# Structural and Resilience Analysis of the German Transmission Network

Project for Statistical Analysis for Network Data course

Patrick Poetto, Goar Shaboian

2024-06-12

## 1 Critical Role of Grid Resilience in Safety

Power grid networks are among the most critical infrastructures that a country has to manage. They facilitate the generation, transmission, and distribution of electricity to the final consumers. These kind of networks are composed of interconnected components such as power plants, transformers, transmission lines, substations, and distribution systems. The robustness and reliability of power grids against possible disrupting events are vital for the stability of modern societies, as they power homes, industries, hospitals, and any essential services.

As already mentioned, a typical power grid is divided into three main segments:

1. **Generation**: This involves power plants that generate electricity from various sources, including fossil fuels, nuclear power, and renewable energy sources like wind and solar.
2. **Transmission**: High-voltage transmission lines carry electricity over long distances from power plants to substations. These lines are designed to minimize power losses and ensure efficient energy transfer.
3. **Distribution**: The distribution network delivers electricity from substations to end-users. This network operates at lower voltages and involves numerous localized systems.

Power grids are exposed to numerous challenges, including aging infrastructure, increasing demand, integration of renewable energy sources, and cybersecurity threats. Among these, the resilience of power grids to targeted attacks is a growing concern. Targeted attacks on power grids can have devastating consequences, leading to widespread blackouts, economic losses, which may be considered as threats to national security if the disrupting event is deliberately conducted. In such a context, power grid resilience refers to the ability of the network to withstand, adapt to, and recover from disruptions. Analyzing the resilience of power grid networks, particularly against targeted attacks, involves understanding how different components of the network are interconnected and how their failure impacts the overall system. This type of analysis is crucial for designing strategies to enhance the robustness of power grids.

The primary objective of the present project is to analyze the resilience of power grid networks under targeted attacks. Specifically that is:

1. Identify critical nodes and links within the power grid network whose failure could lead to significant disruptions.
2. Evaluate the impact of targeted attacks on the stability and functionality of the power grid.
3. Propose strategies to enhance the resilience of the power grid network against such attacks.

To achieve these objectives, the project will employ network statistical analysis to assess the vulnerabilities of the European power grid network. The findings will help in formulating effective mitigation strategies to safeguard power grid networks against potential targeted attacks.

## 2 Dataset description

As discussed, investigating the effects of policies on electricity transmission systems is a critical and complex issue that requires a thorough approach. One major challenge is ensuring that these policies are publicly and widely accepted, which necessitates transparency in both the research and decision-making processes (Medjroubi et al. (2017)). However, models and data in the power grid field are often not publicly available, which impedes the evaluation of existing models and approaches, thereby affecting the reproducibility of results. The lack of accessible data is due to security concerns and the sensitivity of the information, as such data could be exploited for malicious purposes, such as disrupting operations. Some agencies release local country-specific data, however, they are often not geo-referenced, which limits the conclusions that can be drawn by analysing the data (Medjroubi et al. (2017)).

An attempt to address this problem was made by SciGRID project launched in Germany and funded by the German Federal Ministry of Education and Research, which was created for the purpose of developing automated generation of models of power grids for the purposes of research and practical applications. The area of interest for this project were the European transmission networks, with a specific focus on German systems. The authors of the project noted that the absence of scientific discourse regarding the underlying methods, processes, and outcomes suggests that there is limited opportunity for learning and skill development in constructing electrical grid models (Matke, Medjroubi, and Kleinhans (2016)). As an attempt to solve this problem, a publicly available dataset (collected at the 18.07.2016 date) comprising transmission networks of a list of European countries.

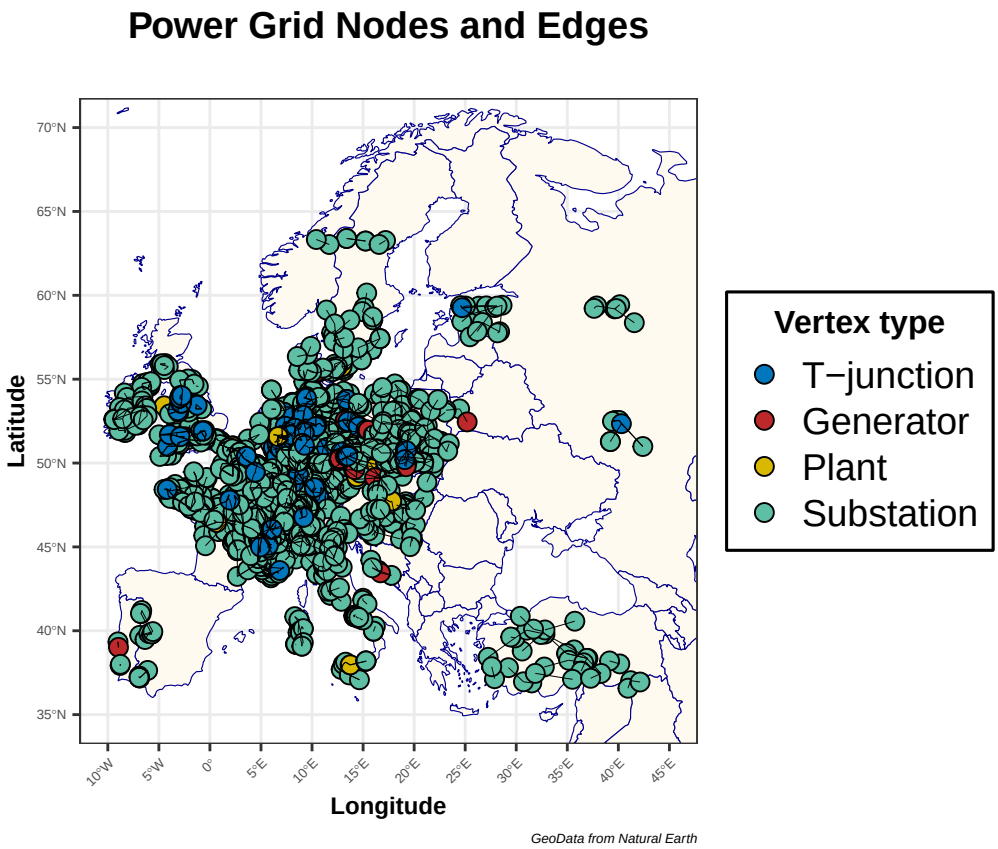


Figure 1: SciGRID: European transmission network

The automated model created by SciGRID relied on data made available by the OpenStreetMap project under the Open Database License. OpenStreetMap, an open-source voluntary project that aims at providing accessible and free geographic information. It is a leader in the field of the Volunteeered Geographic

