MASTER'S THESIS 2026

A Comparative Study of Edge Addition Algorithms for Power Grid Robustness

Sandra Christoffersen, Gina Christoffersen

ISSN 1650-2884
LU-CS-EX: 2026-36

DEPARTMENT OF COMPUTER SCIENCE
LTH | LUND UNIVERSITY

EXAMENSARBETE
Datavetenskap

LU-CS-EX: 2026-36

A Comparative Study of Edge Addition Algorithms for Power Grid Robustness

En jämförande studie av kanttilläggsalgoritmer för ökad robusthet i elnät

Sandra Christoffersen, Gina Christoffersen

A Comparative Study of Edge Addition Algorithms for Power Grid Robustness

Sandra Christoffersen
sandrachristoffersen00@gmail.com

Gina Christoffersen
gina.christoffersen@gmail.com

June 5, 2026

Master's thesis work carried out at
the Department of Computer Science, Lund University.

Supervisor: Jonas Skeppstedt, jonas.skeppstedt@cs.lth.se

Examiner: Flavius Gruian, flavius.gruian@cs.lth.se

Abstract

Power grid networks around the world face huge expansion plans as the demand for energy is expected to grow each year. One critical perspective when developing modern power grids is network robustness. Adding new transmission lines to improve robustness can be modeled as a graph optimization problem using edge addition algorithms. The objective functions to optimize are often topological and electrical robustness metrics. Two such metrics are effective graph resistance and algebraic connectivity, that mostly have been studied on synthetic IEEE test grids. Further research is needed to better understand the relationship between graph connectivity and robustness against cascading failures. In this study, three greedy edge addition algorithms were compared and evaluated under targeted attacks and cascading simulations on a realistic Nordic transmission model. The results indicated that both minimizing and maximizing algebraic connectivity can increase power grid robustness against cascading effects in certain attack scenarios. Minimizing effective resistance demonstrated varied robustness performances for different graph structures. Results also showed how the algorithms behaved differently depending on synthetic or realistic power grid data.

Keywords: Nordic power grid, Effective graph resistance, Algebraic connectivity, Robustness, Targeted attacks, Cascading failure

Acknowledgements

We would like to express our appreciation to our supervisor, Jonas Skeppstedt, for his guidance, feedback, and availability throughout the thesis process. His quick responses, even during weekends, supported the progress of this work.

We are also grateful to our parents for their encouragement and continuous support over the course of our education.

Finally, we would like to thank each other for the collaboration and hard work shared throughout this project. Writing our study together has been fun and memorable.

Contents

Chapter 1
Introduction

1.1 Context and Problem

Electricity is a fundamental part of modern society and is closely linked to economic growth. A stable energy source is critical for industrial and corporate development, as well as a greater willingness to invest. Therefore, power outages and power grid failures can be costly for business and human life [1]. There are many different causes for outages and power failures such as natural disasters, random failures or malicious attacks [2]. Both natural disasters such as flooding and storms, and random failures often cause local malfunctions, but this can trigger cascading events that can lead to more global outages [2, 3]. Targeted attacks by militants and terrorists often target the most vulnerable points to create maximum damage [4].

Power grid networks around the world require rebuilding and expansion as the electricity demand in society increases [5]. The growing demand for energy is mainly due to the energy transition of the industry and transport sectors, as well as an increased use of data centers. Sweden's transmission system operator Svenska kraftnät makes a similar assessment of the need to expand the power grid in their network development plan 2026 - 2035 [6]. The security of the energy supply in Sweden for the next ten years includes the addition of new transmission lines of around 2900 km [6].

There needs to be a bigger focus on robustness when developing modern power grids [5]. It is particularly relevant today, as some of the existing infrastructure approaches the end of its lifespan [5], in fact 45% of all investment in Svenska kraftnät's planned investments are allocated to an aging power grid [6]. It is also worth considering the current unstable political climate. For example, thus far in the Russian war against Ukraine, more than 50% of the Ukrainian power grid has been destroyed [7]. When rebuilding and expanding, many parameters must be taken into account, such as robustness, cost and geographic location. The power grid of Sweden is designed under the N-1 robustness criteria, meaning the failure of any one link will still ensure a secure supply of energy [8]. However, this is not sufficient for withstanding larger disturbances such as cascading failure and targeted attacks [8, 9].

A power grid network consists of a high voltage transmission network that transports electricity from power stations to local distribution networks. The high voltage transmission lines reduce energy losses such as heat loss and keep power constant. These can be either alternating current (AC) or direct current (DC) lines, depending on efficiency, distance or system requirements. Transformer stations transform the voltage and safely reduce it to medium and low voltage for the distribution network that supplies cities and industries [10]. In robustness studies, power grids are commonly modeled as a graph G = (V,E) [2, 11, 12]. Transmission lines and transformation stations are modeled as edges (E) because they connect two power stations (buses). Vertices (V) in the network such as generators and consumer points are called nodes or buses. The network has loads which are energy consummation from for example industries and households. The generators are energy production such as nuclear power and wind power. Not all nodes have power or demand and are simply transit nodes that facilitates power.

The problem of optimizing transmission expansion can be modeled with graph modifications such as adding edges [11, 13]. An edge addition algorithm can optimize a robustness metric with multiple constraints like budget of edges, economic and geographical constraints. Some approaches to optimizing the robustness of a graph focus on topological metrics, while others integrate electrical parameters to model real power flow or a combination of both [2]. Identifying the optimal edge to add is computationally heavy for large graphs with many constraints. Therefore, heuristic algorithms and approximations are often required, as many of the most common topology strategies are NP-hard [14]. Efforts to address a combination of all these factors are still an active research area, highlighting the need for further investigation into optimization of robustness and edge addition methods.

1.2 Addressing the Problem

Much has been studied in the field of network robustness and a range of metrics have been introduced. Two such metrics are effective graph resistance and algebraic connectivity, both related to graph structure. These can be used as objective functions when optimizing edge addition strategies. Effective graph resistance is associated with power flow distribution which can be an important aspect of robustness against cascading effects [15]. Algebraic connectivity indicates how well connected a network is and thus more difficult to disconnect under failures or attacks [16]. However, a highly connected network could also facilitate the propagation of overloads and cascading effects in power grids [13]. The complete relationship between connectivity and robustness against cascading failure in power grids appears to be less studied. The trade-off between preserving connectivity to prevent island formation with loads and no generation, while also wanting to decrease the risk of cascading failure could perhaps benefit from more research. Our thesis contributes to this area by further investigating the minimization and maximization of connectivity and flow-based metrics, to compare and evaluate with a different combination of topological and electrical robustness metrics and attack scenarios within the same framework. Effective graph resistance and algebraic connectivity were identified through a literature review of previous studies and selected for this report because they capture different network aspects that may affect the propagation of cascading failures differently. We therefore compare the following three edge addition algorithms:

1. Minimizing effective graph resistance
2. Minimizing algebraic connectivity
3. Maximizing algebraic connectivity

Furthermore, most studies on the topic of power grid robustness are performed on IEEE benchmark systems. These do not fully capture the real properties of power grids and therefore not the complexity of cascading events. This is due to synthetic data and lack of geographic information, resulting in all transmission lines being modeled with a uniform length of 1 kilometer [17]. In this study we use an IEEE test grid as well as the Nordic power grid, a larger and more realistic transmission model to reflect the complexity of electrical data and geographic locations. Our contribution is thus to highlight different properties of realistic and synthetic test grids. Evaluating robustness metrics and attack scenarios under more realistic conditions provide different insight into transmission planning.

In summary, three greedy edge addition algorithms were investigated and compared in regards to power grid robustness under constraints. Two types of node attacks were selected, degree node attack and electrical significant node attack. These strategies were chosen because they required different information of the grid, such as topological and electrical data, to simulate attackers with varying level of grid knowledge. We chose to focus on node attacks as removing a node also means that all its connected edges get deactivated, which has a larger structural impact on the network. This was then evaluated by two different robustness metrics, largest cluster size and served power demand. While one captures purely topological robustness, the other considers power flows and system function. We chose this combination of metrics because it allows the study of both the structure of the network and its ability to deliver electricity after an attack. It was done on an open source PyPSA realistic Nordic power grid model and a synthetic IEEE test grid. Our report attempts to answer the following research questions:

- RQ1: How do different edge addition algorithms differ in their ability to increase the robustness of electric power networks under budget constraint of edges?
- RQ2: Which of the edge addition algorithms is most suitable from a robustness perspective depending on the type of attack it is exposed to and the size of the graph?

The first research question addresses the problem of identifying an edge to add in regards to a robustness metric, effective graph resistance and algebraic connectivity. The second question aims to evaluate the algorithms through targeted attacks and cascading scenarios.

1.3 Contribution Statement

An important part of the research process consisted of an extensive literature review focused on selecting relevant robustness metrics, as well as suitable approximation methods and algorithms. The search effort was divided among both authors, where Gina focused on investigating power grid metrics and Sandra focused on analyzing different approaches. Together we aimed to identify gaps in the current research and motivate the methodological choices in our study.

An additional big part of the project consisted of creating a custom graph structure that directly interacts with the power flow calculation tool. It appeared to reduce computational overhead otherwise caused by repeated conversions between a graph library and the power system tool, as well as faster graph modifications. For this and for all of the project we used pair programming, frequently alternating roles between driver and navigator. This approach proved to be efficient for problem solving and allowed constant review of the code. Other implementations includes the algorithms, robustness metrics, attack strategies and the cascading simulation. Another significant part of the work consisted of constructing the Nordic power grid dataset from the open-source PyPSA framework. Together we modeled, converted and processed the Nordic power grid to fit the custom graph structure.

For the writing process, the workload was distributed equally. Gina was mainly responsible for writing the sections describing the robustness metrics, DC power flow and cascading simulation. Sandra was mainly responsible for writing the sections describing the datasets, attack strategies and network preliminaries. We both contributed to writing about the algorithms and experimental set up. We were both responsible for conducting the simulations and generating the experimental results. The result and discussion sections were therefore produced together. Throughout the study we collaborated and discussed topics between us when writing the report and reviewed and edited all sections together.

1.4 Report Outline

The report is structured as follows. Chapter 2 introduces edge addition algorithms, robustness metrics and attack methods. Chapter 3 explains the experimental methodology for cascading simulation and data processing. Chapter 4 presents the results and robustness evaluation of adding transmission lines to power grids. Chapters 5 and 6 discuss the results and conclude the study.

Chapter 2
Background

The expansion of power grids presents a complex challenge. It requires considering both topological and electrical aspects, failure scenarios, and multiple constraints such as budget of edges and geographical locations. This chapter covers the necessary concepts to understand the problem and methodological approach to add new transmission lines to a power grid. Table 2.1 gives an overview of the terminology needed for a graph representation of the problem.

Terminology

Term	Graph model
Power grid	A set of electrical stations connected by transmission lines, modeled as a graph.
Graph	A set of nodes connected by edges.
Bus	A node in a power grid modeling generators, loads and connections between transmission lines.
Transmission line	Modeled as an edge connecting two buses.
Transformer	Modeled as an edge connecting two buses with different voltages.
Generator	Modeled as a node in a graph.
Load	Modeled as a node in a graph.

Table 2.1: Terminology used throughout the study.

2.1 Network Preliminaries

A power grid can be modeled as an undirected graph G(V,E), where power flow can easily be redistributed both ways along an edge [18]. Transmission lines and transformation stations are modeled as edges (E) because they connect two nodes. Vertices (V) in the network such as generators and consumer points are called nodes. Matrix concepts and graph theory are required to model the problem in this study as a graph and use network metrics for robustness evaluation and attacks. A graph G(V,E) can be represented by an adjacency matrix $\boldsymbol{A}$. Each element a_{ij} is 1 or 0, indicating if there is an edge between node i and j or not. Networks like power grids can be weighted graphs to represent grid properties, such as the ability to transmit flow along a line. Then a_{ij} is an edge weight w_{ij}:

$$a_{ij} = \begin{cases} w_{ij}, & \text{if } (i,j) \in E \\ 0, & \text{otherwise} \end{cases} \tag{2.1}$$

The diagonal matrix $\boldsymbol{D}$ contains the nodal degrees in the diagonal elements. This constitutes the sum of the adjacency elements of all edges connected to node i: $d_i = \sum_{j=1}^{|V|} a_{ij}$. These two matrices define the Laplacian matrix $\boldsymbol{L}$ of the graph as $\boldsymbol{L} = \boldsymbol{D} - \boldsymbol{A}$:

$$L_{ij} = \begin{cases} d_i, & \text{if } i = j \\ -w_{ij}, & \text{if } (i,j) \in E \\ 0, & \text{otherwise} \end{cases} \tag{2.2}$$

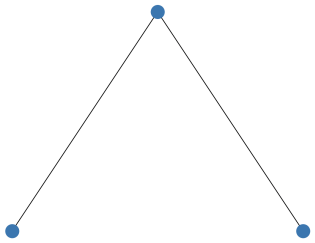

Figure 2.1: A graph with 3 nodes and 2 edges.

The Laplacian matrix represents how much a node deviates from the values of its neighbors in the graph and is related to graph connectivity. As an example, the graph in figure 2.1 has the adjacency, degree, and Laplacian matrices given by:

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad D = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad L = D - A = \begin{bmatrix} 1 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 1 \end{bmatrix}$$

For an undirected graph, $\boldsymbol{L}$ is a symmetric $|V| \times |V|$ matrix with ordered real and non negative eigenvalues: $0 = \lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_{|V|}$ [19]. A connected graph has one eigenvalue = 0. If a graph has n components, the multiplicity of eigenvalues = 0 is n [20]. A matrix with eigenvalues $\lambda_1 = 0$ is singular and therefore does not have a standard inverse matrix of $\boldsymbol{L}$. Instead a generalization of an inverse matrix is used, the Moore-Penrose pseudo-inverse

L^+ [19]. It is an approximation where the least square error is minimized, most often with singular value decomposition [21]. These concepts are essential for computing effective graph resistance and algebraic connectivity.

To reflect how connected a network is relative to its size, graph density GD can be used. It is a metric of how dense a graph is and can be used to compare graph structures, even when they have different number of nodes. A graph with $GD = 0$ has zero edges and a graph with $GD = 1$ has all possible edges present in the graph. The graph density can be computed as [22]:

$$GD = \frac{2|E|}{|V|(|V| - 1)} \tag{2.3}$$

2.2 Robustness Metrics

Many robustness metrics have been studied in complex network theory to quantify a graph's ability to remain connected and functioning after failure or attacks [23]. The aim is to minimize damage and loss in network functionality. These metrics can be used as objective functions for optimization and to evaluate different graph modification algorithms. Topological metrics study the graph structure and how it is connected through nodes and edges, such as degree and betweenness centrality metrics [23]. Betweenness centrality measures the importance of nodes based on how often they appear on the shortest paths between each node pair [18]. These are often used when identifying vulnerabilities and critical components in graphs. Spectral metrics study the adjacency and Laplacian matrix representations of the graph using eigenvalues and eigenvectors, such as algebraic connectivity and effective graph resistance [23]. The efficiency of these metrics to evaluate power grid robustness and capture both topological and electrical properties will be discussed in the section of edge addition algorithms 2.3.

