Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira,
Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26393-cd

Applying Computational Network Analysis Methods for Critical Infrastructure Robustness: Integrating Centrality Metrics and Model Simplification for Efficient Failure Simulations

Veronica Li Aguirre

Civil and Environmental Engineering, Princeton University, United States. E-mail: veronicali@princeton.edu

Jürgen Hackl

Complex Infrastructure Systems Group, Princeton University, United States. E-mail: hackl@princeton.edu

This research work presents computational network analysis methods to assess the robustness of critical infrastructure under failure scenarios while improving simulation efficiency. We propose modeling infrastructure systems as unweighted and undirected graphs to evaluate robustness through percolation-style node removal failure simulations. Removal of nodes are prioritized by topologically-focused network metrics, degree and betweenness centrality, with and without recalculating the rankings, and compared to random selection. To reduce computational burden, we introduce a model simplification that removes sequential degree-two nodes while preserving overall topology. We demonstrate the methods on the Seattle road network (23,303 nodes, 34,243 edges) and a simplified version with 9% fewer nodes and 6% fewer edges. Results show that targeted removals degrade network connectivity more effectively than random failures. Dynamic update of the betweenness centrality metric over the percolation process is the most disruptive scenario which highlights the value of adaptive prioritization of assets in the evolving network during failures. The simplified model yields an average 16% reduction in computation time with minimal impact on collapse behavior, indicating that omitting degree-two nodes can improve practicality without sacrificing accuracy. The study provides transferable methods for identifying critical assets and conducting efficient robustness analysis of large-scale infrastructure networks with more than twenty thousand nodes.

Keywords: Infrastructure Resilience, Network Analysis, Model Simplification, Failure Simulation, Centrality Metrics.

1. Introduction

The need to replace aging infrastructure while improving sustainability and resilience to climate change presents major challenges for critical service providers. Infrastructure managers face growing urgency to integrate resilience measures as climate extremes intensify, service demands exceed capacity, cybersecurity threats rise, and failure risks increase. Interruptions to critical water, electricity, or transportation services can severely impact public health, safety, and quality of life. To maintain reliable services, managers require tools to prioritize system renewal and prevent failures of key operational nodes and segments. The current practice for infrastructure capital replacement prioritization is managing a database of assets ranked by age and condition, which may not fully capture the criticality of assets to overall system performance nor the changing system conditions during failures (Kulkarni, 2020). Technological limitations hinder practical adoption of integrated and large urban-scale infrastructure models for proactive vulnerability detection and real-time decision-making in emergency reponse (Kulkarni, 2020). As infrastructure management becomes increasingly data-driven, computationally intensive models often lack the adaptability needed for timely hazard or outage response (Mintoo et al., 2022). Erath et al. (2009) highlight how computational demand in vulnerability assessment methodology is especially true for traffic modeling in urban road networks. They identify that a major constraint on the use of traffic assignment models for analyzing transport-related failures is the computational intensity. These challenges highlight the need for infrastructure engineering strategies that enhance both resilience and computational efficiency.

Network science and computational modeling techniques enable engineers and planners to assess the robustness of networks in failure scenarios. Robustness analysis via failure simulations is a means to identify critical nodes and pathways whose failure would most significantly impact overall network connectivity (Callaway et al., 2000). Network robustness refers to the ability of a network to maintain its overall connectivity and functionality despite failures or attacks on its components (Albert et al., 2000). Computational modeling techniques represent actual infrastructure networks as graphs to conduct failure simulations. We propose that robustness assessment via percolation theory applied to graph models of infrastructure networks can help identify critical system components, guide capital replacement prioritization, and inform emergency response planning.

This study applies network analysis methods to evaluate infrastructure robustness with topologically focused centrality metrics and model simplification techniques. The unique contributions of this work are threefold:

- We compare static and dynamic prioritization approaches in targeted attack simulations to highlight the importance of infrastructure asset reprioritization during failure events.
- We identify a model simplification technique of omitting network nodes of degree two to reduce computational overhead while maintaining accuracy.
- We demonstrate the scalability of these robustness assessment methods on large infrastructure networks through a case study on an urban road network of over 20,000 nodes.

By comparing failure strategies, prioritization approaches, and model versions, we identify effective techniques for accurate robustness assessment with reduced computational overhead. These findings inform scalable and transferable methods for infrastructure robustness assessment that balance detail with computational practicality.