Information, and provides not only maps, but also a system of softaware, tools and applications, as well as thorough and exhaustive documentation of data collection and processing (Mooney, Minghini, et al. (2017)). It is a reliable source of information, used widely in practical applications and research (Jokar Arsanjani et al. (2015)), with regularly provided updates and checks performed by the community of contributors.

Power information in OpenStreetMap generally details individual structures, like overhead power lines and nuclear power plants, with the exception of Germany, where 'power route' objects have been well-documented as a widely accepted standard. Those objects are rarely found outside of Germany (Wiegmans (2016)), hence this analysis will be limited to investigating the structure of the transmission network in Germany, with the possibility to extend the results to a wider geographical locations remaining a future possibility.

The data provided is freely available, with thorough documentation provided on the methods of data collection, processing and abstraction. The transmission network components that were included under the **power** category of the *openstreetmap* database were defined and included in the **SciGRID** dataset in an automatised fashion.

The dataset provides network data, including nodes (vertices) and links (edges). The **nodes** provided in SciGRID are electrical substations, which are represented in the OpenStreetMap topology by objects 'substation', 'stations' 'plants' and 'generators'. Those OMS relations are investigated, with relations representing incomplete electrical circuits excluded. Objects with 3 substations and a T-junction (where a transmission line branches out in two lines) are included in the SciGRID dataset by thoroughly investigating all nodes that are associated with 3 or more transition lines, and then confirming the type of the object by checking the start and end of the connection lines for each of 3 segments.

The **substation** category represents a facility that controls the flow of electricity, with the sizes of the substations varying significantly. They generally contain one or more transformers that can change the voltage. **Plants** refer to large-scale industrial facilities that generate more than 1MW of power, and they might also be used for energy *storage*. **Generators** refer to objects that create power, but on a smaller scale than **plants**, and they might include objects such as solar panels, micro-hydro and wind turbins that are typically stand-alone structures ("OpenStreetMap Wiki" (2023)).

The **edges** recorded in the dataset represent the transmission lines that connect the power relations. The edges recorded do not strictly follow the actual paths of the transmission lines, but an abstraction is introduced that involves recording edges as simple links between the vertices. The authors underline the fact that, in case of necessity, conserving the geographic information is straightforward (Matke, Medjroubi, and Kleinhans (2016)). In this way, each edge denotes a direct link between two substations, indicating the pathway through which power flows from one point to another within the network.

Another abstraction involved in the data collection process involves recording the vertices as geographical centres of substations that are members of the OMS power relation.

The validation of the collected data was performed by comparing the outcomes of the generated map to the maps made available by the European Network of Transmission System Operators for Electricity. Also, the GridKit project, which was also aimed at generating power transmission maps based on the OSM data, implemented a different approach to data collection in that the network topology derivation relied on the spatial data in OpenStreetMap through heuristic assumptions and extensive data processing rather than on the human-authored *"power routes"*, with the results demonstrating relative coherence in the "relative completeness" metric between the two approached when applied to Germany.

# 3 Preliminary steps

The dataset was accessed from the SciGRID website, with separate files for vertices and edges available.

Since the data concerns a geographic region, it is of interest to include in the analysis some information on the spatial structure of the analysed region, hence the map of administrative regions of Germany was retrieved in order to conduct comprehensive analysis.

```
## Reading layer `1_sehr_hoch.geo' from data source
```

```
##   `C:\Users\goars\LM Data Analytics\networks\project\project_power_grids\1_sehr_hoch.geo.json'
##   using driver `GeoJSON'
## Simple feature collection with 40 features and 11 fields
## Geometry type: MULTIPOLYGON
## Dimension:     XY
## Bounding box:  xmin: 5.871619 ymin: 47.26986 xmax: 15.03811 ymax: 55.05653
## Geodetic CRS:  WGS 84
```

In the dataset, 3 duplicated vertices were included, as well as several vertices that are geographically located outside the country of Germany, thus, data cleaning procedure was implemented in order to remove the mentioned nodes.

The graph for the transmission network was created using *igraph* package, with attributes for edges and vertices included in the graph structure. Additionally, duplicated edges were removed for the further analysis.

```
power_network <-  graph_from_data_frame (edges, vertices,directed = FALSE)
power_network <- igraph::simplify(power_network)
```

SciGRID: German transmission network

The obtain graph is visualised in the *Figure 3*, with the transmission nodes and the recorded links between them depicted on the map of Germany. The plot allows to distinguish between «WHAT ATTRIBUTES???>.

### 3.1 Network cohesion

The network cohesion was investigated to determine if the network is **disconnected**, with the **maximally connected subgraphs** determined by graph decomposition.

```
## [1] FALSE
```

Table 1: Sizes of connected components

| Size of component | Frequency |
|---|---|
| 1 | 5 |
| 463 | 1 |

It is evident that there is one **giant component** that includes most of the nodes of the transmission network, and 5 **isolated nodes**. For further analysis, only the giant component was investigated since it represents the core structure of the network and is essential for understanding overall connectivity, information flow, and identifying key nodes or patterns that could significantly impact network behavior.

```
power_subgraph <- decompose (power_network)[[1]]
vcount (power_subgraph) /vcount (power_network) # .989
```

```
## [1] 0.9893162
```

The obtained network includes almost 99% of the nodes from the initial transmission network, which implies that there was no noticeable loss of information caused.