Two metrics used in this study to evaluate power grid robustness after attack scenarios are largest cluster size and served power demand. These were chosen because they capture different power grid properties like the structure of the network and system function. The following section describes the metrics used in this study.

2.2.1 Largest Cluster Size

From a topological approach, preserving graph connectivity can maintain network functionality. When a power grid is fragmented due to attacks or malfunction, the network forms islands. Blackouts, frequency instabilities and overloaded lines cause loads to be disconnected from generation. The ability to maintain network functionality could potentially be quantified by the robustness metric largest cluster size ratio (LCS) [24] and is used in our study. This is defined by the number of nodes in the largest component divided by the total number of nodes, capturing network reachability and flow robustness [23]:

$$LCS = \frac{|CC_{\max}|}{|V|} \tag{2.4}$$

where $|CC_{\max}|$ is the largest cluster component. A connected power grid may still experience line overload and voltage collapse. However, a bigger largest connected component value can still suggest a less severe fragmentation and possibility of operational stability.

2.2.2 Served Power Demand

In power grids, a primary quantity of interest is the ability to maintain acceptable operational performance after a potential attack or malfunction. After cascading failure, this can be quantified as the amount of served power demand (SPD) divided by the total power demand in the whole network [12]:

$$SPD = \frac{\text{served power demand}}{\text{total power demand}} \tag{2.5}$$

This metric captures the generation and load demand dynamics that constitutes power grid robustness. It accounts for the cascading failure and load shedding that occurs when demand exceeds available generation. In our study, the DC power flow model is used to compute served demand and will be discussed further in the method section 3.

2.3 Edge Addition Algorithms

One of the fundamental goals in network robustness is to find ways of improving or maintaining graph robustness. Different methods such as edge rewiring, edge protection or edge addition, aim to do this through optimizing a defined robustness metric [11, 19, 25]. Edge rewiring means replacing or switching connection without changing the number of edges in the graph. Edge protection could mean identifying critical edges, whose removal would cause big network failure and therefore must remain unchanged. Edge addition is chosen in this study to model transmission line expansion. Many graphs and robustness measures have been proposed and evaluated along different types of defense and attack scenarios. The challenge in adding a number of edges to a graph in an optimal way is a combinatorial and computationally heavy problem. A common way to approach this problem and speed up computation is by using greedy algorithms that iteratively choose local optimums to construct an approximate solution [15]. At each iteration, all candidate lines are evaluated based on a robustness metric. If multiple lines return the same value, a random line of these is chosen. However, greedy algorithms do not necessarily guarantee an optimal solution [26].

The following section describes the three edge addition algorithms and their corresponding robustness metrics studied in this paper. The three edge addition algorithms are:

1. Minimizing effective graph resistance
2. Minimizing algebraic connectivity
3. Maximizing algebraic connectivity

2.3.1 Effective Graph Resistance

One established robustness measure is effective graph resistance, R_G [15]. This metric tries to capture both graph theory and power grid properties. By modeling the power grid as an electrical circuit, effective resistance accounts for fundamental laws of power flows. The effective resistance R_{ij} between two nodes can be calculated as:

$$R_{ij} = L^+_{ii} - 2L^+_{ij} + L^+_{jj} \tag{2.6}$$

where L^+ is the Moore-Penrose pseudo-inverse of the weighted Laplacian matrix L. The edge weights are based on line impedances, reflecting electrical paths and power flow dynamics. This will be further explained in the DC power flow section 3.2. R_{ij} represents the potential difference between any node i, where current is supplied, and node j, when current is extracted. The power flow is thus modeled as electrical distances rather than physical distances, which means electrical paths might look different than the physical topology of the grid [12]. The sum of all node pairs' effective resistances is the total effective graph resistance, R_G:

$$R_G = \sum_{i=1}^{|V|} \sum_{j=i+1}^{|V|} R_{ij} \tag{2.7}$$

It can also be computed through the Laplacian eigenvalues [12]:

$$R_G = |V| \sum_{k=2}^{|V|} \frac{1}{\lambda_k} \tag{2.8}$$

R_G is used to evaluate the robustness of a graph and constitutes the objective function of the optimization problem [15]. Minimizing (min) a graph's R_G means more paths for power flow and suggests a more robust graph against edge failures, such as exceeding line capacities, because power can be easier redistributed [12, 15]. Adding a transmission line to a network always decreases the R_G as adding a new parallel path for flow reduces the effective resistance between nodes [12]. This means the aim of the algorithm should be to select an edge that maximizes the decrease of R_G.

Evaluating a candidate line means temporarily adding it to the graph and computing a new pseudo inverse of the Laplacian matrix to be able to calculate the equation 2.6. The potential gain when adding a candidate edge (i,j) is gain(i,j)= $R_G - R_{G'}$, where $R_{G'}$ is the effective graph resistance with the added edge (i,j). Instead of recomputing a new pseudo inverse $L^+_{G'}$ for each candidate line, we simply update the original graph's pseudo inverse L^+_G using the Sherman–Morrison formula of a rank-1 update [15]:

$$L^+_{G'} = L^+_G - \frac{L^+_G b b^T L^+_G}{1/w_{ij} + R_{ij}} \tag{2.9}$$

where b is a unit basis vector $e_i - e_j$. The gain is then computed by:

$$R_G - R_{G'} = |V| \frac{\|L^+_G[:, i] - L^+_G[:, j]\|^2}{1 + R_{ij}} \tag{2.10}$$

where the notation $L^+_G[:, i]$ means the i_{th} column of the pseudo inverse of the Laplacian matrix of the original graph. R_{ij} is defined in equation 2.6.

The problem of adding k optimal edges to minimize effective graph resistance is NP hard [14]. One way to produce an approximate solution can be by using a greedy algorithm, which have often showed a solution of high quality [15]. Algorithm 1 was implemented in this report based on [15, 19]. The algorithm begins by generating a set of candidate edges (C) based on the input graph and computing a weighted Laplacian matrix and its pseudo inverse. For the addition of k edges, there are k iterations. The greedy edge addition algorithm computes

the gain(i,j) for each candidate line and selects the line with the biggest gain, in other words minimizing the effective graph resistance. The selected lines are added to the graph. In algorithm 1, the gain function is referring to equation 2.10.

The optimization problem of adding k edges to a graph, can be represented by a binary choice variable $x_{ij} \in \{0, 1\}$ that indicates whether or not the candidate edge (i,j) $\in C$ is added to the solution. This formulation provides a definition of the objective of the edge addition algorithm and shows the combinatorial nature of the problem with a large number of candidate lines:

$$\max_{x} \quad R_{\mathrm{G}} - R_{\mathrm{G}'}(x) \tag{2.11}$$

$$\text{s.t.} \quad \sum_{(i,j)\in C} x_{ij} = k \tag{2.12}$$

$$x_{ij} \in \{0, 1\} \tag{2.13}$$

Algorithm 1 Greedy minimization of effective graph resistance edge addition

```
1:  function EdgeAddition(G, k)
2:      Input: Graph G = (V, E), number of edges to add k
3:      Output: Updated graph G
4:      C ← CandidateEdges(G)
5:      L ← ComputeLaplacian(G)
6:      L⁺ ← ComputePseudoInverse(L)
7:      for step ← 1, ..., k do
8:          bestEdge ← None
9:          bestGain ← −∞
10:         for each (i, j) ∈ C do
11:             gain ← GainFunction(L⁺, i, j)
12:             if gain > bestGain then
13:                 bestGain ← gain
14:                 bestEdge ← (i, j)
15:             end if
16:         end for
17:         add bestEdge to G
18:         remove bestEdge from C
19:     end for
20:     return G
21: end function
```

2.3.2 Algebraic Connectivity

Another well established robustness metric is algebraic connectivity [25, 27, 28], which is defined as the second smallest eigenvalue λ_2 of the Laplacian matrix L of the graph. For an unweighted graph, the Laplacian matrix is only reflecting the topology. Adding a transmission line to a network always increases the algebraic connectivity [27]. Maximizing (max)

the algebraic connectivity implies a more connected graph and thus more difficult to disconnect into components when attacked [25]. However, a highly connected power grid could potentially suggests easier propagation of cascading failure [13].

Evaluating a candidate line means temporarily adding it to the graph and computing a new eigenvalue. For a larger graph, one way to avoid recomputing the Laplacian matrix and its eigenvalues, is a first order approximation of the increase in algebraic connectivity when adding an edge. The normalized eigenvector to λ_2 is called the Fiedler vector v. By differentiating the eigenvalue $\lambda_2(L_G)$ with respect to a small perturbation of the Laplacian matrix, an estimation of how much the eigenvalue λ_2 changes when adding an edge is given by $(v_i - v_j)^2$ [13, 27]:

$$\lambda_2(L_{G'}) = \lambda_2(L_G) + (v_i - v_j)^2 \tag{2.14}$$

where v_i is the i_{th} component of the Fiedler vector and $\lambda_2(L_{G'})$ is the second smallest eigenvalue of the Laplacian matrix with an added edge. This result constitutes the objective function of the optimization problem, meaning that we want to add edges to the graph that maximizes $(v_i - v_j)^2$. The problem of optimally adding a fixed number of edges to maximize algebraic connectivity is NP hard [29], however the greedy algorithm for this problem has shown to be close to the optimal value [27]. To further study the relationship between connectivity and robustness, both minimization and maximization of the increase of algebraic connectivity were investigated. For simplicity, only the minimization case is described as the corresponding implications also hold for the maximization case. The following greedy algorithm was implemented in this report with the objective function being minimized in one case and maximized in another. At each iteration, the greedy edge addition algorithm adds the edge that minimizes (or maximizes) the increase of algebraic connectivity according to $(v_i - v_j)^2$ [13, 27]. Algorithm 2 begins by generating a set of candidate edges based on the input graph and computing the Fiedler vector for G. For the addition of k edges, there are k iterations. The greedy edge addition algorithm computes the difference $(v_i - v_j)^2$ for each candidate line and selects the line with the smallest (or largest) difference, in other words, minimizing (or maximizing) algebraic connectivity. The selected lines are added to the graph.

The optimization problem of adding k edges to a graph can also be represented by a binary choice variable $x_{ij} \in \{0, 1\}$ that indicates whether or not the candidate edge (i,j) $\in C$ is added to the solution of k edges. This formulation presents the minimization case of the objective function of the edge addition algorithm. It shows the combinatorial problem with a large number of candidate lines:

$$\min_{x} \quad (v_i - v_j)^2 \tag{2.15}$$

$$\text{s.t.} \quad \sum_{(i,j)\in C} x_{ij} = k \tag{2.16}$$

$$x_{ij} \in \{0, 1\}. \tag{2.17}$$

Algorithm 2 Greedy minimization of algebraic connectivity edge addition

```
1: function EdgeAddition(G, k)
2:     Input: Graph G = (V, E), number of edges to add k
3:     Output: Updated graph G
4:     C ← CandidateEdges(G)
5:     v ← ComputeFiedlerVector(G)
6:     for step ← 1, ..., k do
7:         bestEdge ← None
8:         minDiff ← ∞
9:         for each (i, j) ∈ C do
10:            diff ← (v_i − v_j)^2
11:            if diff < minDiff then
12:                minDiff ← diff
13:                bestEdge ← (i, j)
14:            end if
15:        end for
16:        add bestEdge to G
17:        remove bestEdge from C
18:    end for
19:    return G
20: end function
```

2.4 Attack Strategies

A common way of evaluating network robustness is to simulate natural failure and targeted attacks [11, 24]. It is a way to further evaluate different graph modification algorithms and robustness metrics. To simulate natural disasters or malfunction, random nodes are removed from the graph and the damage is quantified. Such an approach is one way to estimate how robust a graph is against aging infrastructure and expected operational degradation. Malicious attacks however, target the most vulnerable components to cause severe network disruption and operational failure [18]. Power grids are one of the most critical infrastructure and significant power outages could cause societal collapse [1]. It can be simulated by stress testing the graph with a series of targeted attacks on critical network components. Nodes or edges are strategically removed based on a chosen metric to maximize damage to the network structure or functionality. After each node is removed, the set of critical nodes is recalculated. This adaptive attack was used in this study to make sure that the most critical component is attacked at each step as the grid changes. The robustness was then evaluated under cascading failures using the robustness metrics discussed in section 2.2.

The attacker's choice of strategy depends on the amount of available network information. Operational data is often confidential due to security concerns and detailed grid information can be limited [30]. However, any form of sensitive data can be compromised due to security leaks or attempts to gather information for foreign intelligence agencies. This potential threat should be accounted for when building and expanding the power grid. In our report, the attacker is assumed to work with varying levels of information about the network.

We chose one purely topological attack and one where electrical data was needed, to capture two of levels of information.

2.4.1 Highest Degree Node

Some transmission line layouts may be partially observable through analyzing, for example online maps and field observations, which opens up the possibility of targeted topological attacks. Power grid networks often possess scale-free characteristics. A scale-free network has few nodes with many edges and many nodes with few edges, making the network especially vulnerable to attacks on nodes with many connections [2]. One strategy used in the experiments is the attack on the node with the most neighboring edges, in other words the highest degree d_i node [23, 31]. The max degree d_{max} of a node is defined as:

$$\arg\max_i \sum_{j \neq i} a_{ij} \tag{2.18}$$

where a_{ij} is the element of the unweighted adjacency matrix A_{ij}. The metric identifies the most connected nodes that potentially constitute critical network components [18]. In the degree node removal attack, each connected edge is deactivated and loses its ability to transmit power flow.

2.4.2 Electrical Node Significance

Another strategy used in this study is especially designed for power grids and assumes knowledge about power flows. The electrical node significance γ_i is a metric that identifies nodes with large amounts of power distribution:

$$\gamma_i = \frac{P_i}{\sum_{j=1}^{|V|} P_j} \tag{2.19}$$

where P_i is a node's injected power and $\sum_{j=1}^{|V|} P_j$ the total net injected power in the network [12]. Consequently, this metric represents a ratio of the total network power distribution contributed by node i and can identify nodes with more heavily loaded connections. These nodes therefore have potentially a great influence on network flows. DC power flow calculations were computed to obtain the power flows of the graph, see section 3.2. Removing the highest electrical significant node γ_i causes the power to be redistributed in the grid. This could potentially lead to overloaded lines and cascading effects [32].

