Optimized network robustness and dismantling

Bruno Diogo Mesquita de Sousa

Thesis to obtain the Master of Science Degree in

Information Systems and Computer Engineering

Supervisors: Prof. Francisco João Duarte Cordeiro Correia dos Santos
Prof. José Rui De Matos Figueira

Examination Committee

Chairperson: Prof. Daniel Jorge Viegas Gonçalves
Supervisor: Prof. Francisco João Duarte Cordeiro Correia dos Santos
Member of the Committee: Prof. Alexandre Paulo Lourenço Francisco

January 2021

Acknowledgements

I would like to thank Professor Francisco Correia dos Santos and Professor José Rui Figueira for the help and support they provided me with while working on this dissertation.

I would also like to thank my family and friends for their continued support throughout these last five interesting years at Instituto Superior Técnico.

to my grandparents Lídia and Francisco,

Resumo

Muitos dos sistemas sociais, económicos e biológicos, presentes no nosso dia-a-dia, podem ser modelados como redes complexas. O aumento da complexidade da nossa sociedade, como consequência direta do progresso tecnológico e ciêntifico nas últimas decadas, tem levado a que muitos destes sistemas se tenham tornado dependentes entre si. Assim, torna-se mais adequado modelar estes sistemas usando redes complexas multi-camada, em vez de redes complexas de uma só camada, de forma a facilitar a análise de como estes sistemas interagem entre eles. Uma vez que é crucial garantir que estes sistemas funcionem corretamente, mesmo que sofram ataques ou falhas aleatórias, é importante estudar as propreidades de robustez destas redes. Esta tese adopta duas abordagens distintas para o estudo da robustez de redes multiplex com duas camadas. A primeira abordagem analisa o impacto que diferentes distribuições de grau têm na robustez destas redes. Os resultados obtidos indicam que as propriedades de robustez que as distribuições de grau manifestam em redes de uma só camada, estão igualmente presentes em redes multiplex. Enquanto que redes com duas camadas scale-free são robustas contra falhas aleatórias e frágeis contra ataques intencionais, redes com duas camadas exponênciais demonstram o comportamento oposto. Redes com uma camada scale-free e uma camada exponencial demonstram robustez elevada contra ataques intencionais e falhas aleatórias, reduzindo as fragilidades que cada uma das distribuições de grau exibem quanto estão isoladas. A segunda abordagem desta tese, usando algoritmos de optimização, um método de religação e uma nova forma de medir robustez em redes multiplex, mostrou resultados promissores no aumento da robustez. Optimizar a robustez de uma camada da rede, R_l, leva a um aumento da robustez global da rede multiplex, R_d, até 17%, o que indica que a robustez de cada camada isolada tem impacto na robustez global da rede. Contudo, a optimização da robustez global, R_d, não leva necessáriamente ao aumento da robustez das camadas, podendo mesmo torná-las mais frágeis, podendo levar a uma redução de até 10%. Optimização multi-objetivo mostrou ser eficáz, levando a uma melhoria de ambas as medidas de robustez de até 52% para R_l e 24% para R_d, sugerindo que é possivel optimizar, simultaneamente, a robustez das camadas individuais e de toda a rede multiplex.

Abstract

Many relations and interdependences in social, economic and biological systems can be modeled and studied as complex networks. As a consequence of technological and scientific progress in recent decades, our society's increased complexity has led many of these systems to become interconnected. As such, it becomes more suitable to transition from single-layer networks to multi-layer networks as a way to properly represent, analyze and study the different relationships between these systems. Since these systems must work in environments where random failures or hostile attacks may occur, it becomes of utmost importance to study the robustness of these complex, multidimensional topologies. This dissertation presents two approaches to study the robustness of multiplex networks with two layers. The first approach focuses on studying how the combination of distinct degree distributions impact the robustness of multi-layer networks. We show that the robustness properties associated with single-layer degree distributions also manifest on multi-layer networks. In particular, while networks with two scale-free layers are robust to random failures and fragile to targeted attacks, networks with two exponential layers show the opposite behaviour. We further show that combining a layer with a scale-free degree distribution, and another with a homogeneous degree distribution, whether it be an Erdös-Rényi layer or a lattice layer, displays significantly improved robustness to both random failures and targeted attacks, effectively reducing the fragilities observed when both layers have the same degree distribution. In the second part of this thesis, we show that simple optimization algorithms — combined with rewiring and a novel robustness measure adapted to multi-layer networks — offer promising results on improving the robustness of these multidimensional structures. Optimizing the robustness of one layer, R_l, leads to improved robustness on the whole multi-layer network, R_d, of up to 17%, suggesting that intrinsic robustness of one particular layer does impact the robustness of an entire multi-layer network. However, when the optimization is guided by R_d, although showing considerable improvements of up to 27% in this measure, it does not improve the robustness of the rewired layer. In fact, it can effectively damage its robustness, in some cases, up to 10%. Finally, multi-objective optimization showed to be effective, leading to significant improvements on both robustness measures, with R_l improving up to 52% and R_d up to 24%, suggesting that it is possible to optimize the robustness of the individual layers and the whole multi-layer network, simultaneously.