## 4 Descriptive statistics - centrality measures

Centrality measures are fundamental in network analysis, providing insights into the characteristics and functional dynamics of complex networks. These measures are pivotal for identifying the most influential or significant nodes within a network, thereby elucidating the roles and positions of various entities in relational contexts. By quantifying the prominence of nodes based on different criteria, centrality measures enable to lok for patterns of connectivity and interaction, which are essential for understanding the overall topology of the network.

## 4.1 Degree distribution

The **node degree distribution** is an essential characteristic of the network that provides information on the static situation of the network: it describes the frequency of each degree within the network, highlighting the connectivity pattern among nodes. A degree distribution can indicate whether a network follows a uniform, random, or scale-free topology. Analyzing this distribution helps identify key nodes with high connectivity, which can be crucial for understanding the robustness and vulnerability of the network. Furthermore, it provides insights into the potential efficiency and resilience of the network under various conditions.

The degree centrality is computed just as:

$$C_D(v) = \deg(v)$$

In this formula, $\deg(v)$ represents the degree of node $v$, which is the number of edges connected to $v$.

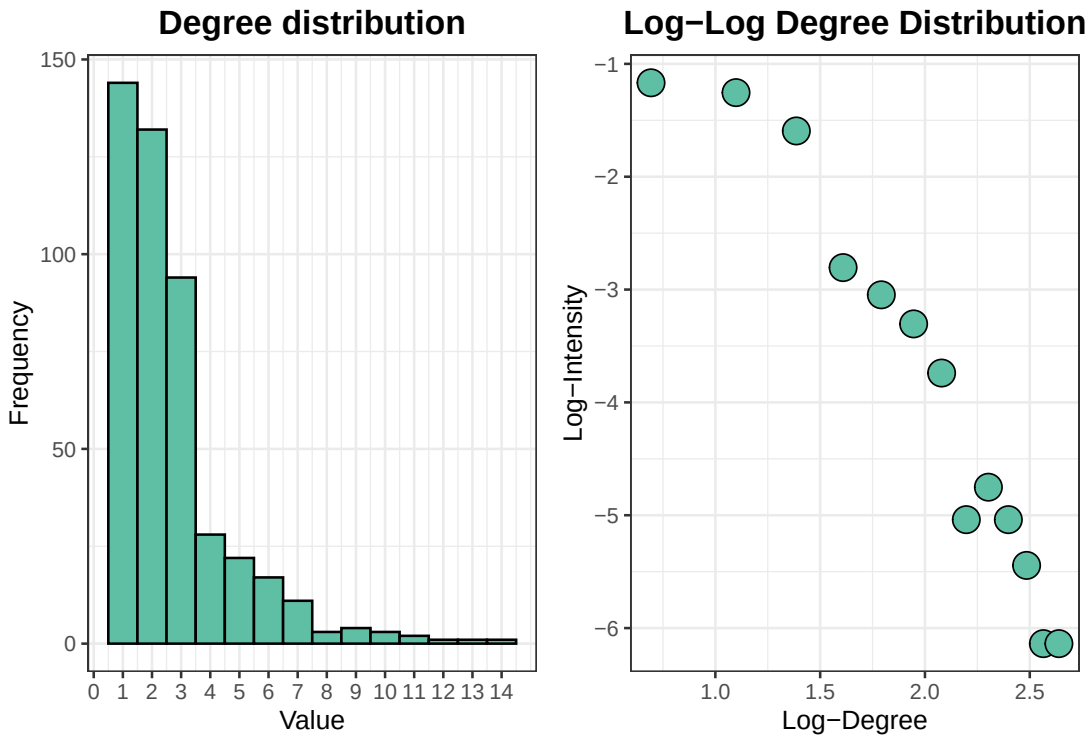


Figure 2: Degree distribution and the log-log degree distribution for the transmission network

The plots provide insight into the degree distribution and potential scale-free nature of the network.

Degree Distribution (Left Plot):

- **Observation**:
  - Skewed right, most nodes have a low degree.
  - Highest frequency at degree 1 and 2.
  - Fewer nodes with higher degrees; frequency decreases significantly with higher degrees.
  - Typical of power-law distribution or scale-free networks.

Log-Log Degree Distribution (Right Plot): - **Observation**: - Roughly linear trend in log-log scale. - Indicates degree distribution follows a power-law. - Supports the scale-free network hypothesis with few highly connected hubs.

Key Insights: - **Network Structure**: Likely scale-free with a few hubs and many low-degree nodes. - **Hub Nodes**: Important in the network, indicating high influence or control points. - **Robustness and Vulnerability**: Robust to random failures but vulnerable to targeted attacks on hubs. - **Real-World Implications**: Common in social networks, the internet, and biological networks.

Overall, these plots suggest a scale-free network with a power-law degree distribution, highlighting crucial aspects of its topology and behavior.

The degree distribution of the analysed network is highly skewed, with most of the transmission networks having low degree (2), and significantly fewer high-degree nodes.

It is also of interest to investigate the average degree of neighbors for the vertices, since it will allow to gain insight into the possible connection that exist between vertices of different degrees.