Chapter 3
Method

In this report, the effectiveness of edge addition algorithms was studied under different attack scenarios. The transmission lines that were chosen by optimizing with respect to a robustness metric, were evaluated by plotting and data retrieving. It was done by identifying and removing critical components of the power grid and simulating cascading failures. Two power grids were used in this study, the IEEE 118 synthetic test grid as a benchmark which is used in many power grid studies [12], and a more realistic PyPSA Nordic graph with geographical coordinates to compare to. The following section describes the methodological workflow of the study.

3.1 Approach

The thesis process began with an extensive literature review to understand the problem and find suitable methods and evaluation metrics. Based on the findings from the research, the proposed approach was implemented. Firstly, we developed a custom graph structure in Python to reduce computational overhead otherwise caused by repeated conversions between a graph library and pandapower, an open-source Python tool to model electric power systems [33]. Our graph structure directly interacts with pandapower, enabling more flexible graph manipulations during experiments. It also allowed us to have better control over the graph representation, handling the network data and retrieval of graph attributes. Selected information was stored in the custom graph structure to avoid frequent access to pandapower data structures. This design choice was motivated by empirical observations during development, where direct access to the custom structure appeared more efficient for the required operations. Furthermore, during edge addition algorithms, all candidate edges are evaluated by temporarily adding them to the graph and then removing them again. To speed up computations, we implemented certain graph modifications at the Laplacian matrix level to provide faster updates instead of updating pandapower data structures.

Next, we extracted the test grids from open source data such as buses, transformers,

transmission lines and geographical coordinates. The IEEE test grid was obtained from pandapower library and the Nordic grid from PyPSA. We processed this information to fit the graph structure and a weighted graph representation of the power grid was created. Thereafter, we implemented the edge addition algorithms, along with a random edge addition baseline and robustness metrics, and applied to the test grids. Furthermore, we implemented an attack and cascading algorithm to model DC power flow under different conditions. Figure 3.1 illustrates a flowchart of the experiments. The experiment begins by creating a graph representation of the power grid and then applies the edge addition algorithm, followed by repeated attacks on the most critical nodes. After each attack, DC power flow calculations identify if any lines are overloaded, in which case they are removed. If there are not, the stopping criteria is satisfied and the power grid robustness is evaluated. The cascade terminates when there are no more overloaded lines, and the whole process terminates when there are no more attacks.

Lastly, we implemented a plotting and evaluation framework to obtain results and to quantify the robustness of the power grid. It is visualized by a robustness curve, showing the evaluation metric after each node removal as a function of the number of removed nodes. To compare the robustness performance of the algorithms relative to the random edge addition baseline, the area under the robustness curve in all plots were calculated with the trapezoidal rule, a numerical integration technique. The area under the robustness curve represents an overall performance of the network throughout the attack and cascading scenario. A large area would suggest that the network maintains a high served demand or largest cluster size for a long time, and thus a more robust power grid. The relative change in area was calculated for each algorithm with:

$$\Delta A_i(\%) = \frac{A_i - A_{\text{baseline}}}{A_{\text{baseline}}} \cdot 100 \tag{3.1}$$

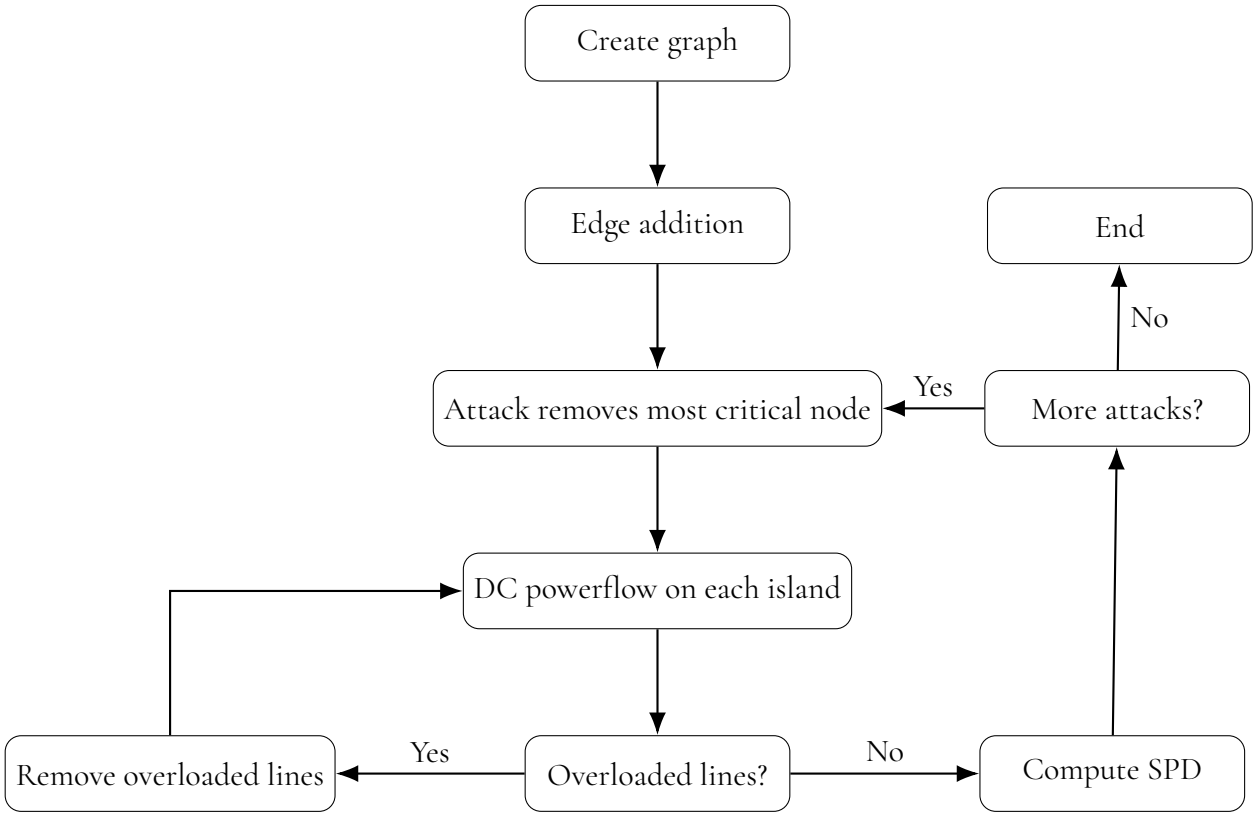

Figure 3.1: This figure shows the flowchart of the experimental setup.

3.2 DC Power Flow

To simulate a power grid with electrical properties, power flow values were calculated using pandapower. The injected power $P_i + \mathrm{j}Q_i$ at a node is the sum of active power P_i and reactive power Q_i, where $\mathrm{j} = \sqrt{-1}$ denotes the imaginary unit. Electrical supply or demand is set for each node in the graph and nodal power flow equations can then be solved. These are derived from physical laws that determine electrical properties of the network, such as current and power balance at each node. Transit nodes with no generation or load were represented as demand nodes with no injected power. The DC power flow model is a linear approximation of AC power flow and has a 5% line flow error margin [12, 34]. It neglects reactive power and assumes small variations of voltage magnitudes and voltage angle differences in all nodes. These simplifications apply well to high voltage transmission lines [4] and enable a linear set of equations, which speeds up computation time of power flows. pandapower's DC power flow solver is based on the Newton-Raphson method [33] and can be calculated by solving the following nodal equations:

$$P_i = \sum_{j=1}^{|E|} Y_{ij}(\theta_i - \theta_j) \tag{3.2}$$

where P_i is the nodal injected active power and θ_i is the nodal voltage angle. Y_{ij} is the nodal admittance matrix, which is the inverse of the impedance matrix Z_{ij}. The impedance Z_{ij} of

a line between node i and j is the resistance R_{ij} and reactance X_{ij} of an alternating current: $Z_{ij} = R_{ij} + \mathrm{j}X_{ij}$, where again $\mathrm{j} = \sqrt{-1}$ denotes the imaginary unit. The nodal admittance matrix is thus given by:

$$Y_{ij} = \frac{1}{R_{ij} + \mathrm{j}X_{ij}} \tag{3.3}$$

In the DC approximation, R_{ij} is assumed to be much smaller than X_{ij}, resulting in neglecting resistance. To reflect power flow in the grid, the edge weights for the Laplacian matrix was therefore given by $w_{ij} = \frac{1}{X_{ij}}$ and used when computing effective graph resistance [35].

In summary, DC power flow was used when modeling line overloads and cascade failures in this study. It allowed an efficient computation of nodal voltage angles and power flows to determine the distribution of power, in particular when computing electrical node significance attacks and served power demand.

3.3 Cascading Simulation

To evaluate the edge addition algorithms and model a power grid attack scenario, we implemented a cascading algorithm in Python. The algorithm simulates an attack on a critical node and removes potential overloaded edges. If the removal of these lines cause more overloaded lines, a cascade has begun. If an attack resulted in multiple disconnected components, these were identified using a NetworkX function. NetworkX is a Python package that can be used for graph operations [36]. To solve the DC power flow equations, a reference point needs to be assigned to a bus in the power grid. It is called the slack bus, as it balances mismatches between generation and demand. It compensates for power losses along the transmission lines due to impedance [37]. If the slack bus was removed during an attack, or a component of the grid gets disconnected from the slack bus, we assign a slack bus to a bus in each component with a functional generator. The DC power flow equations can then be solved for each self-sufficient component.

To be able to run the DC power flow solver on each component, we created independent sub grids and the islands' served demand were calculated. This is the smallest value between the sum of all loads in that island and the sum of all generators in that island. To get the total served power demand of the whole grid, all islands' SPD are summed.

The solution to the DC power flow was used to identify and remove edges that exceeded line capacity, to simulate circuit breaks [38]. This happens as a result of the redistribution of power from neighboring edges after an attack. We modeled the simulation as a while loop and the DC power flow was applied at each island to recalculate the power flow. The cascade continued until there were no more overloaded lines in the grid [32]. The power grid robustness was then quantified by the remaining served demand after potential cascading failures, as visualized in the flowchart 3.1.

3.3.1 Cascading Risks

To further investigate the relationship between connectivity and cascading behavior, the IEEE 118 test grid was attacked under two different cascading risks. Initial experiments on the original IEEE 118 bus system did not produce any overloaded transmission lines, even

under extreme attack scenarios. The power test grid to begin with is very robust, due to high transmission capacity. It generally allows easy redistribution of power flow when component failure occurs. To stress the power grid further, a second experiment was performed in which line capacity limits were reduced by 97%. This increases the likelihood of overloads and thus increases the cascading risk, simulating a grid with operational conditions closer to the limit. The updated line capacity of IEEE 118 is then slightly below the line capacity of the Nordic grid.

3.4 Datasets

In this section, the two power grid datasets used in our study are described.

3.4.1 IEEE 118

The IEEE 118 bus system dataset is a standard synthetic test power grid often used in power network studies [12] for benchmarking. The dataset contains various different electrical and structural information. In figure 3.2 the topology of the IEEE 118 network is visualized, where the coordinates of the nodes are arbitrary. It has 118 buses modeled as nodes, 9 transformers modeled as edges, 19 generators and 91 loads [39]. Nodes can have generation, load, transit functionality, or a combination of these. Only 8% of the nodes are transit nodes, which is an indication that generation and load are distributed across most of the power grid rather than being concentrated to a small number of buses.

In addition, the network has 177 AC lines modeled as edges with line capacity of 16.57 kilo Ampere (kA) and 41.42 kA which are made up numbers according to the publisher of the dataset [17]. The power grid is labeled as robust by the publisher [17]. It makes it improbable that the lines overload or that the graph would exhibit cascading failures. To also investigate how different overloading risks impact the different edge addition algorithms, the edge capacities were reduced to simulate higher load conditions and induce cascading failures, thereby stressing the grid. Furthermore, the graph density for the IEEE 118 test case is 0.027, calculated with the graph density equation 2.3. Coordinates are available, but they are arbitrary and do not reflect geographic locations or physical information and were only used for plotting reasons. This also means that all edges have the length of 1 kilometer (km). The dataset is published by University of Washington and contains partial synthetic electrical data based on a power grid from 1962 [17]. The dataset was downloaded from the open-source pandapower network calculation tool, released under a BSD license [33].

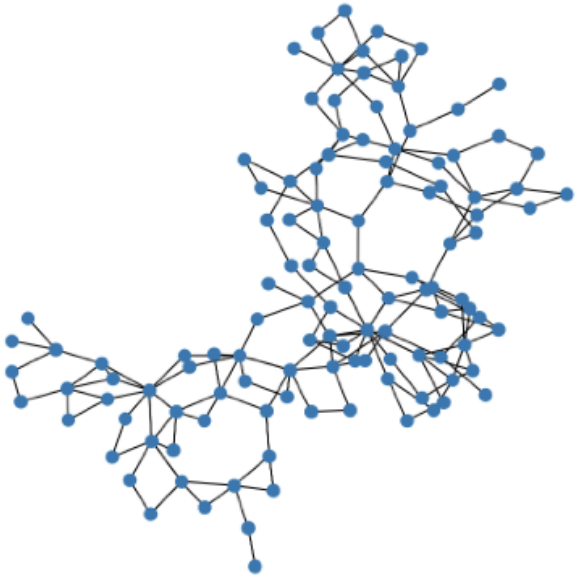

Figure 3.2: This figure shows the spatial representation of IEEE 118 power grid graph.

3.4.2 Nordic Power Grid

The other dataset that was used is a transmission grid of Denmark, Finland, Norway and Sweden, which will be called the Nordic power grid. In the figure 3.3, the graph topology is visualized using node coordinates that reflect their actual spatial positions and where edge lengths represent the scaled distance between connected nodes. We placed the graph over a free domain Nordic map. We generated the dataset using the open-source PyPSA framework released under GPLv3 license, a tool for modeling energy systems developed at the Technical University of Berlin [40]. More details of the implementation will be discussed in section 3.4.3. They built the framework on public electrical information, maps and data to simulate realistic grids and power system behavior. It is used in both academic research and industry applications [40]. The tool allows for building the power system model on country specific data. PyPSA also creates a time series but for the purpose of this study only one time frame was used, 2013-01-01 to 2013-01-02.

The generated model has 459 buses modeled as nodes, 742 AC lines modeled as edges with line capacity of 2.58 kA. It has 50 loads in the specific time frame and 182 generators with generation from 12 different energy sources: combined cycle gas turbine, oil, offshore wind, coal, nuclear, waste, lignite, biomass, solar, onshore wind, and hydroelectric. The table 3.1 shows the distribution of loads and generation in the different countries. It is similarly modeled as in the IEEE 118 power grid where nodes can have generation, load, or both, while some nodes are transit nodes. The Nordic power grid is significantly more sparse with generation and load compared to IEEE 118 power grid with 50% of total nodes being transit nodes.