2. Background Literature

The application of network science percolation theory to infrastructure robustness assessment has been explored in various studies. Artime et al. (2024) summarizes the development of percolation theory and its application to complex networks, including infrastructure systems. They argue that percolation is the most studied, direct, and intuitive framework to approach network dismantling. They define percolation as an experiment where network nodes are removed according to predefined rules or attacking protocols and then different statistical and geometrical properties of the residual network are computed. They further explain how network dismantling can be done in a static or dynamic manner, where the node removal order is computed once at the beginning of the simulation or recalculated after each node removal step to account for the changing state of the network. Cohen et al. (2001) apply percolation theory to analyze the robustness of the Internet under intentional attacks. They find that removal of the higest connectivity sites changes the connectivity distribution such that the connectivity of the remaining network needs to be recalculated accordingly. Callaway et al. (2000) apply percolation theory to analyze the robustness of networks under random failures and targeted attacks. Their work demonstrates that these methods can effectively model the robustness of networks to breakdown or sabotage.

There have been several percolation studies that are based on network topology to identify critical nodes in failure simulations of civil infrastructure systems. Network centrality metrics such as degree and betweenness centrality are informed by topological information to identify critical nodes and pathways within infrastructure systems (Rodrigues, 2019). Albert et al. (2000) introduce the model of intentional attack where the most critical nodes with the highest connectivity, or degree centrality, are targeted first. Dunn and Wilkinson (2013) identify strong correlations between these centrality measures and flow through the corresponding node for infrastructure networks. Morone and Makse (2015) addresses the problem

of quantifying network node influence by finding the optimal set of structural influencers. To do this, they find the minimal set of nodes which, if removed, would break down the network into many disconnected pieces. As the influencers are removed from the network, they determine that the natural measure of influence is the size of the largest connected portion of the network remaining. Wang et al. (2019) analyze the robustness of critical infrastructure networks under targeted attacks using betweenness centrality to identify critical nodes. They find that targeted attacks based on betweenness centrality are more effective at disrupting network connectivity compared to random failures.

The broader impacts of the infrastructure robustness assessment and computational work in this study are based on the most recent research in network analysis. Mintoo et al. (2022) discuss the role of AI-driven digital infrastructure in enhancing national resilience. They highlight the importance of integrating advanced computational methods into infrastructure management for improved resilience. Erath et al. (2009) present a traffic assignment model that requires enormous computational intensity and high input data quality for road network vulnerability assessment. Artime et al. (2024) advise that early warning indicators of impending network collapse and repairs along with adaptive responses to an evolving collapse are the best line of defense. They ultimately acknowledge that understanding how systems react and adapt to external shocks is an overarching goal for future research. These studies underscore the need for efficient computational network analysis for infrastructure robustness assessment and motivate the methods applied in this research.

3. Methods

This study employs network analysis techniques to evaluate the robustness of critical infrastructure systems. We use georeferenced network data to generate a planar graph G of nodes connected via edges. A graph is defined as $G = (V, E)$ where V is the set of nodes and E is the set of edges. The graph G is unweighted and undirected to focus solely on the network structure in the analysis. Unweighted means that all nodes and edges are considered equally important in the analysis. Undirected means that edges do not have a direction, allowing travel in both directions along each edge.

We assess the susceptibility of the network to failure under different scenarios: random failure and targeted attacks. We model attacks or failures of system nodes by removing nodes from the network and assessing the impact on the overall network structure. Failure simulations are conducted by systematically removing nodes from the network and measuring the size of the largest connected component, or core of the network that remains, after each node removal. We run failure simulations by removing one node in each removal step until the largest connected component is reduced to a single node or no nodes remain. Each node removal step is considered a distinct closure scenario in relation to the original network. The nodes are ranked by network centrality metrics in the targeted attack scenarios and randomly selected in the random failure scenarios. We run all the failure simulations on two versions of the network data: one version including all nodes of the actual system and a simplified version where the network is re-wired to omit sequential nodes of degree two.