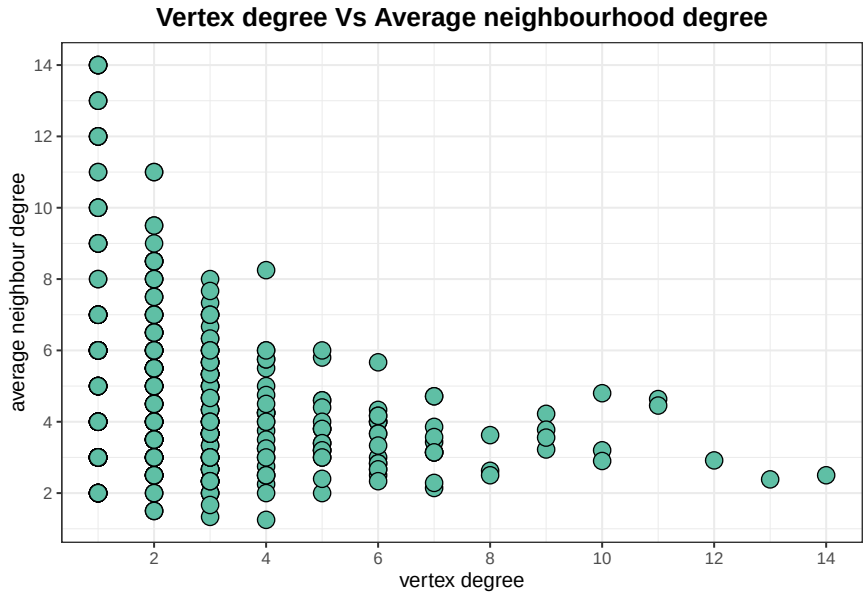


Figure 3: Scatterplot for the degree distribution of the nodes with respect to the degree distributions of the neighbouring nodes

*Figure 3* demonstrates that the nodes with high degree do not link with other nodes with high degrees, instead the trend that vertices with degrees higher than 7 do not link with vertices that have degrees 10 or higher. This observation allows to make a preliminary suggestion that the possible 'hubs' are not directly connected to each other.

- **Observation**:
  - Generally, lower-degree vertices tend to have neighbors with higher average degrees.
  - As vertex degree increases, the average neighborhood degree tends to decrease.
  - This trend suggests that high-degree nodes are often connected to low-degree nodes, indicative of a disassortative mixing pattern.

Key Insights: - **Network Structure**: The negative correlation between vertex degree and average neighborhood degree. - **Disassortative Mixing**: High-degree nodes tend to connect with low-degree nodes, a common trait in many real-world networks like the internet. - **Implications**: This pattern affects the robustness and dynamics of the network, influencing things like spread of information or resilience to attacks.

Overall, the plot highlights a disassortative mixing pattern in the network, where high-degree nodes prefer connections with low-degree nodes.

## 4.2 Closeness and betweenness distributions

The closeness centrality distribution represents the frequency of nodes based on their closeness centrality scores, which measure how quickly a node can reach all other nodes in the network. Analyzing this distribution helps identify nodes that have the shortest average path length to all other nodes, indicating their efficiency in information dissemination or resource access within the network. The closeness centrality is computed as:

$$C_C(v) = \frac{1}{\sum_{u \neq v} d(v,u)}$$

Where, $C_C(v)$ is the closeness centrality of node $v$, $d(v,u)$ is the shortest path distance between nodes $v$ and $u$.

The betweenness distribution represents the frequency of nodes based on their betweenness centrality, indicating how often nodes act as intermediaries in the shortest paths between other nodes. Analyzing this distribution helps in identifying nodes that play crucial roles in facilitating communication and connectivity within the network, basically bridges and bottlenecks which control the flow of information.

The between centrality measure is computed as:

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

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

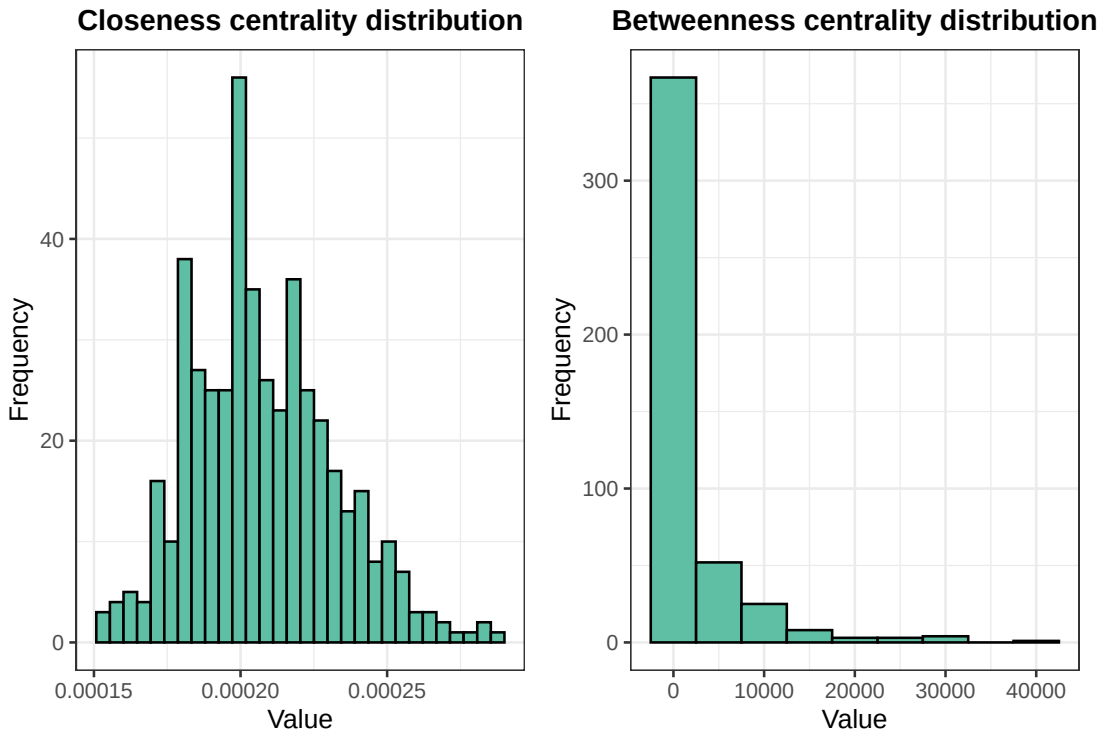


Figure 4: Distributions of the closeness and betweenness centralities

Spatial embeddedness and planarity of urban infrastructure networks limit the range of their node degree values. In principle indeed a power grid should show a hierarchical structure where a few critical distribution

nodes have very high degree, while generation nodes should show low degree (i.e. a plant is connected to a transformer/substation) and the global topology, speficically on a nationwide scale, is composed by a grid of the longest possible transmission lines, in order to preserve efficiency during the transmission itself. Therefore, pursuing analysis based on the distribution of node degrees e.g. scale free aspect could not be accomplished in such networks. This kind of network though is unsurprisingly characterized by some power law distribution in betweenness centrality. Thus, scale free aspect could be observed in the betweenness centrality distribution.