Keywords

Complex systems Network Science Optimization

Multiplex networks Network robustness

Contents

1 Introduction **3**

2 Fundamental Concepts and Related Work **5**

2.1 Fundamental Concepts 5

2.1.1 Network robustness 5

2.1.2 Degree Distribution 6

2.1.3 Multi-layer Networks 7

2.1.4 Optimization 8

2.1.4.1 Greedy 8

2.1.4.2 Simulated Annealing 8

2.2 Related Work 9

2.2.1 Finding the most robust degree distributions 9

2.2.2 Enhancing robustness of pre-existing networks 12

2.2.3 Multi-layer networks 20

2.2.4 Summary of Related Work 23

3 Methodology and Implementation **25**

3.1 General aspects 25

3.2 Network generation 25

3.2.1 Power-Law 26

3.2.2 Exponential 26

3.2.3 Lattice 26

3.2.4 Duplex networks 26

3.3 Measuring robustness of duplex networks 26

3.3.1 Random failures . . . 27
3.3.2 Targeted attacks . . . 27
3.3.2.1 Degree based attacks . . . 27
3.3.2.2 Betweenness based attacks . . . 27
3.4 Optimization . . . 27
3.5 Overview . . . 28

4 Results **35**
4.1 Single Layer networks . . . 35
4.2 Distribution Combination . . . 35
4.2.1 ER-ER and SF-SF Networks . . . 36
4.2.2 ER-SF Networks . . . 38
4.2.3 L-SF Networks . . . 38
4.3 Optimization of network robustness . . . 39
4.3.1 Layer robustness optimization . . . 39
4.3.2 Global robustness optimization . . . 39
4.3.3 Multi-objective optimization on layer and global robustness . . . 40
4.4 Overview . . . 40

5 Conclusion **45**
5.1 Future Work . . . 46

Bibliography **49**

List of Figures

2.1 Network collapsing under a targeted attack. When 42% of nodes are removed, the largest component of the network reaches 0. 6

2.2 Robustness measurement R. For every node removed from the network, the relative size of the largest cluster, S(q), is summed. 6

2.3 Degree distribution of an Erdös-Rényi network. N = 5000 nodes, Avg. degree <k> = 2.6 7

2.4 Degree distribution of a Scale-Free network. N = 5000 nodes, Avg. degree <k> = 2.6 7

2.5 Degree distribution of a lattice network. N = 5000 nodes, Avg. degree <k> = 4.0 7

2.6 Example of a multiplex network with two layers. 8

2.7 Example of an optimization problem with local and global minimums. 9

2.8 Adapted from [19]: comparison between the initial robustness values, the theoretical values and the optimized values 16

2.9 Adapted from [14]: Visual representation of the smart rewiring method. 17

2.10 Adapted from [14]: Results showing the considerable improvement with new rewiring method against random rewiring. 18

2.11 Adapted from [23]: Pearson's correlation coefficients of the different measures of robustness. 18

2.12 Adapted form [23]: Pareto's fronts. 19

4.1 Robustness of single-layer Erdös-Rényi network. $N = 5000, < k >= 2.6$. 36

4.2 Robustness of single-layer scale-free network. $N = 5000, < k >= 2.6$. 36

4.3 Robustness of ER-ER duplex networks under random failures and targeted attacks. $N = 5000, < k >= 2.6$. 37

4.4 Robustness of SF-SF duplex networks under random failures and targeted attacks. $N = 5000, < k >= 2.6$. 37

4.5 Robustness of ER-SF duplex networks under random failures and targeted attacks. $N = 5000, < k >= 2.6$. 37

4.6 Robustness of SF-L duplex networks under random failures and targeted attacks. $N = 5000, < k >= 2.6$. 37

4.7 Greedy optimization of layer robustness on an ER-ER network. 41

4.8 Greedy optimization of layer robustness on an SF-SF network. 41

4.9 Greedy optimization of layer robustness on an ER-SF network. 41

4.10 Simulated annealing optimization of layer robustness on an ER-ER network. . . . 41

4.11 Simulated annealing optimization of layer robustness on an SF-SF network. . . . 41

4.12 Simulated annealing optimization of layer robustness on an ER-SF network. . . . 41

4.13 Greedy optimization of duplex robustness on an ER-ER network. 42

4.14 Greedy optimization of duplex robustness on an SF-SF network. 42

4.15 Greedy optimization of duplex robustness on an ER-SF network. 42

4.16 Simulated annealing optimization of duplex robustness on an ER-ER network. . 42

4.17 Simulated annealing optimization of duplex robustness on an SF-SF network. . . 42

4.18 Simulated annealing optimization of duplex robustness on an ER-SF network. . . 42

4.19 Greedy multi-objective optimization of R_l and R_d on an ER-ER network. 43

4.20 Greedy multi-objective optimization of R_l and R_d on an SF-SF network. 43

4.21 Greedy multi-objective optimization of R_l and R_d on an ER-SF network. 43

4.22 Simulated annealing multi-objective optimization of R_l and R_d on an ER-ER network. 43

4.23 Simulated annealing multi-objective optimization of R_l and R_d on an SF-SF network. 43

4.24 Simulated annealing multi-objective optimization of R_l and R_d on an ER-SF network. 43

List of Tables

4.1 Robustness optimization guided by R_l. 44

4.2 Robustness optimization guided by R_d 44

4.3 Robustness optimization guided by R_l and R_d 44

List of Algorithms

1 Calculation of MCGC relative size 29

2 Random failures 29

3 Degree based attack 30

4 Betweenness centrality based attack 30

5 Calculation of R_l 31

6 Calculation of R_d 31

7 Greedy optimization algorithm 32

8 Simulated annealing optimization algorithm 33

1 Introduction

Many of the real-world systems that support our society have an intrinsic network-like structure. Such systems include technical infrastructure, like electric power grids, water supply networks and computer networks, as well as biological networks built within ourselves, like neural networks and gene regulatory networks. A particular type of complex networks are multi-layer networks. These networks are characterized for having multiple layers, each one representing a different kind of relation between the nodes of the network. The nodes are instanced on all layers, but interact differently within each layer. Most complex systems incorporate multiple levels of interactions between its nodes. For example, transportation network of a country can incorporate multiple types of transportation. A person travelling from point A to C, can do such by using a type of transportation between A and B, and a different one between point B and C. Representing this system through a single-layer network would make this analysis difficult, requiring the use of metadata to differentiate links and nodes. By using multi-layer networks, we can effectively isolate the different types of relationships and analyse the properties and behaviour of each one, while still being able to study how they interact between each other and the impact that each one has on the whole system.