Figure 3.3: This figure was produced by extracting and processing data from the PyPSA network. It shows the spatial placement of the Nordic power grid nodes according to their geographic coordinates, overlaid on a public domain Nordic map [41].

Country	Denmark	Finland	Norway	Sweden
Number of Loads	4	11	18	17
Load Demand (MW)	3339	9751	14741	14610
Nodes with Load (%)	13	5	21	13
Number of Generators	24	55	30	73
Generation (MW)	11974	22548	8025	35067
Nodes with Generation (%)	75	65	14	56

Table 3.1: This table shows the distribution of loads and generators in the different countries.

Additionally, there are 8 high voltage direct current (HVDC) links, 6 of them are underwater links, such as the transmission line between Denmark and Norway. They are often used to transfer power over long distances [42]. The whole network has a single voltage level of 380 kilovolt (kV) and therefore contains zero transformers. The graph density is 0.0071, calculated with the graph density equation 2.3. Buses have geographic coordinates and all electrical components have information about which country they are located in and some corresponding data.

3.4.3 Nordic Power Grid Dataset Conversion

We converted the PyPSA network, the Nordic power grid, into a pandapower network representation to have a common tool for the datasets. In the conversion, we had to convert units to fit pandapower needs. During the conversion between frameworks, model-specific requirements and missing parameter values were encountered. Most adaptations (choosing slack bus, missing values, power balancing and HVDC lines modeling) were based on methods reported in the literature, which will be discussed further in this section.

The graph has no islands. Loads and generators were assigned to buses based on their country. Within each country, they were randomly allocated to available buses. This was because there was no available information of exact location, only regions were specified. Regions with more nodes were more likely to have a higher concentration of loads and generators. As it is a modeled transmission grid and not a distribution grid, the nodes with loads can represent the demand of a city or area. Additionally, many of the generators had no available data for efficiency and no net produced effect. Consequently, max capacity for the generators was used and scaled to meet power balancing demands. This method has been used in power grid studies, where generators are scaled to produce 90% of total load demand as the rest is assumed to come from the slack bus [38]. This was achieved by scaling all generations by 0.62.

Furthermore, the PyPSA dataset did not provide a slack bus which is required to run DC power flow calculations in pandapower. There exist many different strategies when choosing slack buses which optimize for different objectives, such as minimizing approximation loss or fast convergence rate [43]. We implemented the first perspective, thus the generator with the highest generation was assigned as the slack bus.

Data for 8 lines in the PyPSA dataset for resistance and reactance were not available, so the median values of the respective categories were assigned. We implemented the HVDC lines as AC lines with 380 kV due to the lines having comparable characteristics, which was also done in [44].

3.5 Candidate Edges

The set of possible candidates edges to add in the edge addition algorithms consists of all possible bus combinations, excluding buses that are already connected. The IEEE 118 candidate set contains 5350 edges, and the Nordic power grid has 104524 candidate edges, not including transformers.

The candidate lines which are added do not have electrical data and it is modeled with the mean values of the already existing edges for each needed parameter. For example, the

reactance value assigned to a new edge was set to the mean value of the reactance of all existing edges in the network, which is a common way to model new edges in network studies [12]. The coordinates of buses are in longitude and latitude, thus we calculated the transmission line distance in regards to the earth's surface, not with the Euclidean distance.

3.6 Number of Added Edges

In our study, the number of lines to be added is defined before the start of the algorithm, which means that a combination of more or fewer edges could potentially result in a more or less optimal solution. From a robustness perspective, a cascade could be more severe if too many lines are added [2], suggesting that there is a critical number of lines that would be optimal to add. To find a good number of edges to add, edges were gradually added to the graph and evaluated after 20% high degree node attacks. This simulation of edge addition followed by attacks was done for 20 different sizes of edge additions. The number of added edges was spanning from 5% to 100% of the number of edges present in the original graph, $|\boldsymbol{E}|$. The number of added edges in this study was 15%, to represent a moderate gradual expansion of the Nordic transmission network and a consideration of analyzing the results of the robustness performance when adding more edges. As mentioned in the introduction, around 2900 km new transmission lines are planned to be built in Sweden alone over the next ten years. It constitutes 18% of the total amount of transmission line distance in Sweden today [45].

3.7 Baseline

We implemented a random edge addition algorithm that selects random edges to add to the graph, used as a baseline to compare and evaluate edge addition algorithms. This has similarly been done in [13, 46]. The algorithm performs k iterations, each time selecting a random edge from the candidate list and adding it to the graph, where k denotes the number of edges to be added. Thereafter, an attack and cascade simulation is performed. After each node is removed followed by a possible cascading event, a robustness metric is computed, resulting in multiple discrete measurement points. The whole process was repeated five times independently with five different seeds. The corresponding points from each run were averaged to one robustness curve to establish a baseline. Furthermore, by comparing against random edge addition with the same number of added edges, the effect of edge addition in itself can be isolated from the potential general benefit or disadvantage of increased connectivity. Consequently, the average performance of the algorithm's result could provide a good baseline as a point of reference.

The robustness curves produced by the random edge addition algorithm and attack simulation were somewhat smoother than those of the other algorithms and did not exhibit as large drops as often in the corresponding metric values. This is due to it being the average graph curve of five random seeds, that is, random edge addition also have significant drops in performance but the averaging slightly evens out the curve.

Some previous research has suggested that random edge additions can have somewhat strong robustness characteristics in certain network structures and scenarios [38, 46]. Specif-

ically, how a more random graph structure could be more robust against an outbreak of a cascading event. However, it further suggests that if a cascading event begins, a very random structure may fragment faster than a more ordered structure [38]. Another study implied that random addition was more robust compared to more targeted edge additions in some network structures [46].

Chapter 4
Results

This chapter presents the results and findings of the investigation of edge addition algorithms and robustness metrics. These are evaluated through targeted attacks and cascading events. The figures can be interpreted as follows. The figures show an evaluation metric from section 2.2 as a function of fraction of removed nodes. After each node removal based on a strategy from section 2.4, a possible cascading event takes place after which the remaining structure or function is evaluated. This results in discrete measurement points after each node attack. The points corresponding to the random edge addition are obtained as explained in section 3.7. The line between the points is used only to visualize the overall trend.

4.1 IEEE 118 Graph Dataset

This section shows the results of edge addition algorithms and targeted attacks on the IEEE 118 graph dataset. The different algorithms demonstrate various performances. Overall, the effective graph resistance edge addition performed the best and min algebraic connectivity edge addition performed the worst.

4.1.1 Number of Added Edges

The results of adding more and more edges to the graph can be found in figure 4.1. The figure shows the evaluation metric SPD after 20% node removal, as a function of the fraction of added edges, see section 2.2.2. It was run for 20 different sizes of edge addition, resulting in 20 discrete measurement points. The results indicate that adding more edges to the graph can improve robustness in terms of how much electrical demand can still be served after attacks, when the algorithm optimizes for minimizing effective graph resistance. However, the improvement seems to stabilize after around 20% of edges have been added. Maximizing algebraic connectivity shows the same initial behavior of increased robustness but decreases

after a peak and never recovers again. Minimizing algebraic connectivity does not show an increase in robustness until more edges are gradually added.

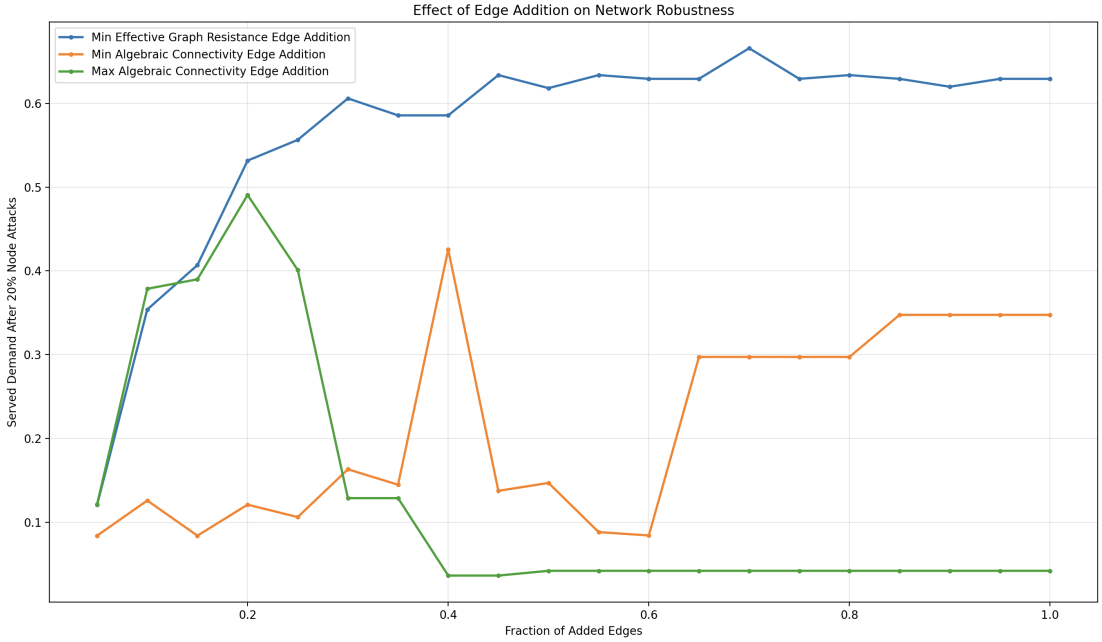

Figure 4.1: This figure shows the served demand after removing 20% of nodes with node degree attack in the IEEE 118 graph against the fraction of added edges.

4.1.2 Highest Degree Node Attack

The robustness improvement of the IEEE 118 graph after different edge addition algorithms is evaluated after a node attack on the highest degree nodes. According to the topological robustness metric ***LCS***, the max algebraic connectivity edge addition algorithm performs slightly better than the others, see figure 4.2. When 20% of the nodes are removed, around 60% of its largest component still remains intact. Minimizing the algebraic connectivity on the other hand, performed worse than random edge addition. When 20% of the nodes were removed, only 20% of its largest component remained intact. Minimizing effective resistance showed slightly better performance than random edge addition.

According to the electrical robustness metric ***SPD***, the effective graph resistance edge addition algorithm performed the best, see figure 4.3. When 20% of the nodes are removed, just under 50% of all power demand can still be served. While certain node removals cause big drops in served demand for some edge addition algorithms, effective graph resistance decreases more steadily.

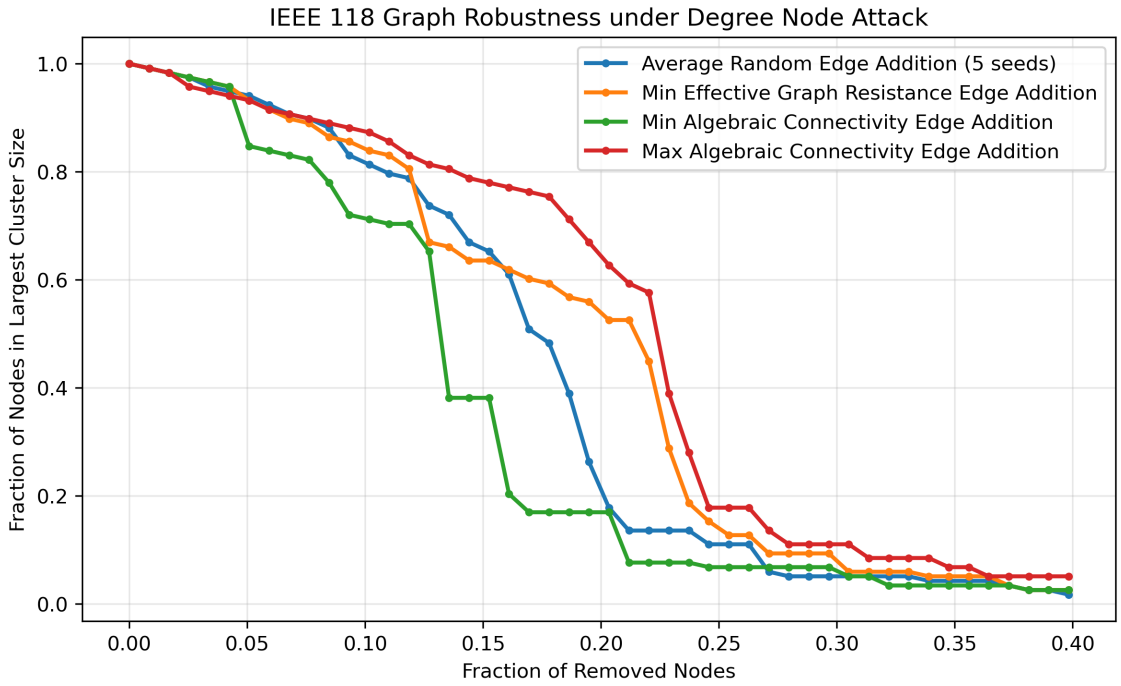

Figure 4.2: Four edge addition algorithms with 15% of total edges added measured with the robustness metric largest cluster size with highest degree node removal.

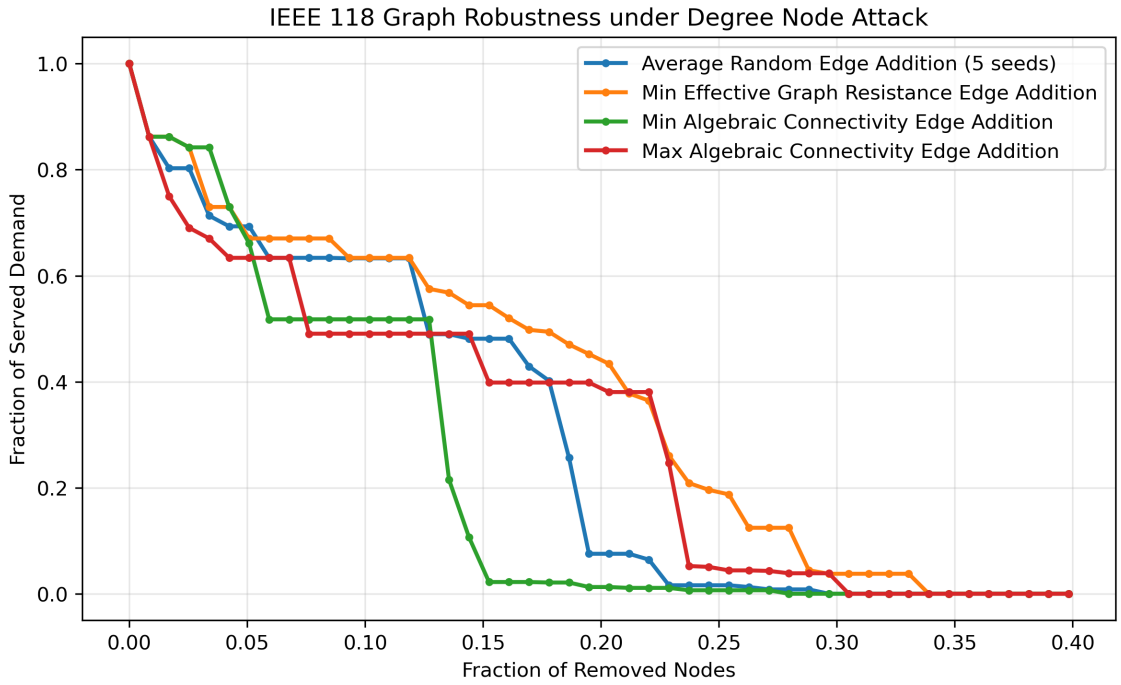

Figure 4.3: Four edge addition algorithms with 15% of total edges added measured with the robustness metric served power demand with the highest degree node removal.