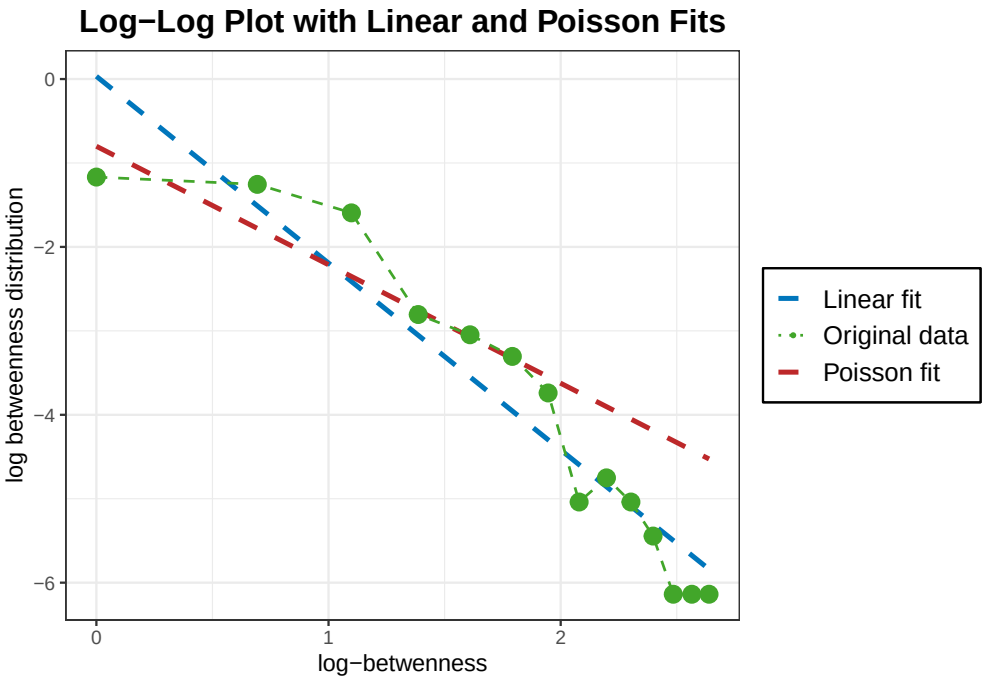


Figure 5: Linear and Poisson Fits for betweenness centrality distribution

The analysis have displayed a decently well behaved fit both for the linear and the Poisson models but the linear model seems to have better catched the overall shape of the original data.

### 4.3 Eigenvector centrality and clustering coefficients

The eigenvector centrality distribution captures the frequency of nodes based on their eigenvector centrality scores, reflecting the influence of each vertex not only by their direct connections but also by the importance of their neighbors. Analyzing this distribution helps identify the most influential nodes in terms of their overall connectivity and the centrality of their neighbors.

The clustering coefficient distribution shows instead the frequency of nodes based on their clustering coefficient values, indicating the tendency of nodes to form tightly knit groups or clusters. This distribution provides insights into the network's local cohesiveness and the prevalence of subgraph structures. The eigenvector centrality is computed as:

$$C_E(v) = \frac{1}{\lambda} \sum_{u \in N(v)} A_{uv} C_E(u)$$

Where $C_E(v)$ is the eigenvector centrality of node $v$, $\lambda$ is the largest eigenvalue of the adjacency matrix $A$, $N(v)$ is the set of neighbors of $v$, $A_{uv}$ is the element of the adjacency matrix indicating the presence (1) or absence (0) of an edge between nodes $u$ and $v$.

The clustering coefficents instead are computed as:

$$C(v) = \frac{2e_v}{k_v(k_v - 1)}$$

Where, $C(v)$ is the clustering coefficient of node $v$, $e_v$ is the number of edges between the neighbors of node $v$, $k_v$ is the degree of node $v$, which is the number of neighbors of $v$.

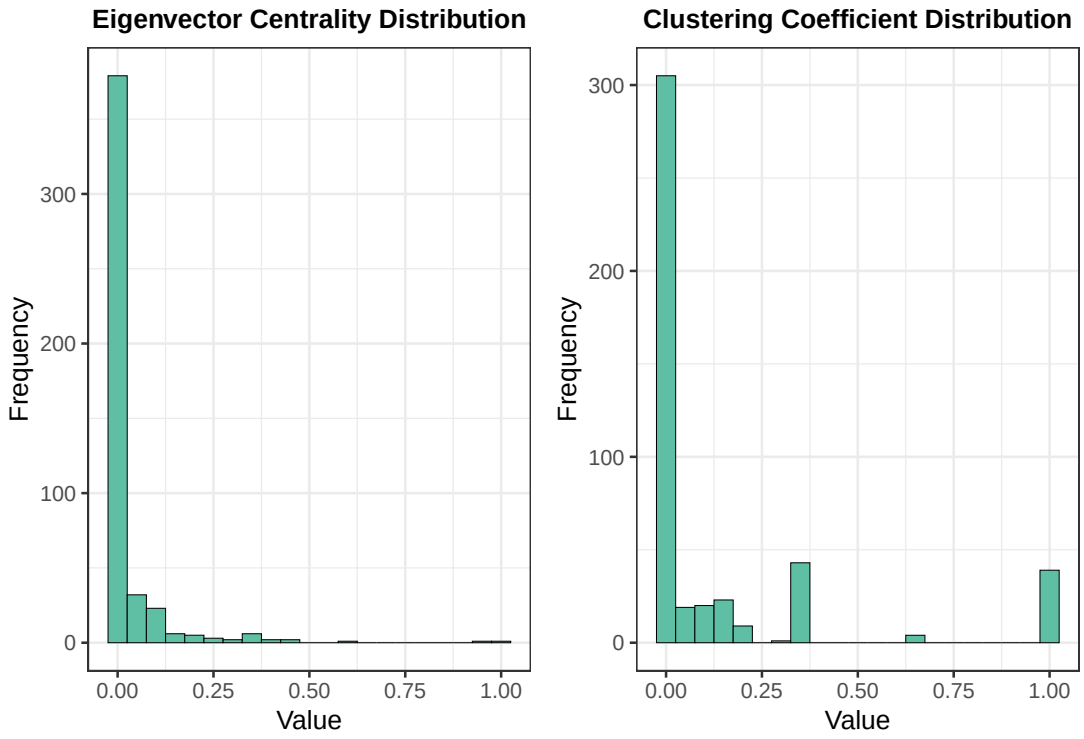


Figure 6: Distributions of the eigenvecotr centrality and the local clustering coefficients