From previous work done on single-layer networks [2, 32], it is known that particular degree distributions offer better robustness in particular settings. While exponential distributions show increased robustness to targeted attacks, they are fragile against random failures. Power-law distributions, however, show the opposite behaviour, being robust against random failures, but fragile against targeted attacks. Optimization techniques [13,14,17,23] have proven to be effective in enhancing the robustness of single-layer networks. Algorithms, such as greedy and simulated annealing, together with rewiring methods which ensure the degree distribution remains stable, can greatly improve network robustness without causing major changes to the network topology.

Given the previously stated motivation and overall context, this thesis will focus on the study of robustness on multiplex networks with two layers, also known as duplex, and no degree correlation between layers. In multiplex networks, every layer is independent, meaning a node does not need to function in every layer of the network. The first question this thesis aims to answer is whether the robustness properties of exponential and power-law distributions carry over to multiplex networks. More specifically, it would be interesting to learn if a network with two exponential layers is robust against targeted attacks and fragile against random failures, if a network with two power-law distributions is robust against random failures and fragile against targeted attacks, and what happens when a multiplex network incorporates an exponential layer and a power-law distribution. Another particular network configuration studied in this

thesis is the combination of a layer with a power-law distribution and a layer with a lattice. A lattice is a network which has a grid-like structure and all nodes have a degree of 4, and can provide interesting robustness properties due to its geometrical characteristics and single-point distribution. Regarding optimization, the first question this thesis aims to answers is if optimizing the robustness of only one layer leads to an improvement of robustness of the whole multiplex network. Next, this thesis studies if optimizing the robustness of the multiplex network, while rewiring one specific layer, also leads to improved robustness on that particular layer. Lastly, this thesis studies if multi-objective optimization is effective on optimizing layer robustness and multiplex robustness simultaneously.

The remainder of this paper is divided into four chapters. Chapter 2 presents some fundamental concepts regarding complex networks and robustness, as well as relevant work on network robustness from two different points of view, intrinsic robustness of degree distributions and active improvement of robustness of already existing networks employing optimization methods. Chapter 3 describes the proposed methods used in this thesis, including calculating the size of the largest connected component of a multiplex network, network dismantling algorithms and optimization algorithms. Chapter 4 presents the relevant obtained results. Chapter 5 outlines the findings of this thesis, as well as possible future work that could be developed to further understand robustness on multiplex networks.

2 Fundamental Concepts and Related Work

This chapter describes some of the key concepts in regards to complex networks, network robustness and optimization, as well as an overview of the articles and papers whose results and findings are the groundwork for this thesis. In Section 2.1, the fundamental concepts are divided in complex networks (Section 2.1.1), multi-layer networks (Section 2.1.2), network robustness (Section 2.1.3) and optimization (Section 2.1.4). Afterwards, relevant literature regarding network robustness and robustness optimization is presented in Section 2.2. This section is organized in the following order. Section 2.2.1 focuses on the importance degree distributions have on network robustness, Section 2.2.2 highlights some optimization techniques used to actively improve the robustness of specific networks and Section 2.2.3 addresses how robustness can be measured in multiplex networks and highlights other robustness properties observed in multiplex networks. To summarize the chapter, Section 2.2.4 presents an overview of the key concepts and ideas from the related work.

2.1 Fundamental Concepts

2.1.1 Network robustness

Network robustness is the study of how complex networks behave under an hostile and error prone environment. The more attacks and failures a network can endure without compromising the system functionality, the more robust it is. There are several ways of measuring the robustness of a network, with the two most relevant ones being the percolation threshold and the R measurement [13]. The percolation threshold is the percentage of nodes/edges necessary to be removed in order to cause the network to collapse, rendering it no longer functional. Figure 2.1 shows an Erdös-Rényi network collapse under a targeted attack. In this example, the critical percolation threshold, f_c, is ≈ 0.42, where the size of the largest connected component is approximately zero. The R measurement, shown in Figure 2.2 and further described in Section 2.2.2.1, quantifies the robustness of a network by analysing how the largest cluster of the network behaves throughout every iteration of an attack.

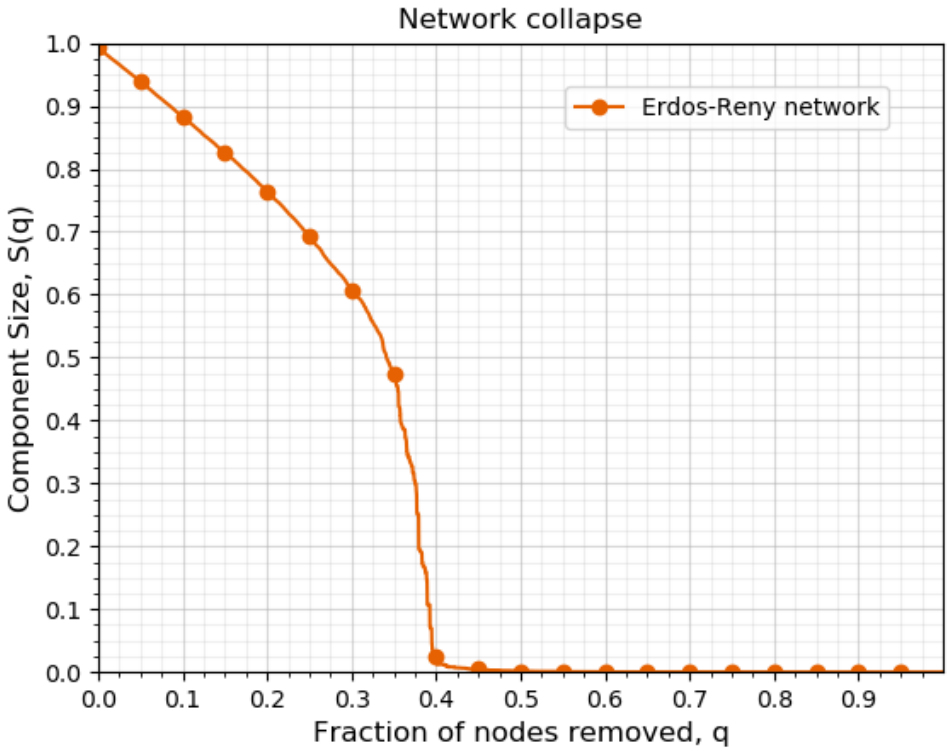

Figure 2.1: Network collapsing under a targeted attack. When 42% of nodes are removed, the largest component of the network reaches 0.

$$R = \frac{1}{N} \sum_{q=1/N}^{1} S(q),$$

Figure 2.2: Robustness measurement R. For every node removed from the network, the relative size of the largest cluster, S(q), is summed.

