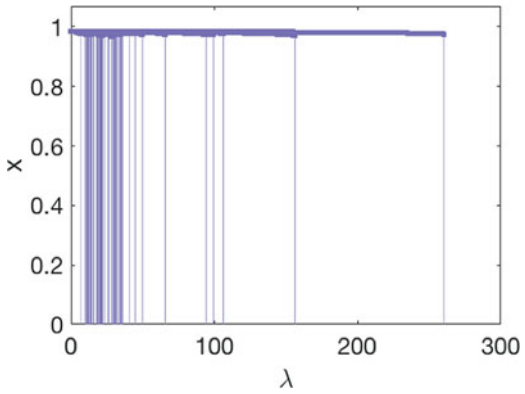

Fig. 7 Performance of the IEEE Bus Test Case under increasing demand

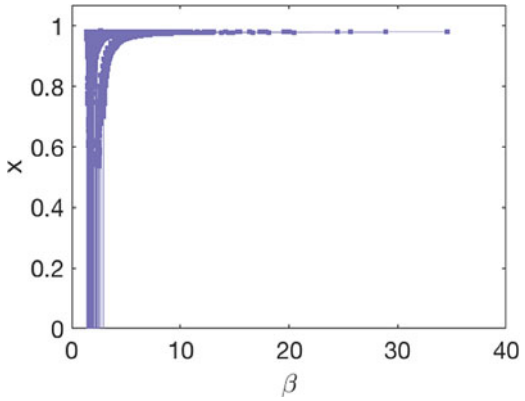

Fig. 8 Predictable behavior when mapping to β-space

4.8 Insights and Conclusions

Based upon these two approaches, it is evident that network science serves as a valuable tool to inform the recovery of a system. Although traditional approaches have focused on risk assessment and methods to avoid collapse, these risk analyses do not typically serve to fully protect a system from failure when faced with extreme or catastrophic events. In addition, through this research, it is clear that failure of even one node can quickly cascade through the system.

We are unable to predict all events; therefore, even the best protections and risk analyses cannot and do not ensure no-failure. Bhatia et al. [14] focused on a way to most efficiently recover a system once it has failed. Although there are many underlying assumptions in this case study, including the data and network structure, the fundamental assumption is that the need for dynamic responses and shifts in the system is unnecessary in this scenario. There is reason to believe that this analysis also works well for similar infrastructure systems, particularly those faced with relatively immediate threats and destruction.

Although there is potential for degradation and dynamic shifts in infrastructure that may allow for gradual adaptation, this chapter focuses on the risks that have small probabilities of occurrence but large-scale impacts. These large impacts imply that failure would quickly cascade, although this is not inherently true.

Simultaneously, every system has hidden universal patterns of resilience [15]. These dynamics could and should be considered for an optimal understanding of a system's ability to adapt and respond to perturbation. The origin of this universality is the initial separation of the system's dynamics and topology. Gao et al. [15] also suggested potential intervention strategies to avoid the loss of resilience or design principles for optimal resilience in systems that would be able to cope with perturbations. This unique approach requires more computational time due to the necessity of knowing the dynamics of the system to be studied, and the β effective must be calculable. Although the dynamics and intricacies of many networks are known, this does not hold true for all networks. Finding the unique input values would require more data than is required by the approach in Bhatia et al. [14].

Therefore, it is safe to conclude that both approaches are of value. However, the way in which each can be used depends on the desired outcome and the inputs that would be required. Additionally, this recovery strategy [14] can be coupled with the universal resilience patterns results [15] to observe the resilience parameters of any given system, and then to study how to recover the system if it were to fail. One approach indicates how to recover, with the end results providing insight into the resilience of the network [14], whereas the other approach indicates the resilience of the network, with the end results providing insight into how to recover. These two approaches are therefore not mutually exclusive and can be coupled. The research here highlights failures in a power grid network, but it can be applied to many other networks within critical infrastructure and beyond.

References

1. Kaplan, S., Garrick, B.J.: On the quantitative definition of risk. Risk Anal. **1**, 11–27 (1981). https://doi.org/10.1111/j.1539-6924.1981.tb01350.x
2. International Panel on Climate Change Secretariat: AR5 Climate Change 2014: Impacts, Adaptation, and Vulnerability. International Panel on Climate Change, Geneva (2014). https://www.ipcc.ch/report/ar5/wg2/
3. Gomez-Baggethun, E., Ruiz-Perez, M.: Economic valuation and commodification of ecosystem services. Prog Phys Geogr. **35**(5), 613–628 (2011)
4. Department of Homeland Security (DHS): Critical Infrastructure Sectors. United States Cyber Security and Infrastructure Security Agency. (2018). https://www.dhs.gov/cisa/critical-infrastructure-sectors
5. Fisher, L.: Disaster responses: more than 70 ways to show resilience. Nature. **518**, 35–35 (2015). https://doi.org/10.1038/518035a
6. National Research Council: Disaster Resilience: A National Imperative. The National Academies Press, Washington (2012). https://doi.org/10.17226/13457
7. Stein, J.L., Stein, S.: Gray swans: comparison of natural and financial hazard assessment and mitigation. Nat. Hazards. **72**, 1279–1297 (2014)

8. Lin, N., Emanuel, K.: Grey swan tropical cyclones. Nat. Clim. Chang. **6**, 106–111 (2016). https://doi.org/10.1038/nclimate2777
9. Linkov, I., Bridges, T., Creutzig, F., et al.: Changing the resilience paradigm. Nat. Clim. Chang. **4**, 407–409 (2014)
10. Barabasi, A., Albert, R.: Emergence of scaling in random networks. Science. **286**(5439), 509–512 (1999)
11. Chawla, N., Ganguly, A.: Complex networks as a unified framework for descriptive analysis and predictive modeling in climate science. Stat Anal Data Min. **4**(5), 497–511 (2011)
12. Watts, D.J., Strogatz, S.H.: Collective dynamics of 'small-world' networks. Nature. **393**(6684), 440–442 (1998)
13. Clark, K., Bhatia, U., Kodra, E., Ganguly, A.R.: Resilience of the US National Airspace system airport network. IEEE Trans. Intell. Transp. Syst. **99**, 1–10 (2018). Accepted (minor changes)
14. Bhatia, U., Kumar, D., Kodra, E., Ganguly, A.R.: Network science based quantification of resilience demonstrated on the Indian Railways Network. PLoS One. **10**(11), 1–17 (2015). https://doi.org/10.1371/journal.pone.0141890
15. Gao, J., Barzel, B., Barabási, A.-L.: Universal Resilience Patterns in Complex Networks. Nature. **530**(7590), 307–312 (2016). https://doi.org/10.1038/nature16948. Nature Publishing Group
16. Kinney, R., Crucitti, P., Albert, R., Latora, V.: Modeling cascading failures in the North American power grid. Eur Phys J B. **46**(1), 101–107 (2005). https://doi.org/10.1140/epjb/e2005-00237-9
17. Newman, M.E.J.: Networks: An Introduction. Oxford University Press, Oxford (2010)
18. Barabasi, A., Posfai, M.: Network Science, 1st edn. University Press (2016). ISBN-10 1107076266
19. Christie, R.: Power systems test case archive (2000). http://www.ee.washington.edu/research/pstca/