## 4.4 Preliminary conclusion on centralities results

Before conducting a more in depth resilience analysis for targeted attacks prevention some preliminary conclusion may be assessed based on the topology features that the study of descriptive statistics has enlighted. It's useful to anticipate that when the proper analysis will be conducted, it will consist on an iterative procedure of identification of critical points which, if disrupted, would bring down the biggest possible network component. This is procedure is similar, rather quite refined, but iterative, meaning that once a node is brought down the computation is repeated on the main component that's left, in order to consistently identify the set containing the most critical nodes.

The descriptive plots actually show a weakly connected situation. The network looks quite sparse based on the degree distribution which highlights that most vertices have very low degree, quickly descending as the degrees increase, meaning that very few nodes have a high number of connections. Although a potential scale-free property on the node degree distribution has been previously hypotesized, a proper analysis showed no evidence in this direction. The degree against average neighbourhood degree number also shows that nodes with high degree tend to have a low average degree in their neighbourhood, that is the nodes they're connected to, suggesting a lack of strongly connected clusters.

Base on the betweenness this kind of sparseness tendence seems to be confirmed. Most nodes have a very low score, meaning that the network has very few interconnecting intermediators, on the countrary it presents several bottlenecks. Notice that the beetweeness seems to fit quite well the scale free property. The closeness

measure instead is somehow bell-shaped meaning the efficiency of nodes in providing a way from one node to another is globally kind of Normal. Eventually, eigenvector and clustering coefficient centralities confirm the sparseness. They have a very similar distribution, the clustering coefficients having a much fatter tail. This provides some evidence that even evaluating nodes as being influenced by their neighbourhood, the network shows rare to not at all cohesion

Based on this information, a very preliminary experiment aimed at identify critical nodes may be conducted by choosing a thresholds based intersection between all these metrics, retrieving only nodes that have the strongest centrality features.

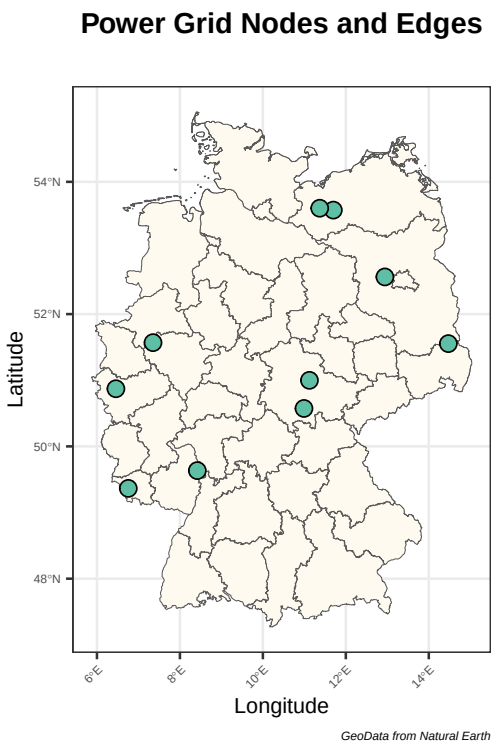


Figure 7: Spatial allocations of the nodes with strongest centrality features

## 4.5 Community detection

Graph partitioning is a fundamental technique in network analysis used to identify substructures or communities within a larger network. This approach can allow to reveal densely connected subgraphs and critical nodes that maintain overall connectivity. This type of analysis is crucial for understanding the organization of the network, which can have significant implications for its resilience and robustness.

By partitioning the network, we can identify key clusters that may represent critical components or regions within the power grid. This allows us to assess how disruptions in one part of the network might propagate and affect other areas, thereby providing insights into potential vulnerabilities. Additionally, graph partitioning helps in optimizing network maintenance and expansion strategies by highlighting which sections of the network are most critical for stability and efficiency. Therefore, employing graph partitioning in this report not only aids in the detailed understanding of the network's structural properties but also enhances our ability to design targeted interventions to improve the resilience of the transmission system.

Graph partitioning procedure allows to identify clusters of nodes that are similar between each other, but are dissimilar from the other nodes. A clustering procedure was implemented that relies on optimising a *modularity score*, which compares the concentration of links between groups of nodes compared to what

would be expected if the edges were assigned at random (or, if where there is degree heterogeneity but no community structure).

At each iteration, nodes are added to the community in a way such that the modularity score of the community is increased, until no improvements are observed. The implemented strategy focuses on local improvements, which has a drawback of possibly missing the globally optial solution, but has the advantage of computational efficiency due to the greediness of the implementation, which is especially beneficial for large networks.

As the result of the clustering procedure, 15 clusters were determined in the transmission network. **Validation** of the graph partitioning was performed by investigating the spatial structure of the obtained clusters.