2.1.2 Degree Distribution

The degree distribution of a network is the probability distribution of its node's degrees. The degree of a node is the number of connections that the node has to other nodes in the network. Networks with different degree distributions have different levels of robustness against targeted attacks and random failures. This thesis will mainly focus on two types of networks: exponential and scale-Free. Exponential networks have a Poisson distribution, characterized by a peak at the average degree and an exponentially decay for larger degrees. Scale-free networks have a power-law distribution, characterized by a high number of nodes with very small degree, and a very small number of nodes with very high degree. Additionally, this thesis also studies the effects of using Lattices, a regular network with a single-point distribution, together with other distributions, on multi-layer networks with two layers. Lattices are characterized by having a grid-like structure where every node has a degree of 4.

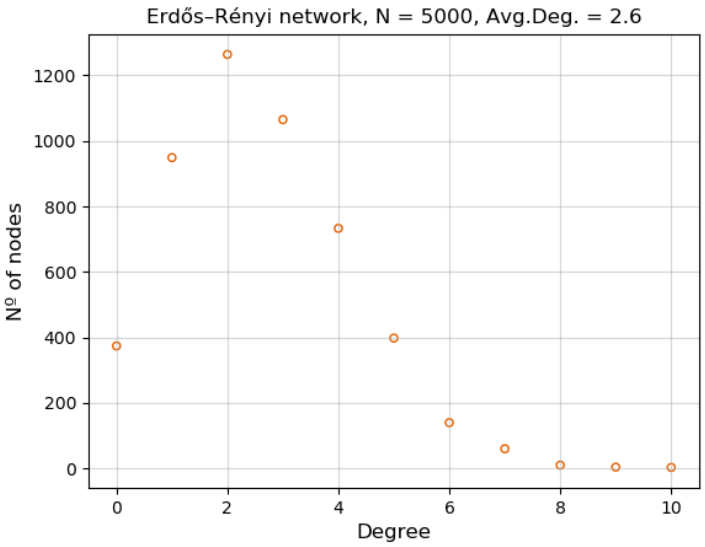

Figure 2.3: Degree distribution of an Erdös-Rényi network. N = 5000 nodes, Avg. degree <k> = 2.6

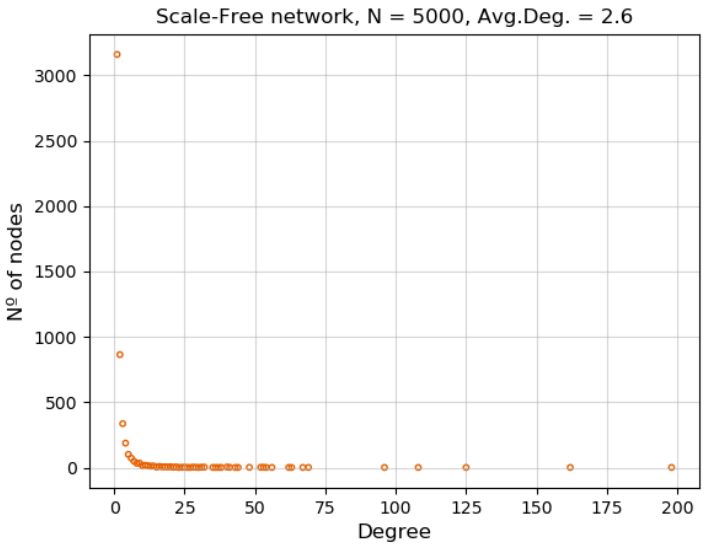

Figure 2.4: Degree distribution of a Scale-Free network. N = 5000 nodes, Avg. degree <k> = 2.6

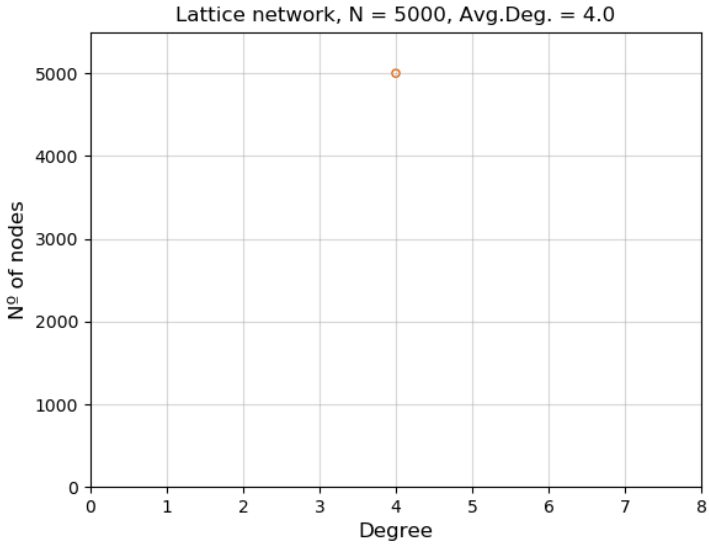

Figure 2.5: Degree distribution of a lattice network. N = 5000 nodes, Avg. degree <k> = 4.0