We compute two centrality metrics to rank the nodes by criticality for the targeted attack scenarios: degree centrality and betweenness centrality. Degree centrality (C_D) is defined as the number of edges incident upon a node (Freeman, 1978). It measures the number of direct connections a node has to other nodes within the network. For road networks, degree centrality indicates the number of road segments connected at an intersection. A high degree centrality at a junction might suggest it is a larger intersection with many connecting roads and more complex traffic signaling. For the undirected graph G, the degree centrality of a node v is given by:

$$C_D(v) = \sum_{u \in V} a_{uv} \tag{1}$$

where a_{uv} are the elements of the adjacency matrix, indicating a connection between nodes u and

v. V is the set of all nodes. Betweenness centrality (C_B) quantifies how often a node appears on the shortest paths between other nodes, indicating its role as a bridge (Freeman, 1977). It is calculated as the fraction of shortest paths between any pair of nodes that passes through a node. How "central" a node is based on the amount of shortest paths that pass through it. Because it is an indicator of a node's control over the network's flow, this metric reflects a node's potential to facilitate or impede traffic movement through the network. In road networks, a node with high betweenness centrality would be critical for traffic flow between different parts of the network. Such nodes, if compromised, could significantly impact the network's performance and reliability.

The betweenness centrality of a node v is calculated by the following formula:

$$C_B(v) = \sum_{s \neq v \neq t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}} \tag{2}$$

where σ_{st} is the total number of shortest paths from node s to node t, $\sigma_{st}(v)$ is the number of those shortest paths that pass through node v, and V is the set of all nodes.

We run targeted attack simulations by removing nodes based on their centrality rankings where the nodes with the highest degree and betweenness centrality values are removed first. The network dismantling is initially done in a static manner where we compute the node removal order by degree and betweenness centrality at the beginning of the simulation process. We run the targeted attack simulations by degree centrality in a static manner only. This is because degree centrality is a local measure that does not change with the removal of other nodes. This is unlike betweenness centrality which is a global measure that can evolve as nodes are removed. An example of this is that when a node with high betweenness centrality is removed, the shortest paths between other nodes may change, leading to a recalculation of betweenness centrality values for the remaining nodes. We conduct multiple runs of the targeted attack simulations by degree centrality for representative average results for the overall network. This is necessary because infrastructure networks can have many nodes of the same degree such that random selection among nodes with the same degree can lead to different network collapse rates.

To test the effectiveness of dynamic reprioritization, we run targeted attack simulations by betweenness centrality in both static and dynamic modes. In static mode, the node removal order by betweenness centrality ranking is computed once at the beginning of the simulation and remains unchanged throughout the node removal process. Next, we conduct network dismantling in a dynamic manner where we recompute the node betweenness centrality values at each node removal step. The comparison of the simulation results for the static and dynamic modes inform which method is the most effective strategy for infrastructure asset prioritization. We run random failure simulations by removing one randomly selected node in each removal step. We average these results to determine the average behavior of network robustness under random failures.

To enhance computational efficiency, we implement a model simplification approach that removes sequential nodes of degree two. This network re-wiring reduces the total number of nodes while preserving the overall network structure. Nodes of degree two lie along paths and do not contribute to alternative pathways in the network. We compare the performance of the full and simplified models to determine whether network simplification for improved computational speed affects robustness analysis results.

4. Case Study

We demonstrate the methods on the Seattle road network as real-world case example. The full Seattle road network data is obtained from Str (2025) and used to build a graph G of 23,303 nodes and 34,243 edges. The graph G is unweighted and undirected, assuming equal importance for all nodes and road segments and bidirectional travel on all road segments. We generate a simplified version of the Seattle road network by removing sequential nodes of degree two. This re-wiring reduces the network to 21,202 nodes and 32,061 edges. We run four types of failure simulations on both versions of the Seattle road

network: targeted attack by degree centrality, targeted attack by betweenness centrality in static mode, targeted attack by betweenness centrality in dynamic mode, and random failure. Because many nodes can have the same degree within each removal step, we run the targeted attack simulations by degree 50 times with random selection among nodes of the same degree. We run the random failure simulations 100 times to account for variability in the random selection process. The performance of the full and simplified models is compared in terms of accuracy and computational time.

The computational work of this research is conducted on an 8-core Intel Xeon CPU with 1010 MHz average speed and 64 GB RAM. We use the open-source NetworkX(Net, 2025b) and NetworKit(Net, 2025a) packages for the analysis of structure, dynamics, and functions of networks in the Python programming language. Particularly, NetworKit provides multicore and parallel computing architectures for computing the betweenness centrality of the large network containing thousands to billions of edges (Net, 2025a). To generate visual renderings of the large-size network and service area, we utilize the open-source QGIS version 3.40.12 Bratislava (QGIS).