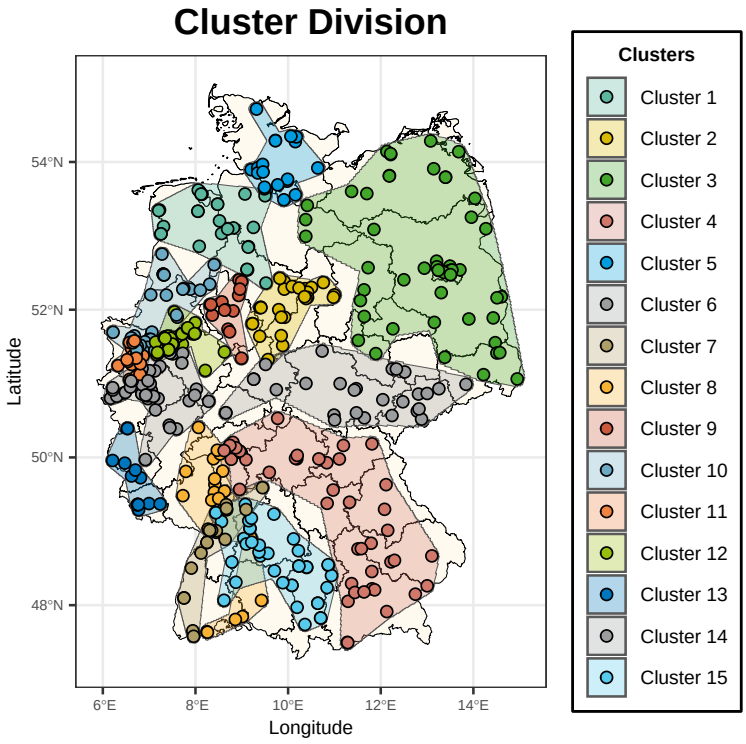


Figure 8: Spatial allocation for the nodes membership based on Fast and Greedy clustering procedure

As evidenced by *Figure 8*, the nodes in the network are clustered into similar well-connected groups according to their geographical locations. It is possible to observe that there are more heterogeneous groups formed in the more industrial and densely populated area in the west of Germany, while, for less populated areas, the transmission network nodes form larger structures. This observation is important for the purposes of understanding the possible underlying structure of connectivity in the analysed network.

# 5 Vulnerability analysis

Detecting potential vulnerabilities in the network structure of power grids is of utmost importance due to the significant risks involved. An attack on a country's power grid system can lead to severe consequences, such as widespread blackouts, economic disruption, and compromised public safety (Cetinay, Devriendt, and Van Mieghem (2018)). In addition to the chance of unexpected power failures or manufacturing defects, it is essential to also consider the ongoing risk of targeted attacks on the electricity transmission network. These attacks aim to exploit weaknesses in the network, potentially causing disruptions in power supply, economic instability, and threats to public safety.

Hence, it is important to perform resilience analysis in order to determine possible weak points of the

transmission network, which could allow to anticipate possible disasters, as well as aid in further decision making process.

The effects of the attacks on the transmission network can be assessed using different metrics, among which are the size of the largest components or its capacity. In this analysis, the size of the component will be used as a proxy for the resilience of the network, since it can help gain insight into the magnitude of the disruption that was caused.

The possibility of **random attacks** is investigated, where the nodes that are removed from the network are chosen randomly, Since this approach will not produce results invariant to permutations, Monte Carlo simulations are used in order to reduce the uncertainty associated with running the experiment.

Additionally, the possibility of **targeted attacks** is investigated: this approach implies that the most *important* nodes in the network will be targeted initially, such that the most disruption can be caused while utilising least resources. The importance of the node is defined according to the different **centrality** metrics that were discussed above. By assessing the consequences of each attack strategy, it will be possible to draw conclusions on which centrality characterises the *importance* of the vertices best.

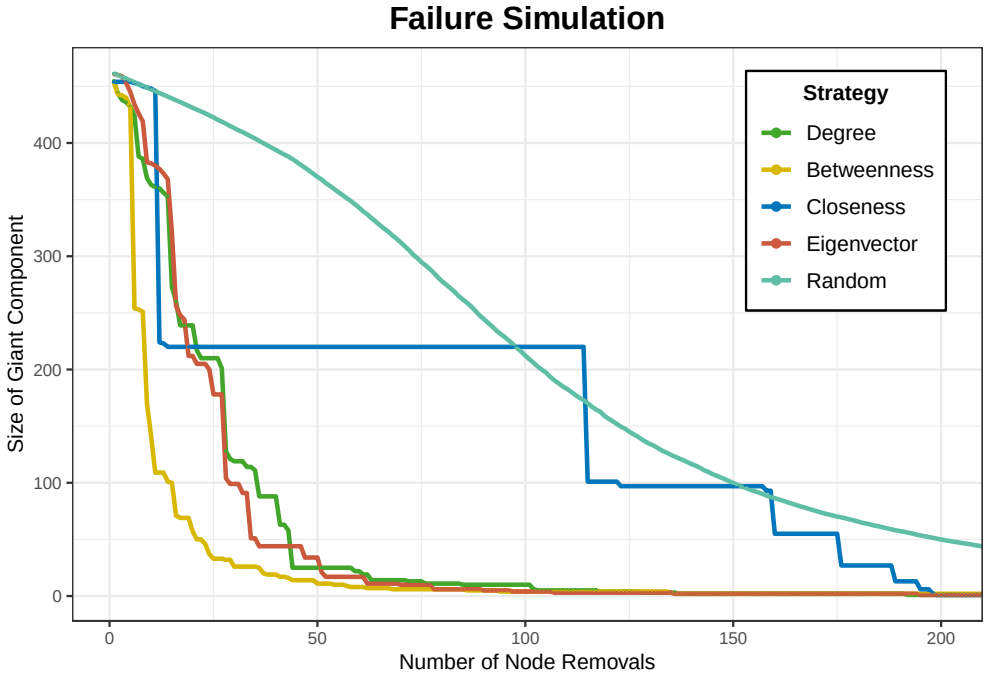


Figure 9: Consequences of implementing different attack strategies on the transmission network

*Figure 9* allows to compare the effects of the implemented strategies on the transmission network. It is evident that **random** attack does not provide significant disruptions to the transmission network, giving evidence of its relative robustness to natural disasters.