2.1.3 Multi-layer Networks

Multi-layer networks differ from traditional complex networks by incorporating multiple layers. Every node is instanced in every layer, but can connect differently within each of them, allowing the modelling of different types of relations between nodes. When measuring the size of the largest connected component of a multi-layer network, we can extend the definition of giant connected component from single-layer complex networks. A node is considered to be part of the giant connected component of a multi-layer network if it connects to the component in at least one of its layers. This thesis focuses on a particular type of multi-layer networks

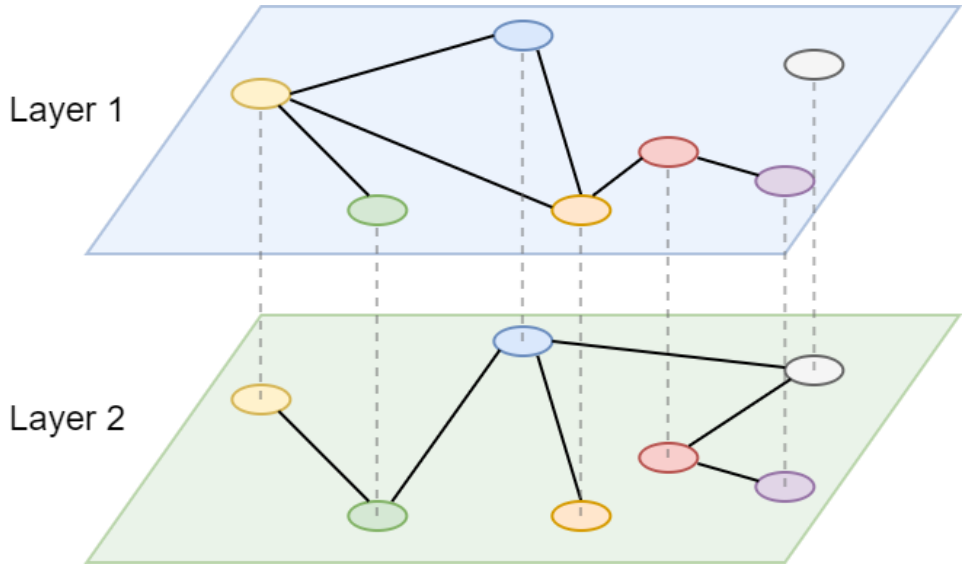

Figure 2.6: Example of a multiplex network with two layers.

called multiplex, whose layers are independent amongst themselves. If a node suffers damage in one layer, it remains functional on the remaining layers. The counterpart, not studied in this thesis, is called interdependent networks. These networks have dependency links between layers, making it so that a node in one layer can be dependent on other nodes in other layers. Removing a node in one layer can lead to cascading failures throughout the whole network.

2.1.4 Optimization

2.1.4.1 Greedy

In optimization, a greedy algorithm is characterized by always choosing the best local option in each step of the process. It is a simple, yet effective optimization algorithm, but has some shortcomings, such as local maximums/minimums and, therefore, it cannot find the optimal solution for many problems.

2.1.4.2 Simulated Annealing

The simulated annealing algorithm is a probabilistic optimization technique that mimics the process of crystal growth. It's main objective is to approximate the global optimal solution of a given problem, which is an improvement over the greedy algorithm. To achieve this, the algorithm accepts worse solutions in the early stages and, as the solution space is explored, the probability of accepting worse solutions decreases. Figure 2.7 illustrates an optimization problem where a greedy algorithm would get stuck at a local minimum but the simulated annealing would not.

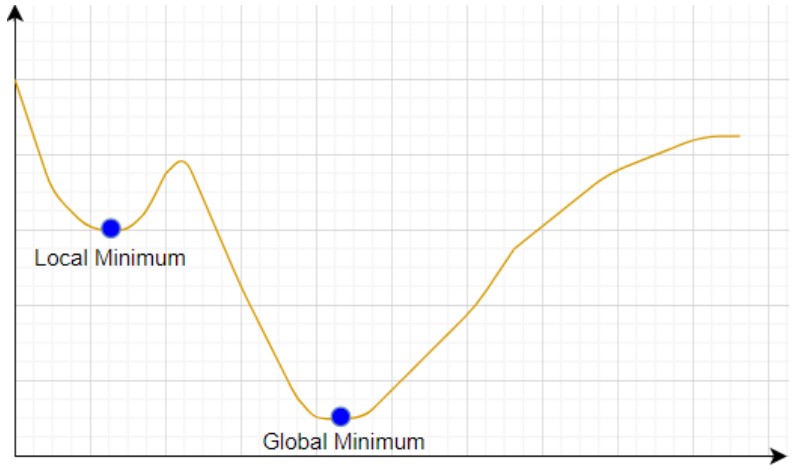

Figure 2.7: Example of an optimization problem with local and global minimums.

2.2 Related Work

This section lists some papers and articles that are relevant to this thesis, either because they present some groundwork to the subject studied, or because they approach similar problems as this thesis.

2.2.1 Finding the most robust degree distributions

While some networks are robust to random failures, they are usually vulnerable to targeted attacks. The same happens the other way around. The following papers focus on studying which degree distributions provide the most robustness to different types of attacks and failures and how networks can be built in a way that can incorporate robustness to random failures and targeted attacks.