5. Results and Discussion

The simplified version of the Seattle road network is mapped in Figure 1 with 21,202 nodes representing intersections and 32,061 edges representing road segments. Nodes of high betweenness centrality have values that are greater than the mean plus one standard deviation of all initial betweenness centrality values. These high betweenness centrality nodes highlight the intersections that function like bridges in the network. The top ranked nodes by degree and betweenness centrality are considered the most critical whose failure would most significantly impact network connectivity. We observe that nodes with high degree centrality are often located at major intersections, particularly at highway on and off ramps. Nodes with the top ten highest betweenness centrality values are situated along Interstate Highway I-5, a key transportation route that vertically cuts through the center of Seattle. I-5 is considered a critical connection between the North and South regions of the city and is known to have high traffic volumes (Haselkorn et al., 2018). The results for all failure simulation strategies on the simplified and full versions of the Seattle road network are shown in Figures 2 and 3. Because we run the failure simulations until the entire network collapses, the plot curves provide a comprehensive view of the network's robustness across the full range of node removals from the initial state to complete collapse. The area under the plot curves in Figures 2 and 3 can be considered a global robustness measure of the whole system under each failure strategy, with the smaller area indicating a more rapid collapse of the network. The results indicate that targeted removal strategies more rapidly reduce the size of the largest connected component compared to random removal. This aligns with the expectation that targeted attacks by centrality rankings are more effective at disrupting network connectivity. In all cases,

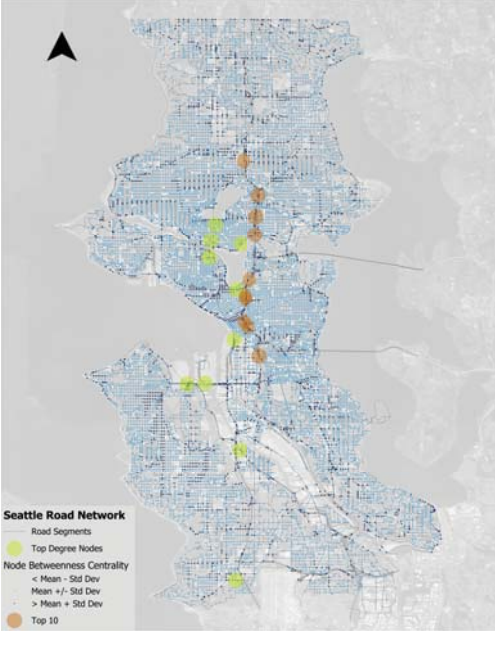

Fig. 1. Map of the Seattle road network segments with nodes colored by initial betweenness centrality. The nodes with the top 10 betweenness and degree centrality values are highlighted.

dynamic dismantling proves more effective than static approaches. This highlights the importance of prioritization updates in failure simulations for infrastructure emergency response planning. As shown by the slower rate of network collapse with the static method, the initial betweenness centrality rankings may not fully capture the evolving criticality of nodes as failures occur. Dynamic reprioritization allows for more accurate identification of critical nodes throughout the failure simulation process. Once a node is removed, the network structure changes, potentially altering the shortest paths between remaining nodes so that the next most critical node from the initial prioritization may not be the most critical node in the updated network.

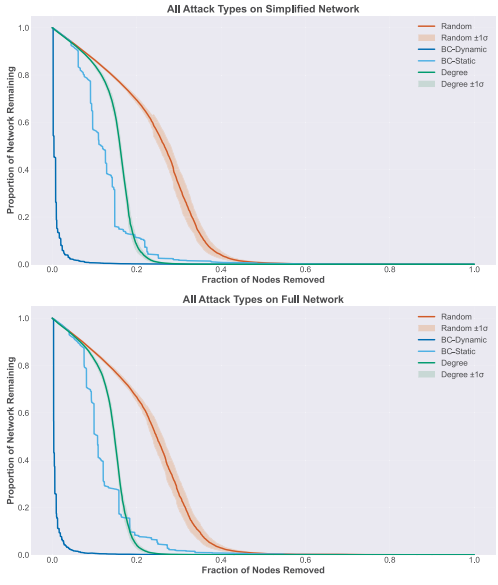

Fig. 2. Failure simulation results for (top) the simplified version and (bottom) the full version of the Seattle road network.