Implementing strategy based on the **closeness** centrality leads to significant damage in the beginning of the attack, with decreasing the size of the giant component in half while removing only 11 nodes, while further damages are very ineffective and, at some points, are similar to the random attack consequences.

Using **eigenvector** and **degree** centralities provide quite similar results,

The degree centrality provides information on the structure of the network in the nearest proximity of the node, which is not necessarily a proper representation of the centrality of a node in the full network.

The **betweenness** attacks providing fastest drop in the giant component size, hence providing the most efficient attack strategy with the least amount of resources used. By incorporating information on the number

of the shortest paths passing through each vertex, this centrality measure provides information on the global network structure, thus explaining the efficiency of using this metric in the attack strategy.

Investigation into which nodes are removed to achieve the disruption to the size of giant component equal to 100 is conducted for the 2 most efficient strategies, in order to determine if there are possible trends that explain their importance.

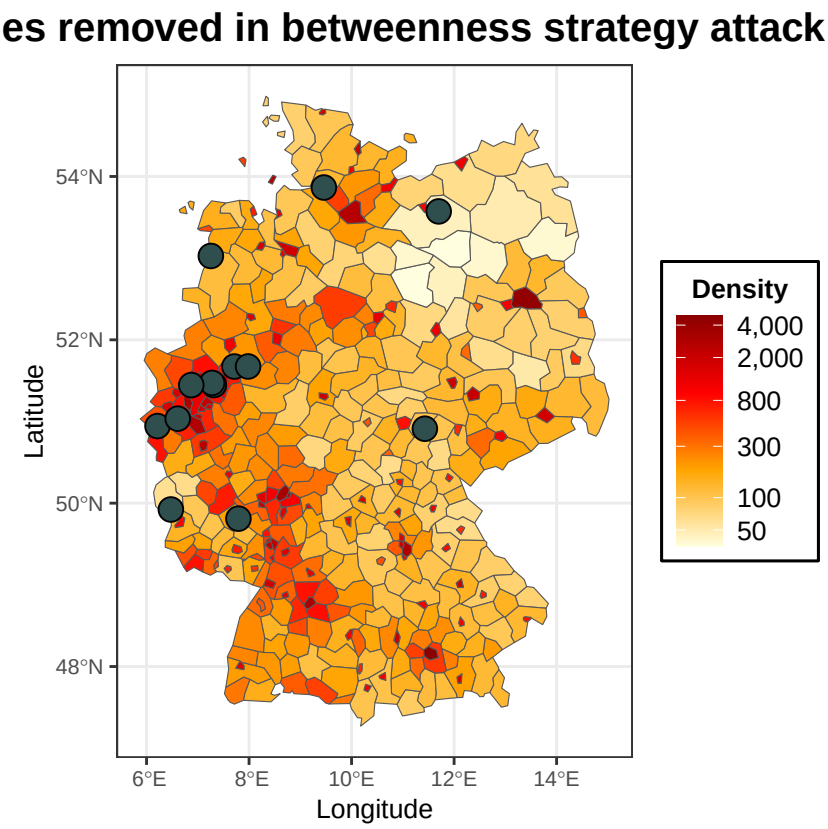


Figure 10: Consequences of implementing different attack strategies on the transmission network

*Figure 10* provides compelling evidence that the impact of node removal on network disruption varies significantly based on population density. In densely populated areas, the infrastructure and key nodes appear to be more robust, requiring the removal of multiple nodes to achieve substantial disruption. This resilience is likely due to higher connectivity and redundancy in densely populated networks, which are designed to withstand multiple failures. Conversely, in sparsely populated areas, the removal of even one or two nodes causes considerable disruption to the transmission network. This observation underscores the critical role of these nodes in maintaining network integrity within less densely connected regions. The vulnerability of such networks to single-node failures highlights the importance of strategic node placement and robust network planning, particularly in areas with lower population density where network resources may be more limited.

# 6 Conclusions

The German transmission network, characterized by a scale-free topology, exhibits a structure where a few highly connected hubs coexist with numerous sparsely connected nodes. This configuration makes the network robust to random failures but highly vulnerable to targeted attacks on critical nodes. Resilience analysis underscores the importance of protecting high-betweenness nodes to maintain network integrity against deliberate disruptions. This highlights the necessity for strategic reinforcement and robust network planning,

especially concerning nodes with high connectivity and criticality.

Furthermore, the critical role of nodes in less populated areas in maintaining overall network integrity cannot be overlooked. Strategic node placement and robust planning are essential to ensure resilience across the entire network. Extending the analysis to incorporate weighted graphs, which account for attributes of the edges, can provide deeper insights into the power flow within the transmission network. Additionally, expanding this work to cover larger geographical areas, given the availability of data, can further enhance understanding and resilience planning for the transmission network.

# References


Cetinay, Hale, Karel Devriendt, and Piet Van Mieghem. 2018. "Nodal Vulnerability to Targeted Attacks in Power Grids." *Applied Network Science* 3: 1–19.

Jokar Arsanjani, Jamal, Alexander Zipf, Peter Mooney, and Marco Helbich. 2015. "An Introduction to OpenStreetMap in Geographic Information Science: Experiences, Research, and Applications." *OpenStreetMap in GIScience: Experiences, Research, and Applications*, 1–15.

Matke, Carsten, Wided Medjroubi, and David Kleinhans. 2016. "SciGRID - An Open Source Reference Model for the European Transmission Network (V0.2)." http://www.scigrid.de.

Medjroubi, Wided, Ulf Philipp Müller, Malte Scharf, Carsten Matke, and David Kleinhans. 2017. "Open Data in Power Grid Modelling: New Approaches Towards Transparent Grid Models." *Energy Reports* 3: 14–21.

Mooney, Peter, Marco Minghini, et al. 2017. "A Review of OpenStreetMap Data." *Mapping and the Citizen Sensor*, 37–59.

"OpenStreetMap Wiki." 2023. https://wiki.openstreetmap.org/wiki/Key:power.

Wiegmans, Bart. 2016. "Improving the Topology of an Electric Network Model Based on Open Data." University of Groningen.