4.1.3 Electrical Node Significance Attack

The robustness improvement of the IEEE 118 graph after edge addition algorithms was also evaluated after a node attack on the most electrical significant nodes. According to the topological robustness metric ***LCS***, effective graph resistance performs the best, see figure 4.4. When 20% of the nodes are removed, around 70% of its largest component still remains intact. Min algebraic connectivity on the other hand performs way worse than random edge addition.

According to the electrical robustness metric ***SPD***, all algorithms struggled to perform better than random and experience fast decline in served power demand, see figure 4.5. However, when 20% of the nodes are removed, only effective resistance remain over 20% of served demand with a less severe drop over fraction of removed nodes.

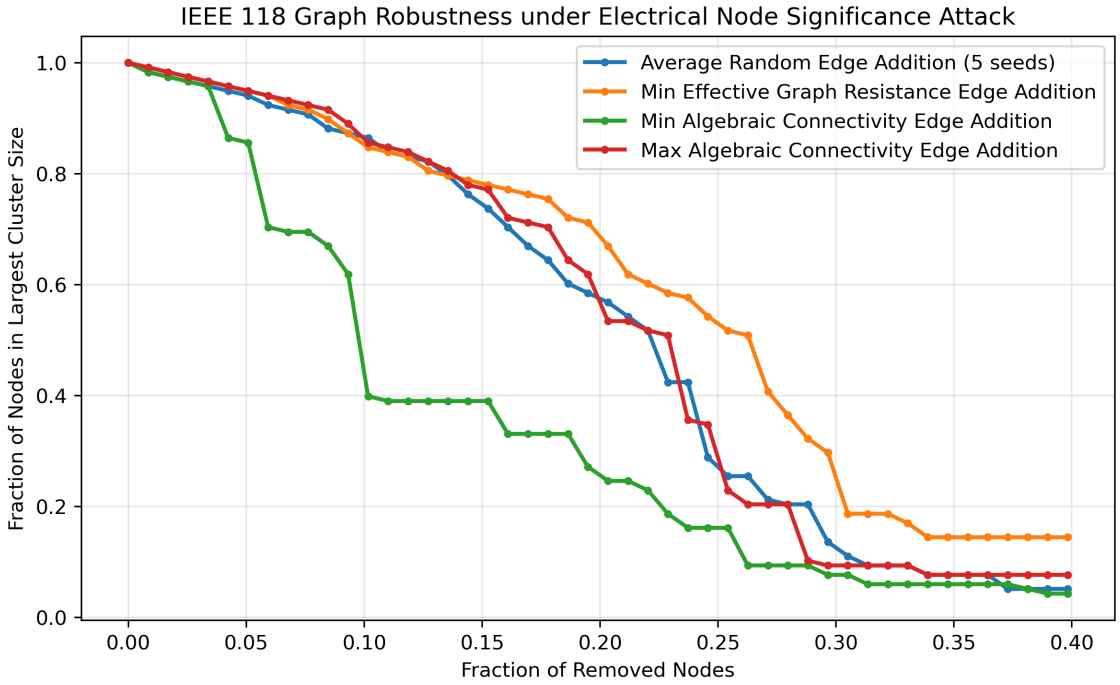

Figure 4.4: Four edge addition algorithms with 15% of total edges added measured with the robustness metric largest cluster size under most electrical node significance removal.

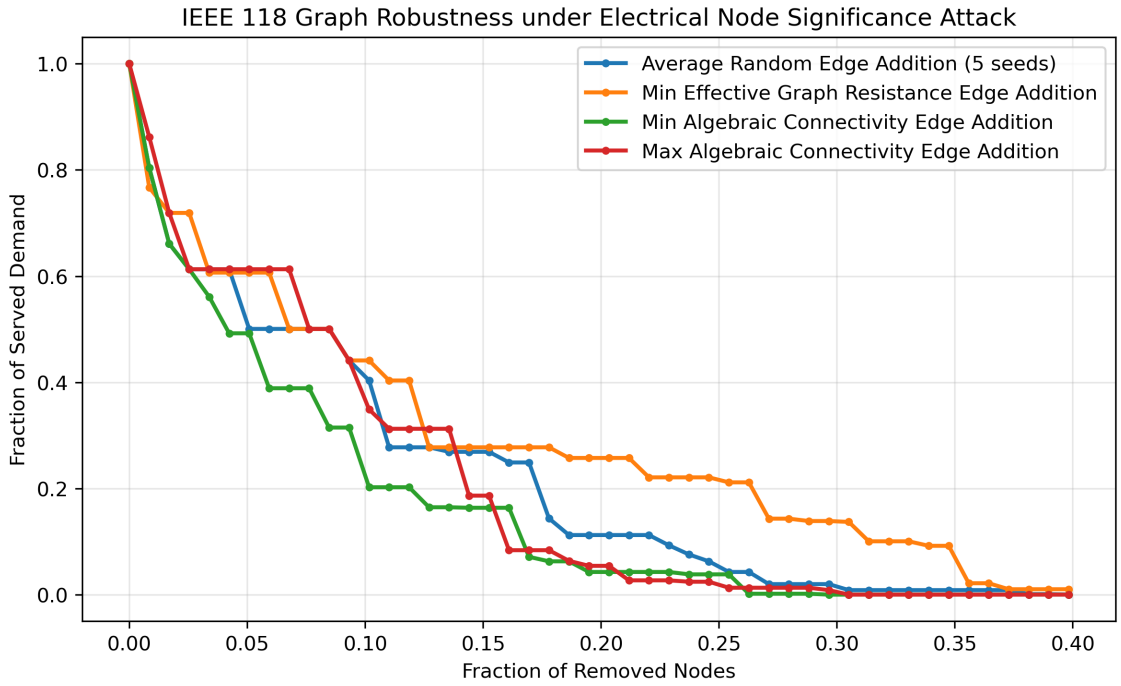

Figure 4.5: Four edge addition algorithms with 15% of total edges added measured with the robustness metric served demand under most electrical node significance removal.

4.1.4 Increased Cascading Risk

Another experiment was conducted on the IEEE test graph. To simulate higher load conditions for the IEEE graph and induce cascading failures, the edge capacities were reduced, see figure 4.6 and 4.7. Min algebraic connectivity outperform outperform all other algorithms for all of the attack progression in both the degree and electrical significance attacks. Max algebraic connectivity experienced the biggest drop in served demand. Min effective resistance performed slightly better than random for the node degree attack.

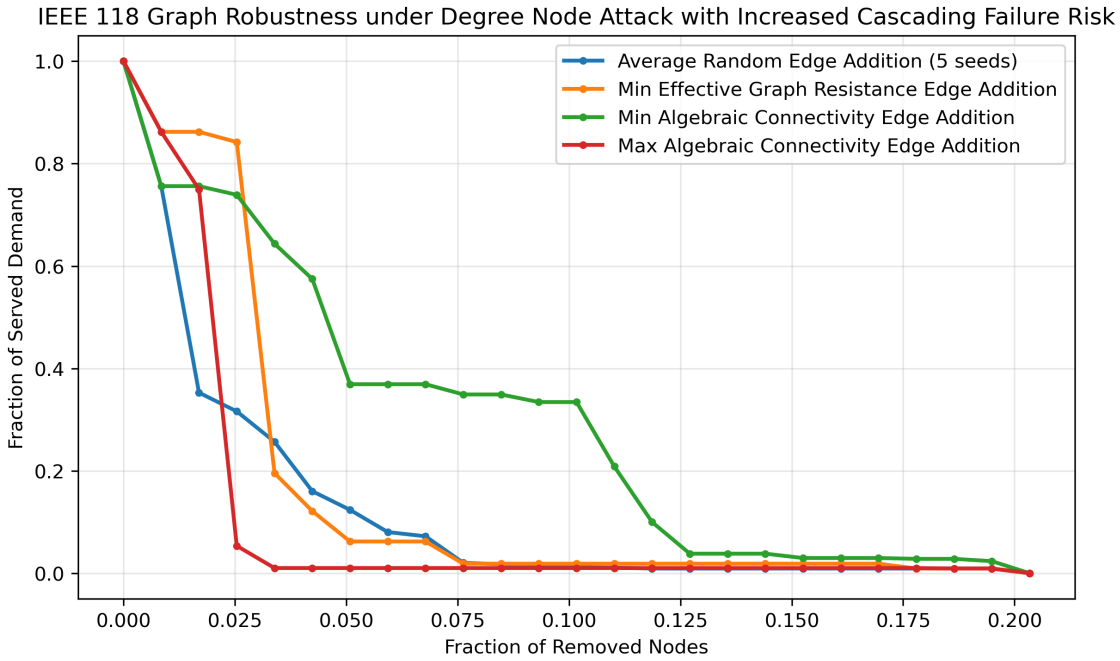

Figure 4.6: Four edge addition algorithms with 15% of total edges added, measured with the robustness metric served demand and highest degree node removal, with increased cascading risk.

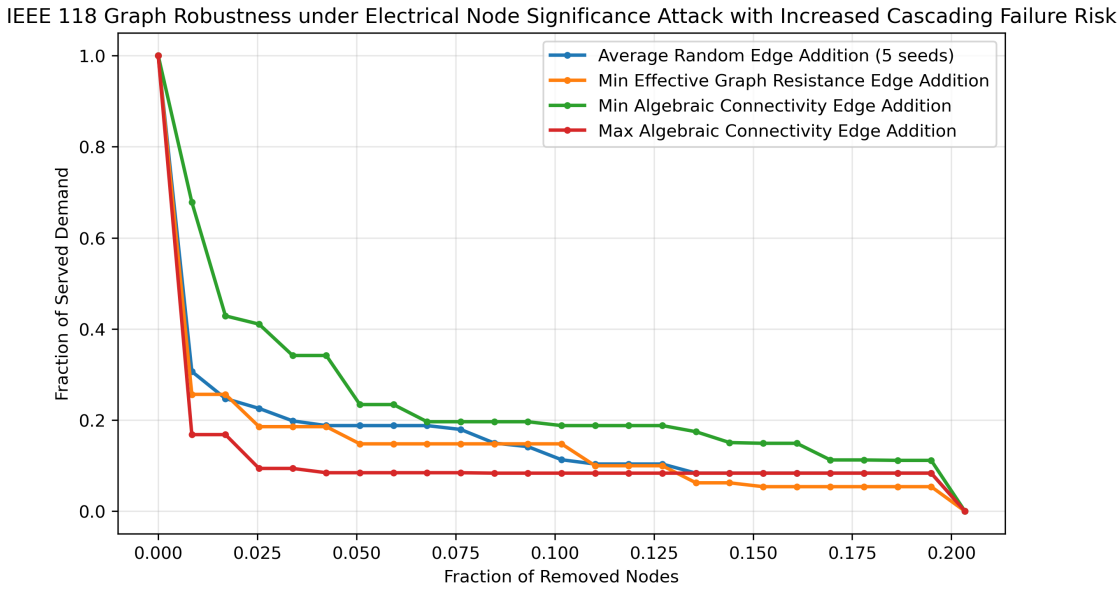

Figure 4.7: Four edge addition algorithms with 15% of total edges added, measured with the robustness metric served demand and electrical significant node removal, with increased cascading risk.

4.1.5 Network Findings

After the edge addition algorithms, the grids were attacked with multiple node removals. The removed node which caused the biggest drop in served power demand percentage points for each algorithm and attack, can be found in table 4.1. Consistent with the notation used throughout this report, R_G denotes effective graph resistance and $\lambda_2(L)$ denotes algebraic connectivity since it is the second smallest eigenvalue. d_i and γ_i respectively stands for degree attack and electrical node significance attack. The column "Removed" shows the number of removed nodes so far after the node from the column in "Node id" is removed. The results show that both min and max algebraic connectivity experienced their biggest drop in SPD much later than for the electrical node significance attack, which happened at the first and second node removal. The column "Comp" shows the number of components in the grid after the removal of the node. The algorithms had no overloaded lines, which shows that the IEEE 118 graph is very robust against cascades. The node id of the removed node is also shown in the same table to reveal if any algorithm and attack scenario struggled with the same or different nodes.

Algorithm	Attack	Removed (count)	Node id	Comp	Overloaded	SPD Drop (pp)
Min R_G	max d_i	1	48	1	0	14
Min $\lambda_2(L)$	max d_i	16	24	12	0	30
Max $\lambda_2(L)$	max d_i	28	24	20	0	19
Min R_G	γ_i	1	88	1	0	23
Min $\lambda_2(L)$	γ_i	1	8	2	0	20
Max $\lambda_2(L)$	γ_i	2	88	1	0	14

Table 4.1: This table shows graph data for the node that caused the biggest drop in served power demand in percentage points (pp) when attacked for the different algorithms. The table is for the IEEE 118 graph.

4.2 Nordic Graph Dataset

This section shows the results of edge addition algorithms and targeted attacks on the Nordic graph dataset. The obtained measurements point for the Nordic figures are more closely packed than for the IEEE results. It is due to it being a bigger graph with more nodes, thus the same fraction of removed nodes constitutes more nodes, resulting in more data points.

4.2.1 Number of Added Edges

The results of adding more and more edges to the Nordic graph can be found in figure 4.8. The figure shows the evaluation metric SPD after 20% node removal, as a function of the fraction of added edges, see section 3.6. It was run for 20 different sizes of edge addition, resulting in 20 discrete measurement points. Minimizing algebraic connectivity and effective graph resistance show a slow increase of robustness as more edges are gradually added. Max

algebraic connectivity shows one peak around 40% of added edges, then decreases and never recovers again.