- **Error and attack tolerance of complex networks**

  One of the first publications that approached robustness of complex networks was a letter written by Réka Albert, Hawoong Jeong & Albert-László Barabási to the science journal Nature in 2000 [2]. The publication begins by acknowledging that there is some basic intrinsic resilience in complex networks that makes it possible for local failures to not lead to the loss of global information-carrying ability of the network. This property can be attributed to the existence of redundant wiring in the network, making it so that if a node in the network fails, there will most likely be alternative paths that do not need the failed node to transmit information to the rest of the network. However, not every redundant system shares the same level of robustness, and there are network configurations that make them more resilient to some types of failures than others. A specific class of networks, called "scale-free", show a high level of robustness against random failures. This networks, characterized by a power-law degree distribution, owe its robustness to its heterogeneity. Since this networks have a large amount of nodes

with a low degree and a very small amount of nodes with a high degree (hub), the chance of a random failure to hit a hub is very small. However, the fact that a small amount of nodes hold such an important role in keeping the network connected makes the network vulnerable to intentional and targeted attacks. On the other hand, there exists a type of network that is weak to random failures but very robust to intentional attacks, the exponential networks. These networks have a degree distribution that peaks at the average degree and decays exponentially for larger degrees. Some examples of such networks are the random graph model of Erdös and Rényi[3] and the small-world model of Watts and Strogatz [4]. To prove these different levels of robustness, the researchers focused on the random graph model of Erdös and Rényi and the scale free model. First, they evaluated how the diameter of the networks changed when a small fraction of the nodes f was removed. The results showed that when the nodes were removed randomly, the network diameter for the scale free networks remained unchanged under an increasing level of errors. Even when up to 5% of the nodes were removed, the communication between the remaining nodes in the network was unaffected. As for the random networks, the diameter increased monotonically with f. Thus, despite the redundant wiring, it becomes increasingly difficult to maintain communication between the remaining nodes. As for targeted attacks, the diameter of the scale-free networks increased rapidly with f, doubling its original value if 5% of the nodes are removed. As for the random network, the diameter increased at the same rate as when random failures were tested. From this results, it is concluded that scale free networks are more resilient to random failures but more vulnerable to targeted attacks and exponential networks are weak to random failures but more robust to targeted attacks than scale free networks. To further understand the impact of random failures and attacks, they decided to study the fragmentation process that happens as nodes are removed form the network. When a certain amount of nodes are removed from a network, small clusters of nodes start to detach from the main cluster. The percentage of nodes that need to be removed from the network in order for the size of the biggest cluster drastically decrease is called the percolation threshold, a definition that has its origin in percolation theory[5]. The results showed that, under random failures, the size of the largest cluster of a random network suddenly drops at $f = 0.28$, while for scale-free networks, no threshold is observed and the network does not collapse, further proving that scale free networks are robust to random failures. As for targeted attacks, the threshold happens for f=0.18 for scale-free networks and f=0.28 for random networks. Again, these results show that scale-free networks are weak to targeted attacks and while random networks behave the same.

- **Optimization of Robustness of Complex Networks**

To further investigate what network topologies are more robust, G. Paul, T. Tanizawa, S. Havlin and H. E. Stanley go into more detail on specific degree distributions in [6]. Their main objective is to find a network design that maximizes both robustness to random failures and targeted attacks while maintaining a constant number of links. This is important because adding new links to a network, while it may increase the

robustness, it can also have a large cost in real world networks and it isn't always a practical solution, for example, in water and power supply networks. They begin by defining an optimization metric for the robustness, based on the percolation threshold[5] and formulate an objective function to maximize robustness to both random failures and targeted attacks. In a first experiment, the researchers evaluate what is the exponent λ that maximizes robustness for scale-free networks, concluding that $\lambda = 2.5$ has the best total robustness, which is an interesting result since most real world networks with a scale-free distribution also have $\lambda \approx 2.5$ [7-9]. Then, they move to a more complex degree distribution, formed by two power laws, the first one with an exponent α and the second one with an exponent λ, while maintaining the same average degree, <k>. The point at which the distribution changes is called the inflation point *a*. The researchers believe that one of the power laws will contribute to robustness for random failures and the other will contribute for robustness to targeted attacks. They conclude that: 1) for a given λ, a and α can be fine tuned to maximize robustness and 2) This degree distribution is more robust than a single power law distribution if λ is close to 1 and α is large enough. They obtain similar results when changing the first power law with an exponential with exponent β. As β increases, the optimization increases. Next, they study the case where the degree distribution is formed by two Gaussian segments. The first Gaussian has its center at κ_1 and width ω_1 and the second one has its center at κ_2 and width ω_2, with $\kappa_2 > \kappa_1$. They observed that the robustness increased as κ_2 increased and it reached the highest values for small values of ω_1. The results of the previous experiment motivated them to study the case where the distribution is composed by two delta functions, which are similar to Gaussian functions, except the integral is always 1. The results indicated that the robustness increased when r, the fraction of nodes in the second delta function to the total number of nodes, approaches zero, meaning that only one node should have a high degree and all the other nodes should have the same degree. In conclusion, the best degree distribution that maximizes robustness to both random failures and targeted attacks seems to be one where nodes can only have 2 possible values, being that only one node should have a large degree while all the other nodes should have the same low degree. The single high degree node provides robustness to random failures, while the small degree nodes provide robustness to targeted attacks.

- **Robustness properties of single-point degree distributions**

  In [1], André X. C. N. Valente, Abhijit Sarkar and Howard A. Stone reach a conclusion somewhat similar to the previous paper [6]. They theorize that a network with at most three distinct node degrees can maximize robustness to both random failures and targeted attacks. Starting with the expression for the percolation threshold for any degree distribution,

$$f_r = 1 - \frac{1}{\frac{<k^2>}{<k>} - 1}, \tag{2.1}$$

  , they derive another formula adapted to a two-peak distribution,

$$f_r = 1 - \frac{< k >}{-k_m k_l + < k > (k_m + k_l - 1)}. \tag{2.2}$$

The theoretical analysis shows that these networks can have a larger percolation threshold for random failures and for targeted attacks than some real-world scale free networks, therefor more robust. They then move on to study if a three peak network, while minimizing the the average number of links, maximizes the two percolation thresholds separately, and not as a combination of both, $f_a + f_r$. Once again using a theoretical analysis, it is concluded that this network configuration does maximize f_a and f_r separately.