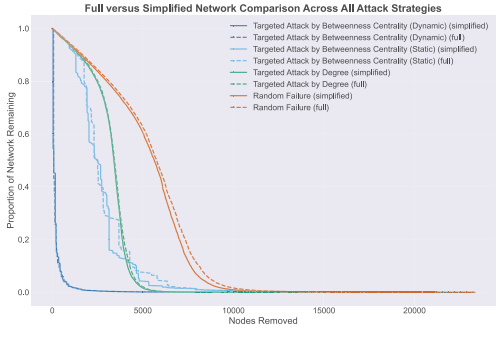

Fig. 3. Comparison of full and simplified network failure simulation results showing the size of the largest connected component as nodes are removed based on different strategies.

The targeted attack by degree and random failure results with standard deviations are included in Figure 2. Figure 3 highlights the average results for the multiple runs of these failure simulation types. The standard deviation of the targeted attack by degree runs appears minimal, with some spread of results around network collapse at the removal of 20% of the nodes. The standard deviation of the random failure runs is greater, although relatively consistent across multiple simulations that have the network reaching complete collapse by the time 40% of nodes are removed. The average curve for random failure of the full network is shifted slightly to the right compared to the simplified network, which makes the full network appear more robust. This can be attributed to how nodes of degree two can contribute to the network's overall robustness. Degree two nodes along a continuous segment can provide means to isolate segments of the network with minimal disruption to the overall system. An example of this is the ability to isolate a road network segment by closing off traffic at two intersections and redirecting traffic around the rest of the network.

The proper comparison of the two network versions is by the number of nodes removed until network collapse shown in Figure 3. The simplified network contains fewer nodes than the full network so the x-axis values differ by 2,101 nodes between the two network versions. Comparison of the network collapse rates by fraction of nodes removed in Figure 2 makes the simplified network appear more robust under targeted attacks by degree and random failures. However, this apparent robustness suggests that a direct comparison of the largest connected component fractions may not be consistent across the two datasets, since the simplified network contains fewer nodes overall.

Model simplification by removing sequential degree two nodes demonstrates an average 16%

reduction in computational time with minimal impact on result accuracy as shown in Table 1. The

Table 1. Computational times in seconds for the full and simplified versions of the Seattle road network data in each failure simulation scenario: Targeted attack by degree, Targeted attack by betweenness centrality (static and dynamic), and Random failure.

Scenario	Full (s)	Simplified (s)	Δ (-%)
Random	117	95	19
TA Degree	240	194	19
TA BC Static	1,096	923	16
TA BC Dynamic	7,553	6,486	14

computational time differences between the full and simplified network data versions in Table 1 show that an 9% reduction in the number of network nodes results in a 14% reduction in computational time for the scenario with the longest runtime which is the dynamic targeted attack by betweenness centrality. In the dynamic targeted attack by betweenness centrality and targeted attack by degree scenarios, the failure simulation results for the simplified and full networks are aligned. This suggests that network simplification can enhance the practicality of these vulnerability assessment techniques in planning for and responding to infrastructure failure events.

6. Conclusion

This research applies network analysis methods to assess infrastructure robustness via failure simulations on a large urban road network. The findings inform scalable, transferable methods to evaluate and strengthen the robustness of critical infrastructure systems. Network analysis techniques based on centrality metrics effectively identify critical nodes whose failure would most significantly impact network robustness. Targeted removal strategies prove more effective than random failures in simulating network collapse. Dynamic reprioritization of node criticality during failure simulations enhances accuracy in robustness assessment. Thus, the integration of dynamic dismantling strategies has promise to more accurately simulate cascading failures. The full version of the network under random failure has the slowest rate of collapse, which can be attributed to the presence of degree two nodes and their role in network robustness. Model simplification by removing sequential degree two nodes improves computational efficiency without compromising accuracy.

The network analysis methods of this study focused on topology to quantify the criticality of network nodes, but future work can additionally assess the network edges. Although no weighting was applied to the graph in this study, future work can use GIS feature class attributes to apply weighting to the network nodes and edges. Weighting on network nodes and edges can be based on road width or service demand. This weighting can provide particular insights on critical system assets. Future road network models can incorporate the underlying traffic flow patterns in the roadways. Consideration of traffic direction and physical constraints can dictate impacts from system failures.