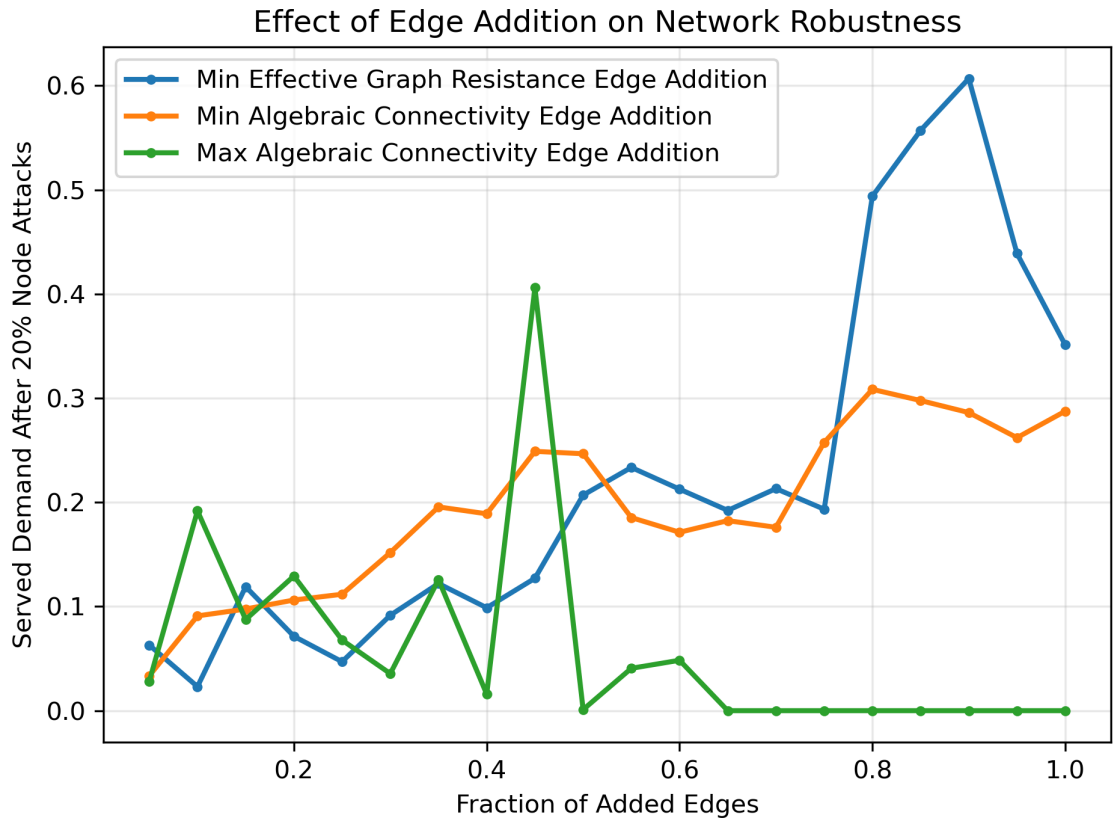

Figure 4.8: This figure shows the served demand after removing 20% of nodes with node degree attack in the Nordic power grid graph against the fraction of added edges.

4.2.2 Highest Degree Node Attack

The robustness improvement of the Nordic graph after edge addition algorithms is evaluated after a node attack on the highest degree nodes. According to the topological robustness metric *LCS*, the max algebraic connectivity edge addition algorithm performs the best, see figure 4.9. When 20% of the nodes are removed, over 60% of its largest component still remains intact. The other two algorithms perform worse than the random baseline edge addition.

According to the electrical robustness metric *SPD*, all edge addition algorithms performed better than random for most part, see figure 4.10. They all experience an initial drop of served power demand as the first node is removed.

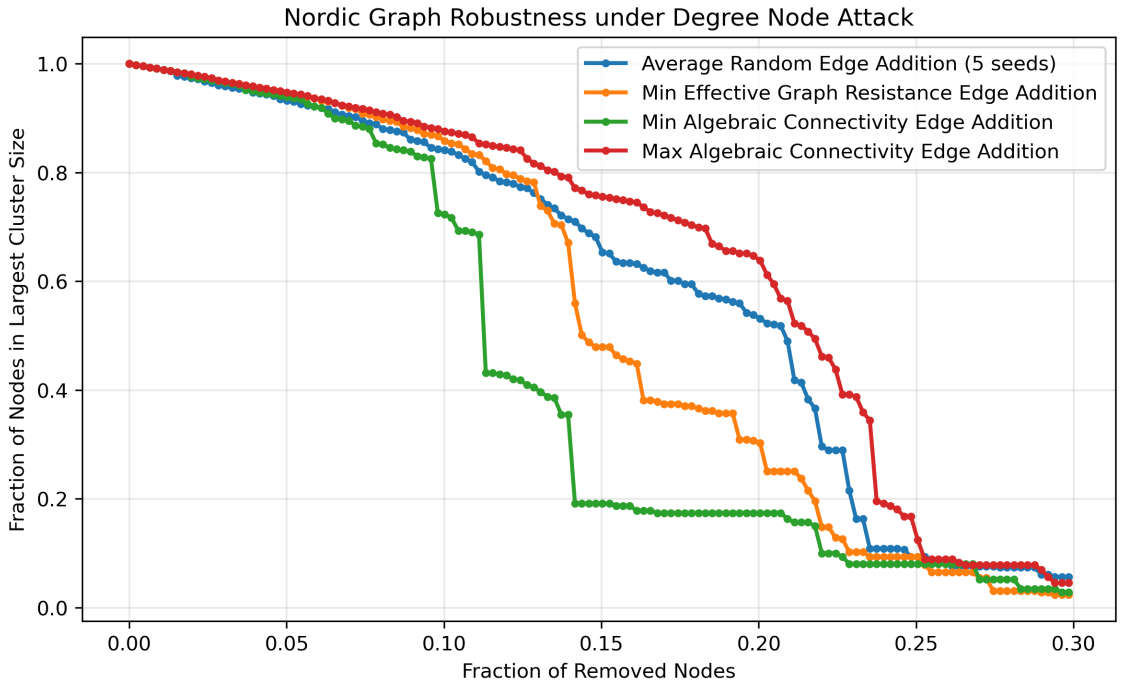

Figure 4.9: Four edge addition algorithms with 15% of total edges added measured with the robustness metric largest cluster size under degree node removal on the Nordic grid dataset.

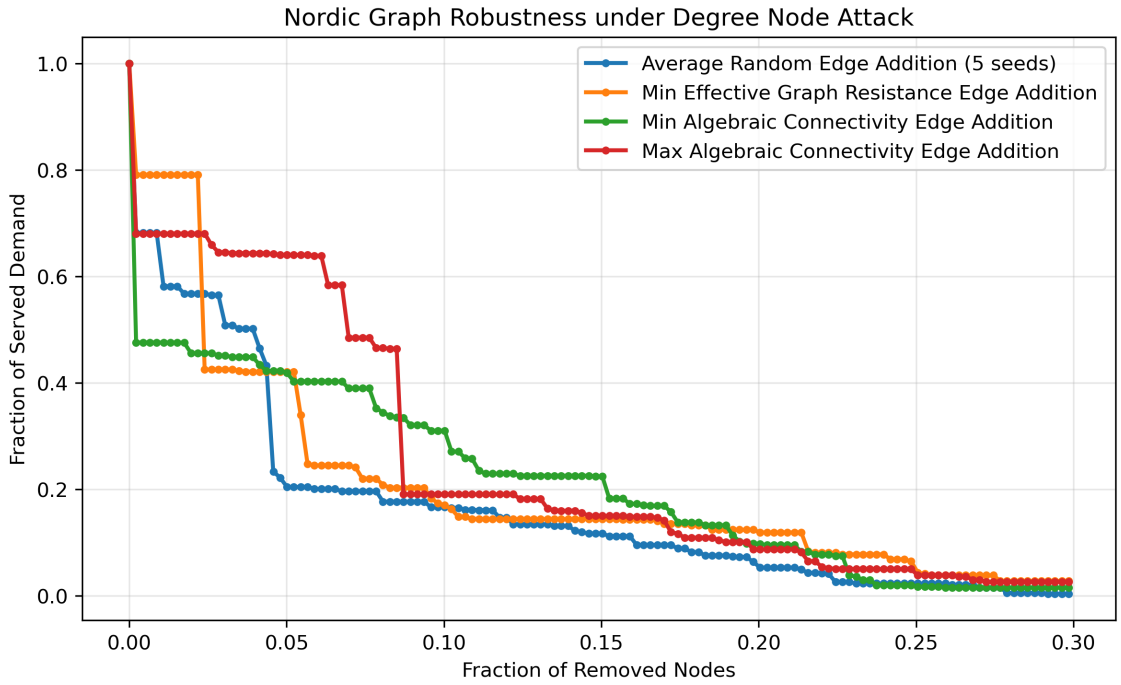

Figure 4.10: Four edge addition algorithms with 15% of total edges added measured with the robustness metric served demand under degree node removal on the Nordic grid dataset.

4.2.3 Electrical Node Significance Attack

The robustness improvement of the Nordic graph after edge addition algorithms was also evaluated after a node attack on the most electrical significant nodes. According to the topological robustness metric LCS, all edge addition algorithms struggled to perform better than random and min algebraic connectivity was way below, see figure 4.11.

According to the electrical robustness metric SPD, max algebraic connectivity performed better than the others in the beginning of the attack, see figure 4.12. The other algorithms show no improvement compared to random.

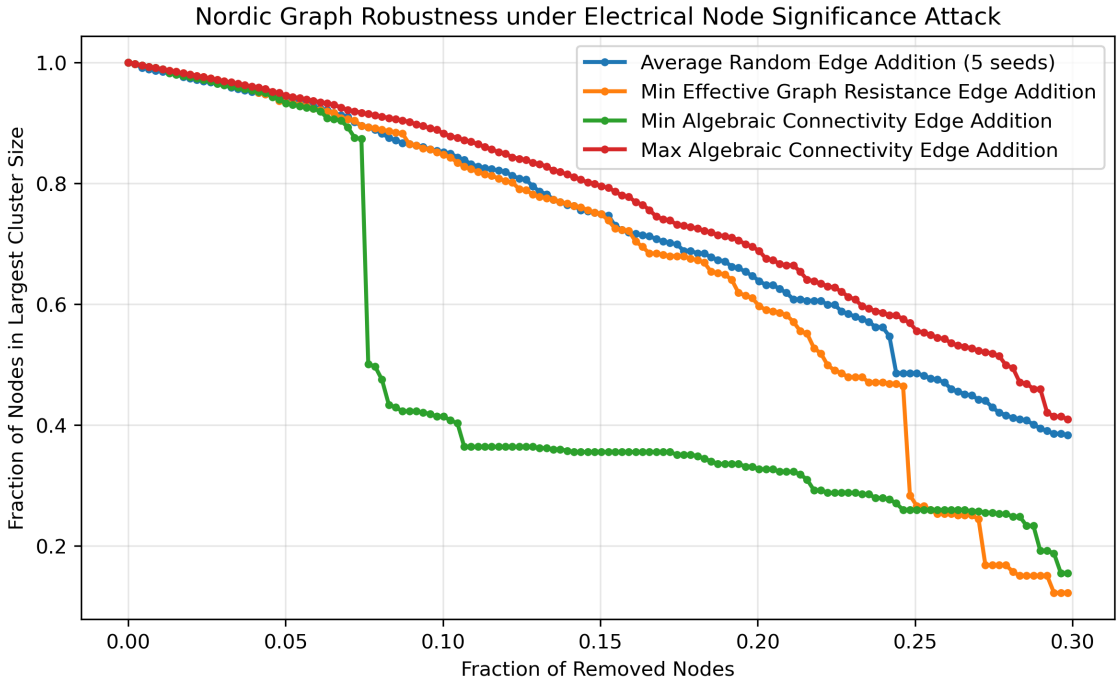

Figure 4.11: Four edge addition algorithms with 15% of total edges added measured with the robustness metric largest cluster size under most electrical node significance removal on the Nordic grid dataset.

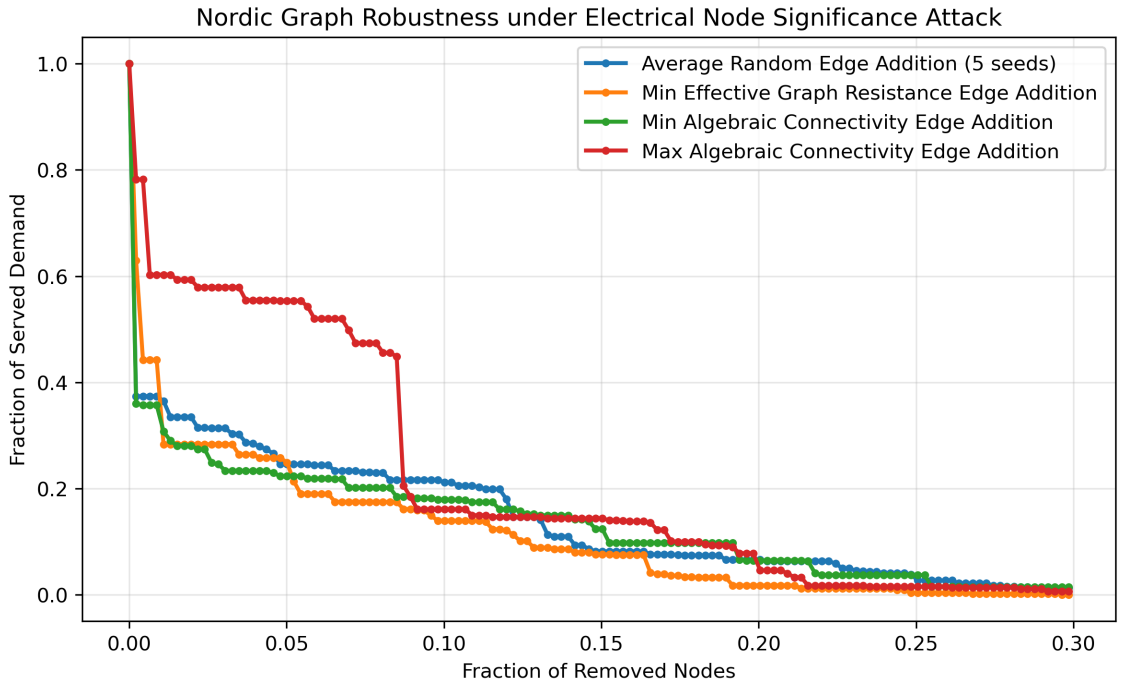

Figure 4.12: Four edge addition algorithms with 15% of total edges added measured with the robustness metric served demand under most electrical node significance removal on the Nordic grid dataset.