- **Theoretical approach to robustness analysis**

  Yu Sun, Peiyang Yao, Dongdong Shui and Yun Zhong developed a framework to study the impacts of structural parameters of a complex network on its robustness in [10]. With previous works [11] showing that the degree distribution plays an important role in the levels of robustness of a network, these researchers focus on finding what degree distribution maximizes the upper limit of robustness of a network and finding relationships between a given degree distribution and other structural parameters. The chosen measure of robustness, based on [13-15], was defined as

  $$R^I = \min_{at_i \in AT} R(at_i), \tag{2.3}$$

  where at_i represents the number i type of attack mode and $R(at_i)$ is the value of robustness measurement shown in [12] with the attack mode at_i.

  The optimization procedure is based on the variable neighbourhood search algorithm [16], and uses the commonly used rewiring method (selecting two random edges and switching them) to create new networks, keeping the number of nodes and edges and the degree distribution unaltered. The studied structural parameters were network efficiency, natural connectivity, algebraic connectivity and average clustering coefficient. The studied distributions were single-point distribution, Poisson distribution, exponential distribution and power-law distribution.

  Results showed that networks with a single point degree distribution were the least robust and networks with a Poisson degree distribution were the most robust, for non-optimized networks. After the optimization procedure, single point degree distribution showed the most robustness, while the power law degree distribution had the lowest. As for the structural parameters, the results showed that network efficiency and algebraic connectivity increases with robustness, while the average clustering coefficient and natural connectivity decrease when the robustness is higher. Also, itâs noticeable that these changes in the structural parameters is more evident when the degree distribution is more consistent.

2.2.2 Enhancing robustness of pre-existing networks

The previous papers were able to find some degree distributions that allow for high robustness to random failures and targeted attacks. Even though this network configurations perform incredibly well in hostile environments, its usefulness is limited. Because these networks have

such a specific degree distribution, it's difficult to find a domain that could be modeled using these networks. Another option would be to modify the degree distribution of already existing networks that have a more vulnerable degree distributions. The problem is that such reconfiguration can have large costs and the topology of network will be greatly changed, which can make the network no longer functional for the required domain. The following papers focus on optimizing network's robustness while keeping the original degree distribution, using different optimization algorithms and different robustness definitions to guide the optimization process.

- **Optimizing network robustness using rewiring methods and a novel robustness measure**

  In [13], Christian M. Schneider, André A. Moreira, José S. Andrade, Jr, Shlomo Havlinc, and Hans J. Herrmanna propose a method to optimize robustness on already existing networks. Instead of using the traditional measure of robustness, the critical fraction of attacks at which the network completely collapses, also known as percolation threshold, the researchers use a measure based on the Giant Connected Component (GCC) of the network that quantifies the connectivity of a network,

$$R = \frac{1}{N} \sum_{Q=1}^{N} s(Q), \tag{2.4}$$

  where N is the total number of nodes and $s(Q)$ is the fraction of nodes in the largest connected cluster after removing Q nodes. The bigger the GCC, the more robust the network is. This measure for robustness has the advantage of taking into consideration the situations where the network does not fully collapse but still suffers significant damage. Also, instead of using the static approach to find the most connected nodes at the beginning of the attack, the authors use a dynamical approach where the degree of each node is recalculated after a node is removed. Although it is computationally more expensive, it is a more realistic and effective strategy of attack. In order to keep the increase of robustness as realistic as possible, they set the constraints that the number of edges and the degree of each node must remain the same during the optimization.
  The optimization method, based on the hill climbing algorithm, consists of the following steps:
  1) Pick two randomly selected edges from the network, (i, j) and (h, k),
  2) Delete (i, j) and (h, k) from the network,
  3) Add (i, h) and (k, j) to the network.
  4) Calculate the robustness of the new network and keep the new network if it is more robust.
  5) Repeat 1 to 4 until no further substantial improvement is achieved.

  Simulations were executed over two different real networks: European power grid and global Internet at the level of service providers in Europe. The results showed significant improvements of the robustness levels for both networks. Even though the robustness is increased, the percolation threshold remained the same, further justifying the choice for

the robustness measure. Also, the resulting networks have an "onion-like" structure, having a core of nodes with a high degree, surrounded by rings of nodes with decreasing degree.

- **"Enhancing network robustness against malicious attacks"**

  An Zeng and Weiping Liu go on to further expand on the idea of improving network robustness against malicious attacks in [17]. While the previous paper [13] focuses on improving a robustness function based on the nodes of the network, An Zeng and Weiping Liu focus on the fact that failures and attacks can happens on the links and not necessarily on the nodes, like a blocked highway or a dysfunctional power cable. They further investigate if increasing robustness in regards to nodes also increases robustness in regards to the edges, and propose an hybrid algorithm that can optimize both measures of robustness.The measure of robustness in regards to the nodes is the same as (1), labeled R_n. As for the robustness in regard to the links, R_l [1], it is very similar to (1), except it considers the removed links instead of removed nodes,

$$R_l = \frac{1}{E} \sum_{P=1/E}^{1} s(P), \tag{2.5}$$

  where E is the number of edges in the network and $s(P)$ is the size of the largest connected component after P links are removed. The optimization algorithm works as follows:
  1) Pick two randomly selected edges from the network, (i, j) and (h, k),
  2) Delete (i, j) and (h, k) from the network,
  3) Add (i, h) and (k, j) to the network.
  4) Calculate the robustness of the new network and keep the new network if it is more robust, in terms of R_n and R_l .
  5) Repeat 1 to 4 until no further substantial improvement is achieved.

  The algorithm only differs when it comes to choosing if the new network is accepted. It will only be accepted if the link swap improves both R_n and R_l, working as multi-objective optimization.