The limitations of this study include the topological focus with unweighted and undirected graphs that do not account for traffic directionality or flow dynamics. The network model is synthetic such that the results may not directly reflect real-world infrastructure performance. The topological focus omits considerations of physical infrastructure attributes and operational conditions that can influence actual robustness. The simplified model ommitting sequential degree two nodes may not capture all relevant features of actual infrastructure systems. The failure simulations assume independent node failures without cascading effects that can occur in actual infrastructure systems. Incorporating specific attack patterns of certain hazards such as earthquakes and wildfires could enhance the realism of the failure event simulations.

Future integration of system dynamics into the network can provide more insight on how the systems would likely respond to unexpected events. The methods of this study demonstrate practical means to define the upper and lower bounds of infrastructure robustness, with actual system per-

formance likely falling between these extremes. The topological basis of this study has potential to extend across multiple network types and to different cities for streamlined and coordinated infrastructure robustness assessment. The methods of this study can be applied to other infrastructure systems such as water distribution, power grids, and communication networks. The application of these to methods to multiple system types within a city can identify overlapping critical service corridors, provide insights on the interdependencies between different infrastructure systems, and allow for coordinated strategic infrastructure planning. As topology is the most fundamental and readily available data for infrastructure networks, almost any city can apply the methods of this study to a wide range of infrastructure system types for capital improvement planning. Additional studies on other infrastructure systems and across different cities can prove the feasibility of these methods for widespread robustness assessment.

References

(2025a). NetworKit. https://networkit.github.io/.

(2025b). NetworkX. https://networkx.org/.

(2025, November). Street Network Database SND.

Albert, R., H. Jeong, and A.-L. Barabási (2000, July). Error and attack tolerance of complex networks. *Nature 406*(6794), 378–382.

Artime, O., M. Grassia, M. De Domenico, J. Gleeson, H. A. Makse, G. Mangioni, M. Perc, and F. Radicchi (2024, January). Robustness and resilience of complex networks | Nature Reviews Physics.

Callaway, D. S., M. E. J. Newman, S. H. Strogatz, and D. J. Watts (2000, December). Network Robustness and Fragility: Percolation on Random Graphs. *Phys. Rev. Lett. 85*(25), 5468–5471.

Cohen, R., K. Erez, D. ben-Avraham, and S. Havlin (2001, April). Breakdown of the Internet under Intentional Attack. *Phys. Rev. Lett. 86*(16), 3682–3685.

Dunn, S. and S. M. Wilkinson (2013, June). Identifying Critical Components in Infrastructure Networks Using Network Topology. *Journal of Infrastructure Systems 19*(2), 157–165.

Erath, A., J. Birdsall, K. W. Axhausen, and R. Hajdin (2009, January). Vulnerability Assessment Methodology for Swiss Road Network. *Transportation Research Record 2137*(1), 118–126.

Freeman, L. C. (1977). A Set of Measures of Centrality Based on Betweenness. *Sociometry 40*(1), 35–41.

Freeman, L. C. (1978, January). Centrality in social networks conceptual clarification. *Social Networks 1*(3), 215–239.

Haselkorn, M., S. Yancey, and S. Savelli (2018, February). Coordinated Traffic Incident and Congestion Management (TIM-CM) : Mitigating Regional Impacts of Major Traffic Incidents in the Seattle I-5 Corridor. https://rosap.ntl.bts.gov.

Kulkarni, T. (2020, January). Leveraging digital infrastructure and data management systems for water infrastructure emergency response planning. *International Journal of Multidisciplinary Research and Growth Evaluation 1*, 56–62.

Mintoo, A. A., A. S. M. Saimon, M. M. Bakhsh, and M. Akter (2022, March). National Resilience Through AI-Driven Data Analytics And Cybersecurity For Real-Time Crisis Response And Infrastructure Protection. *American Journal of Scholarly Research and Innovation 1*(01), 137–169.

Morone, F. and H. A. Makse (2015, August). Influence maximization in complex networks through optimal percolation. *Nature 524*(7563), 65–68.

Rodrigues, F. A. (2019). Network Centrality: An Introduction. In E. E. N. Macau (Ed.), *A Mathematical Modeling Approach from Nonlinear Dynamics to Complex Systems*, pp. 177–196. Cham: Springer International Publishing.

Wang, S., W. Lv, L. Zhao, S. Nie, and H. E. Stanley (2019, June). Structural and functional robustness of networked critical infrastructure systems under different failure scenarios. *Physica A: Statistical Mechanics and its Applications 523*, 476–487.