4.2.4 Network Findings

After the edge addition algorithms, the grids were attacked with multiple node removals. The removed node that caused the greatest drop in served power demand percentage points for each algorithm and attack, can be found in table 4.2. The table can be interpreted as explained in section 4.1.5. Minimizing algebraic connectivity experienced the biggest drops in SPD. It can also be seen in the column "Removed (counts)" that max algebraic connectivity experienced its biggest drop in SPD after many node removals, indicating that no specific node was the most vulnerable. In the overloaded lines column, it can be seen that the cascading effects are very large, causing as much as 245 lines to be overloaded. The total amount of lines in the whole graph is 742, which means that specific node removals disabled 33% of the grid, which indicates that the grid has very vulnerable nodes. Additionally, the graphs where the first node removal caused the largest drop in SPD consequently became severely fragmented, as can be seen in the "Comp" column. Some of the graphs resulted in over 100 separated islands.

Algorithm	Attack	Removed (count)	Node id	Comp	Overloaded	SPD Drop (pp)
Min R_G	max d_i	11	17	67	88	37
Min $\lambda_2(L)$	max d_i	1	272	86	190	52
Max $\lambda_2(L)$	max d_i	1	272	51	153	32
Min R_G	γ_i	1	347	53	128	37
Min $\lambda_2(L)$	γ_i	1	28	107	245	64
Max $\lambda_2(L)$	γ_i	40	358	121	111	24

Table 4.2: This table shows graph data for the node that caused the biggest drop in served power demand in percentage points (pp) when attacked for the different algorithms. The table is for the Nordic power grid graph.

4.3 Overview of Results

A summary and overview of the edge addition algorithm performances can be found in table 4.3 and 4.4 for easier comparison of the results. The table shows the relative improvements of the area under the robustness curve compared to the random baseline according to formula 3.1, in regards to a certain metric and attack. Green indicates that the edge addition algorithm performed better than random in terms of the robustness metric, and red indicates the opposite. In both tables, the absolute performance levels of robustness vary across attack scenarios and can instead be observed in the result plots.

Table 4.3 is structured in a hierarchical way. The first level separates the results into two cases: the standard IEEE 118 network and the IEEE 118 increased cascading risk scenario. Within each case, results are further divided by attack type, where max d_i and γ_i respectively stands for degree node attack and electrical node significance attack, see section 2.4. For each attack type, results are further divided by robustness metric: ***LCS*** and ***SPD***, see section 2.2. Consistent with the notation used throughout this report, R_G denotes effective graph resistance and $\lambda_2(L)$ denotes algebraic connectivity. Effective graph resistance shows the overall best performance in the IEEE test grid. Table 4.4 is structured similarly except for the first level of the hierarchical structure, which only contains the Nordic power grid. Max algebraic connectivity shows the overall best performance in the Nordic grid.

Graph	IEEE 118				IEEE 118 Cascading Risk			
Attack type	γ_i		Max d_i		γ_i		Max d_i	
Metric	***LCS***	***SPD***	***LCS***	***SPD***	***LCS***	***SPD***	***LCS***	***SPD***
Min R_G	+15%	+32%	+11%	+26%	+6%	-11%	+10%	+37%
Max $\lambda_2(L)$	+1.2%	-6.4%	+23%	+3.4%	+2%	-31%	+20%	-15%
Min $\lambda_2(L)$	-33%	-25%	-18%	-25%	-33%	+53%	-18%	+150%

Table 4.3: This table shows a summary of the results of the relative improvements of the area under the robustness curve compared to the random baseline from the IEEE 118 graph.

Graph	Nordic			
Attack type	γ_i		Max d_i	
Metric	*LCS*	*SPD*	*LCS*	*SPD*
Min R_G	-7.5%	-23%	-10%	+23%
Max $\lambda_2(L)$	+5%	+52%	+9%	+50%
Min $\lambda_2(L)$	-34%	-7%	-27%	+28%

Table 4.4: This table shows a summary of the results of the relative improvements of the area under the robustness curve compared to the random baseline from the Nordic power grid graph.

Chapter 5
Discussion

5.1 Minimizing Effective Graph Resistance

Minimizing effective graph resistance performed well across most attack scenarios and metrics in the IEEE 118 test grid, see table 4.3. It also experienced the smallest drop in SPD compared to the other algorithms, see table 4.1. It supports the fact that effective graph resistance captures both electric and structural graph properties. However, this trend did not hold for the Nordic grid as it demonstrated worse or around the performance level of random, apart from one experiment, see table 4.4. A possible contributing factor to the poorer results might be that the IEEE 118 power grid does not reflect geographical properties and all edges have a distance of 1 km, affecting the weighted Laplacian matrix. In contrast, the Nordic grid has realistic transmission distances and the computed edge weight reflects this. Especially since the effective resistance algorithm is influenced by edge weights and path lengths, it behaves very differently in the more realistic setting.

It might also be explained by a different load-node ratio. The Nordic graph has a much lower load-node ratio compared to the IEEE 118 graph. Since effective graph resistance only accounts for line impedance values and does not consider actual load and generation values, improving flow distribution through minimizing effective graph resistance did not necessarily translate into improved load accessibility and served demand. Effective resistance edge addition appears to fail to capture nodal importance and seems to be less suited for networks with a smaller load-node ratio. This could be further studied by comparing graphs with the same load-node ratio to possibly isolate the effect of load ratio.

Interestingly, the effective graph resistance algorithm was the best preforming algorithm in the IEEE 118 graph against the electrical significance attack, see figure 4.4 and 4.5. It might suggest that the grid can survive an electrical attack slightly better when the robustness is optimized with electrical properties in consideration. However, extensive and real power data is rarely publicly available information.

5.2 Maximizing Algebraic Connectivity

As mentioned in the background, maximizing algebraic connectivity makes it harder to disconnect the grid. Consequently, more nodes needed to be removed to disintegrate the graph into multiple components and decrease the largest cluster size, thus making it more robust. The ***LCS*** metric reflects how the topology of the grid changes when attacked, but considers no cascading effects. Max algebraic connectivity always outperformed min algebraic connectivity in regards to ***LCS*** with both attacks, in all datasets. Max algebraic connectivity was generally more robust compared to random against the high node degree attack than electrical significant attack in regards to ***LCS*** in the IEEE graph, see table 4.1 and table 4.3. This is most likely due to it being topological metrics and ***LCS*** not accounting for power flow distribution. However, to draw any definitive conclusions, further validation would require experiments on graphs with more similar network properties, to isolate variations in algebraic connectivity and the affect of the the remaining largest cluster size under different attack strategies.

Maximizing algebraic connectivity generally performed low on ***SPD*** in the IEEE 118 test grid but very high on the Nordic grid, see table 4.3 and 4.4. The worse performance could suggest a lacking aspect of accounting for electrical parameters when optimizing based on max algebraic connectivity. On the other hand, a better performance in the Nordic grid could suggest structural differences in realistic and synthetic grids, such as more vulnerable edges in the Nordic grid. This indicates that the Nordic graph perhaps had more room for improvement in terms of connectivity than the already robust IEEE graph. The Nordic graph is almost four times less dense than the IEEE 118 network, meaning that only a small fraction of all possible edges are present in the graph, see equation 2.3. Maximizing algebraic connectivity identifies edges that connect components, which might only have marginal gain in an already better connected graph, compared to a random baseline. This seems to affect served demand more than keeping the largest cluster size intact.

Increasing connectivity in the IEEE graph in regards to ***SPD*** showed worse performance against attacks than random, suggesting high connectivity increased the risk of cascading failures. However, it is hard to say if these results are topology-dependent or the effect of interactions with other structural properties.

5.3 Minimizing Algebraic Connectivity

In the IEEE test grid, min algebraic connectivity showed poor robustness performance against all metrics and attack scenarios. This could suggest that optimizing for low connectivity makes the graph weaker against attacks. However, there were no overloaded lines or cascading failures in the IEEE 118 test grid due to very high line capacity. Hence, the IEEE 118 test grid fails to capture real cascading effects and min algebraic connectivity instead performed worse than the baseline. The more realistic Nordic grid on the other hand, experienced overloaded lines and cascading failure when attacked. The minimized algebraic connectivity algorithm performed better than random against highest node degree attack in regards to ***SPD***, see figure 4.10. Since the served demand metric better captures robustness against cascading effects than the topological metric ***LCS***, it could suggest a potential relationship between minimizing connectivity and mitigating cascading failure. To further

investigate this, the line capacities in the IEEE test grid were reduced, in order to capture more strained operational conditions, see section 3.3.1. It resulted in cascading effects and an overall fast degradation of the power grid, see figure 4.6 and 4.7. However, these extreme operational conditions allowed for further insight into the behavior of the algorithms. It can be observed that the algorithm that minimizes algebraic connectivity outperformed all other algorithms against both attacks, in regards to ***SPD*** in the IEEE 118 with increased cascading risk. This is unlike the known strong association between a highly connected network and increased robustness. This could indicate that cascading events might be less severe in grids with increased cascading risk, when optimizing for minimized algebraic connectivity.

In the Nordic grid, the min algebraic connectivity algorithm performs well in terms of ***SPD*** under degree node attack, but poorly with respect to ***LCS***, see table 4.4. This could suggest a trade-off between maintaining overall served power demand (the grid's electricity demand is met) and preserving network connectivity (how much of the grid actually has power), under attack scenarios. It appeared like the algorithm prioritized keeping served demand high in remaining connected regions at the expense of increased fragmentation of the grid.

5.4 Baseline

Random edge addition was used as a baseline to compare the different edge addition algorithms' performances. Recall that adding edges to a graph always increases connectivity and decreases effective graph resistance. As discussed in section 3.7, random edge addition therefore allows the optimization strategy to be isolated from the effect of simply adding edges to a graph. However, random edge addition contributes to creating a more random network structure which in some cases seems to give around or even better performances than other edge addition algorithms, see for example figure 4.11. It adds new pathways that sometimes select edges with small and sometimes big connectivity gains, producing a mixture of possible improvements. This suggests that random network structures, with no regard to power grid properties, could add robustness against different attack and cascading scenarios. Another reason for its good performance compared to the other algorithms might be explained by the fact that the network may already possess sufficient connectivity, reducing the advantage of targeted selected edge additions.

Furthermore, another interesting baseline to compare to would have been the optimal edge addition, that is obtained from an exhaustive search. It would quantify how much performance is lost by using a greedy algorithm. However, this is of course only possible for smaller graphs due to it being extremely computationally heavy.

5.5 Adding More Edges

The results of increasing the number of added edges, show that adding more edges to the graph can both improve and reduce robustness in terms of served demand in a power grid, see sections 3.6 and 4.2.1. When the algorithm optimizes for effective resistance, no critical number of edges seemed to be catastrophic for the first 100% of added edges in the IEEE 118 graph, see figure 4.1. Recall that the percentage reflects the proportion of the number

of edges present in the original graph, $|E|$, not the number of candidate edges. The same increase in robustness was not seen in the Nordic graph, see figure 4.8. This could be another possible factor to why min effective resistance performs worse in the Nordic grid, as it seems it would have needed more edges. Furthermore, maximizing algebraic connectivity decreased severely in robustness after the addition of 20% of edges in the IEEE 118 graph. This suggests that the number of added edges and graph connectivity, can have a critical effect on served power demand. A possible reason for this is that the graph becomes too connected and high degree nodes become extremely critical. Minimizing algebraic connectivity when adding edges slowly increased power grid robustness in both graphs. Adding more than 100% of edges to further investigate this behavior could potentially be interesting, but less realistic in terms of power grid expansion. The addition of 15% of edges in the study was a reasonable trade-off between robustness and a realistic budget in the IEEE 118 graph, but maybe should have been bigger for the Nordic grid.

Chapter 6
Conclusions

In our study, three greedy edge addition algorithms have been compared and evaluated under different robustness metrics and attack scenarios. DC power flow calculations allowed cascading simulations to model overloaded lines and power grid disruption. The study was conducted on a synthetic IEEE test grid and the Nordic power grid to provide a more realistic dataset that better reflect actual system conditions and power network behavior. This study contributed with further knowledge about potential robust transmission expansion. The obtained results allow the research questions to be addressed as follows.

- RQ1: How do different edge addition algorithms differ in their ability to increase the robustness of electric power networks under budget constraint of edges?

The results showed that the number of added edges can both improve and reduce the robustness of a graph depending on the metric that is being optimized, as well evaluation method. This means that a thorough analysis should be conducted regarding the number of edges to be added when expansion plans are made. Max algebraic connectivity showed to be the most sensitive to this as adding more edges could severely decrease robustness in regards to ***SPD***. Minimizing effective resistance increased robustness across different scenarios, suggesting good ability to exploit structural or electrical information of the network. However, it possibly showed some weakness to a graph with low load-node ratio. Both minimizing and maximizing algebraic connectivity showed potential to increasing robustness, depending on the level of cascading risk. It suggests a complex relationship between connectivity and power flow.

- RQ2: Which of the edge addition algorithms is most suitable from a robustness perspective depending on the type of attack it is exposed to and the size of the graph?

Max algebraic connectivity increases connectivity and creates more pathways for power to flow, resulting in performing well when evaluated on ***LCS*** and strength against node removal of the highest degree nodes. This is true for the synthetic IEEE 118 graph which is

less dense, has a higher node-load ratio and more arbitrary structure than the Nordic grid. It can be observed that the combination of ***SPD*** and high cascading risk in the IEEE 118 grid is most robust against both attacks when minimizing algebraic connectivity. Min effective resistance showed best overall steady robustness across different attacks and metrics in the IEEE 118 graph. Performing best in the bigger Nordic graph was max algebraic connectivity, suggesting a better possibility of improving less connected networks. All algorithms performed better than random baseline in the Nordic grid in regards to ***SPD*** when high degree nodes were removed. In summary, algorithm performances seems to be influenced by multiple factors and the most suitable algorithm from a robustness perspective would then depend on its application context. The results of this study indicate that we might have to be careful about generalizing results from synthetic test networks to realistic transmission grids. The following section will further discuss the limitations of this study and the need for future research.

6.1 Limitations and Future Work

The findings should not be interpreted as definitive but rather as indications of certain trends within the scope of the experimental approach. Some algorithms showed only marginal improvement over random selection of edges in some attack scenarios, perhaps showing the limitations of a greedy algorithm and approximations of robustness metrics. To further study the nature of robust power grids, less approximate algorithms such as integer linear programming could be applied, to capture the optimal combination of added edges. Another limitation to this work could be the evaluation metric area under the robustness curve. It gives an overall comparison to the random baseline, but may fail to capture important differences through out the progression of attacks. Two algorithms may have the same area, but one performs well in the beginning while the other is stronger in later stages.

Another limitation to this study is not being able to generalize the results to other grids, due to the small number of datasets. It was therefore difficult to draw definitive conclusions in regards to explaining the performance outcomes. One reason for that is that multiple variables are studied at the same time. We can improve this by isolating certain variables and further study the behavior of these algorithms. We would have to obtain or create graphs with the same properties and structure, thus only looking at one network property at a time, such as graphs with the same graph density, connectivity or load-node ratio. Furthermore, we would improve the work by applying the experiments on more graphs, to obtain more data and perhaps then be able to give more conclusive findings.

There were some possible threats to the validity of this study. One threat could be the allocation decisions regarding location of generators and loads. The Nordic power grid dataset had no available coordinates for generators and loads, only the regions to which they belonged. They were therefore assigned random locations within their respective regions using a fixed random seed. Consequently, their exact locations are artificial and may be different from the real Nordic grid. This could result in the generators being more or less vulnerable than in the real grid since now the topology is not necessarily designed to protect the generators. Another possible threat to the validity is during the conversion of the Nordic power grid, for details about the conversion, see section 3.4.3. There was some handling of missing values and framework specific choices were made, such as where to place the slack

bus. Different choices could possibly slightly change the simulation results. However, most decisions were based on how previous studies had approached similar situations.

Some other limitations to this study includes more realistic aspects such as economic constraints and addition of new generation, which are relevant in modern transmission planning. Another example is security regulations like protection systems and operator response as real time damage control of cascading events. These aspects are left for future work, to provide further knowledge of power grid robustness.

References

[1] H. Chen, L. Jin, M. Wang, L. Guo, and J. Wu, "How will power outages affect the national economic growth: Evidence from 152 countries," *Energy Economics*, vol. 126, p. 107055, 2023.

[2] L. Cuadra, S. Salcedo-Sanz, J. Del Ser, S. Jiménez-Fernández, and Z. W. Geem, "A critical review of robustness in power grids using complex networks concepts," *Energies*, vol. 8, no. 9, pp. 9211–9265, 2015.

[3] M. Waseem and S. D. Manshadi, "Electricity grid resilience amid various natural disasters: Challenges and solutions," *The Electricity Journal*, vol. 33, no. 10, p. 106864, 2020.

[4] H. Cetinay, K. Devriendt, and P. Van Mieghem, "Nodal vulnerability to targeted attacks in power grids," *Applied Network Science*, vol. 3, no. 34, 2018.

[5] International Energy Agency, "Electricity 2026," Feb 2026. `https://www.iea.org/reports/electricity-2026`, Accessed: 2026-02-18.

[6] Svenska kraftnät, "Network development plan 2026-2035," 2025. Available at: `https://www.svk.se/om-oss/rapporter-och-remissvar/natutvecklingsplan/`, Accessed: 2026-02-18.

[7] International Energy Agency (IEA), "Russia's attacks on ukraine's energy sector have escalated again as winter sets in," Feb 2024. `https://www.iea.org/commentaries/russias-attacks-on-ukraines-energy-sector-have-escalated-again-as-winter-sets-in`, Accessed: 2026-02-18.

[8] Svenska kraftnät, "Power system operational security: future needs and abilities," August 2025. `https://www.svk.se/4ae285/siteassets/om-oss/rapporter/2025/power-system-perational-security.pdf`, Accessed: 2026-02-18.

[9] K. Shafiei, S. G. Zadeh, and M. T. Hagh, "Power system resilience enhancement using graph learning: A comprehensive robustness and antifragility approach," *Sustainable Energy, Grids and Networks*, vol. 43, p. 101927, 2025.

[10] M. Kamran, "Fundamentals of smart grid systems (chapter 3 - power grids)," pp. 71–131, 2023. https://www.sciencedirect.com/science/article/pii/B9780323995603000053.

[11] M. Tomassini, "Rewiring or adding links: A real-world case study of network vulnerability," *Physica A: Statistical Mechanics and its Applications*, vol. 630, p. 129241, 2023.

[12] Y. Koç, M. Warnier, P. V. Mieghem, R. E. Kooij, and F. M. Brazier, "The impact of the topology on cascading failures in a power grid model," *Physica A: Statistical Mechanics and its Applications*, vol. 402, pp. 169–179, 2014.

[13] S. Lonapalawong, J. Yan, J. Li, D. Ye, W. Chen, Y. Tang, Y. Huang, and C. Wang, "Reducing power grid cascading failure propagation by minimizing algebraic connectivity in edge addition," *Frontiers of Information Technology & Electronic Engineering*, vol. 23, no. 3, pp. 382–397, 2022.

[14] R. E. Kooij and M. A. Achterberg, "Minimizing the effective graph resistance by adding links is np-hard," *Operations Research Letters*, vol. 51, no. 6, pp. 601–604, 2023.

[15] M. Predari, L. Berner, R. Kooij, *et al.*, "Greedy optimization of resistance-based graph robustness with global and local edge insertions," *Social Network Analysis and Mining*, vol. 13, 2023.

[16] Z. Nekudari and A. Ghasemi, "The effect of increasing the algebraic connectivity on cascading failures in power grid networks," in *2021 26th International Computer Conference, Computer Society of Iran (CSICC)*, pp. 1–4, 2021.

[17] University of Washington, "Power systems test case archive," n.d. https://www2.ee.washington.edu/research/pstca/pf118/pg_tca118bus.htm, Accessed: 2026-05-11.

[18] M. Doostinia, D. Falabretti, G. Verticale, and S. Bolouki, "Critical node identification for cyber–physical power distribution systems based on complex network theory: A real case study," *Energies*, vol. 18, no. 11, 2025.

[19] P. C. Socievole, A., "Comparative evaluation of strategies for improving the robustness of complex networks," *Applied Network Science*, vol. 8, no. 3, p. 43, 2023.

[20] F. R. K. Chung, *Spectral Graph Theory*. No. 92 in CBMS Regional Conference Series in Mathematics, American Mathematical Society, 1997.

[21] J. C. A. Barata and M. S. Hussein, "The moore-penrose pseudoinverse: A tutorial review of the theory," *Brazilian Journal of Physics*, vol. 42, pp. 146–165, 2012.

[22] H. D. Bedru, S. Yu, X. Xiao, D. Zhang, L. Wan, H. Guo, and F. Xia, "Big networks: A survey," *Computer Science Review*, vol. 37, p. 100247, 2020.

[23] M. Oehlers and B. Fabian, "Graph metrics for network robustness—a survey," *Mathematics*, vol. 9, no. 8, 2021.

[24] D. Zhou, F. Hu, S. Wang, and J. Chen, "Power network robustness analysis based on electrical engineering and complex network theory," *Physica A: Statistical Mechanics and its Applications*, vol. 564, p. 125540, 2021.

[25] A. Sydney, C. Scoglio, and D. Gruenbacher, "Optimizing algebraic connectivity by edge rewiring," *Applied Mathematics and Computation*, vol. 219, no. 10, pp. 5465–5479, 2013.

[26] Y. Liu, E. K. P. Chong, and A. Pezeshki, "Submodular optimization problems and greedy strategies: A survey," *Discrete Event Dynamic Systems*, vol. 30, pp. 381–412, 2020.

[27] A. Ghosh and S. Boyd, "Growing well-connected graphs," in *Proceedings of the 45th IEEE Conference on Decision and Control*, pp. 6605–6611, 2006.

[28] S. Tauch, W. Liu, and R. Pears, "Measuring cascade effects in coupled networks using algebraic connectivity," in *2014 Australasian Telecommunication Networks and Applications Conference (ATNAC)*, pp. 34–39, 2014.

[29] D. Mosk-Aoyama, "Maximum algebraic connectivity augmentation is np-hard," *Operations Research Letters*, vol. 36, no. 6, pp. 677–679, 2008.

[30] Svenska kraftnät, "Säkerhetsskydd," 2025. Accessed: 2026-06-09.

[31] E. I. Bilis, W. Kröger, and C. Nan, "Performance of electric power systems under physical malicious attacks," *IEEE Systems Journal*, vol. 7, no. 4, pp. 854–865, 2013.

[32] Y. Koç, M. Warnier, R. E. Kooij, and F. M. Brazier, "A robustness metric for cascading failures by targeted attacks in power networks," in *2013 10th IEEE International Conference on Networking, Sensing and Control (ICNSC).*, pp. 48–53, 2013.

[33] L. Thurner, A. Scheidler, F. Schäfer, J.-H. Menke, J. Dollichon, F. Meier, S. Meinecke, and M. Braun, "Pandapower—an open-source python tool for convenient modeling, analysis, and optimization of electric power systems," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6510–6521, 2018.

[34] K. Purchala, L. Meeus, D. Van Dommelen, and R. Belmans, "Usefulness of dc power flow for active power flow analysis," in *Power Engineering Society General Meeting, 2005. IEEE*, IEEE, 2005.

[35] R. Sanchez-Garcia, M. Fennelly, S. Norris, and N. Wright, "Hierarchical spectral clustering of power grids," *IEEE Transactions on Power Systems*, vol. 29, pp. 2229–2237, Sept. 2014.

[36] A. A. Hagberg, D. A. Schult, and P. J. Swart, "Exploring network structure, dynamics, and function using networkx," in *Proceedings of the 7th Python in Science Conference (SciPy 2008)* (G. Varoquaux, T. Vaught, and J. Millman, eds.), (Pasadena, CA, USA), pp. 11–15, August 2008.

[37] A. Salehpour, I. Al-Anbagi, K.-C. Yow, and X. Cheng, "Modeling cascading failures in coupled smart grid networks," vol. 10, pp. 81054–81070, 2022.

[38] D. L. Pepyne, "Topology and cascading line outages in power grids," *Journal of Systems Science and Systems Engineering*, vol. 16, p. 202–221, 2007.

[39] Illinois Center for a Smarter Electric Grid (ICSEG), "IEEE 118-Bus System," n.d. https://icseg.iti.illinois.edu/ieee-118-bus-system/, Accessed: 2026-05-11.

[40] T. Brown, J. Hörsch, and D. Schlachtberger, "PyPSA: Python for Power System Analysis," *Journal of Open Research Software*, vol. 6, no. 4, 2018.

[41] Wikimedia Commons, "File:blank map europe with borders.png," 2026. https://commons.wikimedia.org/wiki/File:Blank_map_Europe_with_borders.png, Accessed: 2026-05-11.

[42] N. R. Watson and J. D. Watson, "An overview of hvdc technology," *Energies*, vol. 13, no. 17, 2020.

[43] A. Exposito, J. Ramos, and J. Santos, "Slack bus selection to minimize the system power imbalance in load-flow studies," *IEEE Transactions on Power Systems*, vol. 19, no. 2, pp. 987–995, 2004.

[44] S. Forsberg, K. Thomas, and M. Bergkvist, "Power grid vulnerability analysis using complex network theory: A topological study of the nordic transmission grid," *Physica A: Statistical Mechanics and its Applications*, vol. 626, p. 129072, 2023.

[45] Svenska kraftnät, "Om transmissionsnätet," 2026. https://www.svk.se/om-kraftsystemet/om-transmissionsnatet/Accessed: 2026-05-20.

[46] M. Tian and P. Moriano, "Robustness of community structure under edge addition," *Phys. Rev. E*, vol. 108, p. 054302, Nov 2023.

Appendices

INSTITUTIONEN FÖR DATAVETENSKAP | LUNDS TEKNISKA HÖGSKOLA | PRESENTERAD 2026-06-05

EXAMENSARBETE A Comparative Study of Edge Addition Algorithms for Power Grid Robustness
STUDENTER Sandra Christoffersen, Gina Christoffersen
HANDLEDARE Jonas Skeppstedt (LTH)
EXAMINATOR Flavius Gruian (LTH)

Robustare elnät med strategiska förbindelser

POPULÄRVETENSKAPLIG SAMMANFATTNING **Sandra Christoffersen, Gina Christoffersen**

Kraftnät runt om i världen står inför stora expansionsplaner på grund av det ökade energibehovet. Detta examensarbete jämför olika algoritmer som stegvis lägger till nya gynnsamma förbindelser för att skapa ett robustare kraftnät mot riktade attacker och kaskadfel.

En stor utbyggnad av elkraftnätet förväntas i stora delar av världen till följd av ett växande energibehov och ett föråldrat kraftnät. Robusthet är en viktig aspekt av det kommande planeringsarbetet för en stabil energiförsörjning. Riktade attacker från främmande makter angriper ofta de mest kritiska delarna av kraftnätet för att förstöra så mycket som möjligt och utlösa stora strömavbrott. En attack mot en viktig station innebär att alla dess direkt kopplade förbindelser sätts ur funktion och flödet av el måste omfördelas. Detta kan orsaka att ledningar blir överbelastade och skyddssystem kopplar bort dem. Fel kan då sprida sig genom nätet och skapa mer problem på nya ställen vilket innebär att en kaskad har utlösts. Hur kan man bygga elkraftnät mer motståndskraftigt mot den typen av angrepp?

Det finns många möjliga kombinationer för att lägga till ett antal nya elledningar till elnätet. Problemet kan modelleras som ett nätverk, det vill säga en graf av noder och länkar vilka representerar elstationer och elledningar. Uppgiften är då att hitta två optimala noder att placera en ny länk mellan. En metod är att optimera för ett robusthetsmått; ett mått som mäter ett systems förmåga att upprätthålla funktion efter störningar eller attacker. Ett sådant mått är effektivt grafmotstånd som beskriver hur vissa vägar i ett nätverk har mer motstånd mot energiflöde. Ett annat mått är algebraisk sammankoppling som beskriver hur väl anslutet ett nätverk är. Att lägga till fler länkar i en graf ökar alltid hur tätt ihopkopplat den är. Frågan är: ska vi välja en länk som minimerar eller maximerar ökningen av sammankoppling? Å ena sidan vill vi ha fler kopplingar för att förhindra risken att nätverket splittras upp i flera delar vid ett angrepp. Å andra sidan vill vi inte ha för många förbindelser som skulle kunna underlätta en potentiell spridning av kaskadfel.

Vårt examensarbete undersöker sambandet mellan hur sammankopplad en graf är, energiflöden och kaskadfel. Detta gör vi genom att jämföra tre olika algoritmer som lägger till nya länkar under olika attackscenarier. Vi modellerar det nordiska elnätet med realistisk data för att hitta eventuella skillnader jämfört med syntetiska nät. Resultaten av vår studie tyder på att både minimering och maximering av nätverkets sammankoppling kan öka robustheten i olika attackscenarier, beroende på grafstruktur och nivå av kaskadrisk.