  A few different networks were used to test the algorithm: Barabási-Albert scale-free networks, US air transportation system and an electrical power grid in part of western Europe. A few interesting conclusions can be drawn from the results of the robustness optimization method. First, it can be seen that improving the robustness in terms of R_n does not improve robustness in terms of R_l,and vice-versa. In fact, it can be seen that in some cases, while one of the measures improves, the other decreases. Secondly, when using the hybrid algorithm that optimizes both R_n and R_l, there is always an improvement in both measures. When testing the networks against targeted attacks to both nodes and links, it can be seen that the networks that were improvised using the hybrid algorithm can preserve the giant component more effectively than when the robustness measures

[1] In this context, R_l is used to define robustness when the attacks target the network links. In the rest of this dissertation, R_l represents the robustness of a particular layer of a multiplex network.

are improved alone.

- **"A theoretical estimation for the optimal network robustness measure R against malicious node attacks"**

  In [19], Liangliang Ma, Jing Liu, Boping Duan and Mingxing Zhou take a theoretical approach to the optimization of robustness problem. While previous work consider that the degree distribution of the network should remain static, the researchers on this paper focus on optimizing the robustness of the degree distribution, allowing it to change during the optimization process, having the number of nodes and edges remaining constant. The chosen measure of robustness is (1), the fraction of nodes in the largest connected component. The theoretical process to estimate the robustness can be divided in two parts: 1) Effects of malicious attacks and 2) Estimation for the largest connected component.

  1) Effects of malicious attacks
  An intentional attack to a network is usually characterized by the sequential removal of the node with highest degree. This causes the maximum degree of the network to decrease as the attack continues. If K is the original highest degree of the network and $\tilde{K}$ is the new highest degree, then we have $\tilde{K} \leq K$. The final formula for $\tilde{K}$ obtained with the theoretical approach is

  $$\tilde{K} = max\{k|N \times \tilde{P}(k) \geq 1, \forall k\}, \tag{2.6}$$

  and the formula for the average degree is

  $$< k >= \sum_{k=1}^{k=\tilde{K}} k\tilde{P}(k). \tag{2.7}$$

  2) Estimation for the largest connected component.
  Based on the works of [20 - 22], the researchers develop a theoretical definition for the size of the largest connected component,

  $$S(Q) = 1 - \sum_{k=0}^{\infty} P(k)\mu^k. \tag{2.8}$$

  To validate the previous formulations, a few experiments were conducted. The first experiment focus on exploring which distribution of the largest connected component is represented by theoretical results, the initial network or the optimized network. The following types of networks were taken into consideration: regular networks, Watts - Strogatz networks, Erdös-Rényi networks, and Barabási â Albert networks, each network with 500 nodes. These networks were optimized using the method in [13].

  The results show that the theoretical distribution of the largest connected cluster is close to the optimized networks, proving the correctness of the theoretical results. Also, it shows that regular networks are the most robust.

  In the following experiment, the researchers focus on regular networks, as they are the most

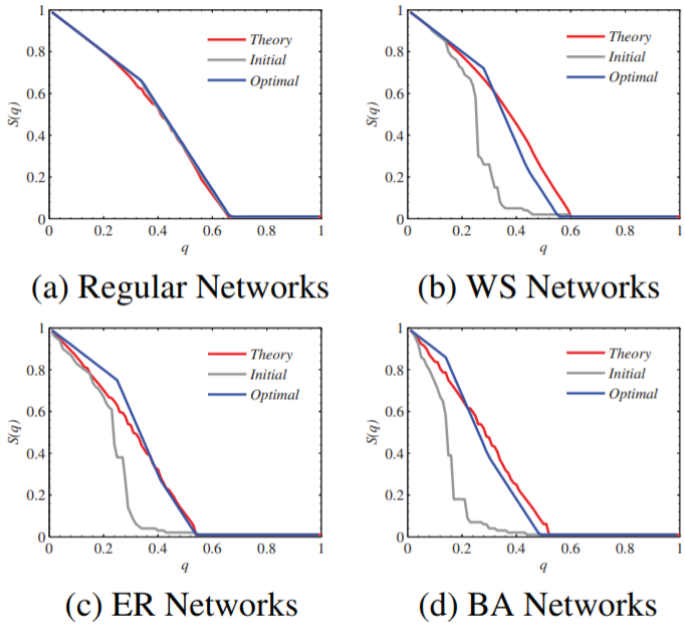

Figure 2.8: Adapted from [19]: comparison between the initial robustness values, the theoretical values and the optimized values

robust according to the previous results, and develop an optimization method. During the optimization process, only the number of edges and nodes is kept invariant, and the degree distribution is optimized. The algorithm used is similar to [13], but the new edge operation is as follows:

1) An edge and two nodes which are not connected are chosen at random.

2) The selected edge is broken down and the two selected nodes are connected.

The results show significant improvements in the levels of robustness, not only when compared to the original network but also when comparing with previous works.

In the final experiment, the researchers analyze the degree distribution of networks varying with the increment of N after optimization.

As can be seen from the obtained results by the researchers,in Figure 2.8, the degree of most nodes in the networks obtained by the proposed method is close to the average degree, which could lead to the conclusion that networks with nodes with similar degree may be more robust against malicious attacks.

- **A more complex rewiring method**

In [14], V. H. P. Louzada, F. Daolio, H. J. Herrmann and M. Tomassini try to improve the rewiring method used to improve network robustness. Previous work select randomly chosen links from the network and swap them to see if it has any impact in the overall robustness of the network. In this paper, a more complex rewiring method is proposed:

1) Select a node i randomly with at least two neighbors with degree larger than one.

2) Select the lowest degree neighbor of i, the node j, and its highest degree neighbor, the node k.
3) Select randomly a neighbor m of node j and a neighbor n of node k.
4) Repeat steps 1-3 until all nodes concerned are different from each other.
5) Remove links e_{jm} and e_{kn}.
6) Create links e_{jk} and e_{mn}.

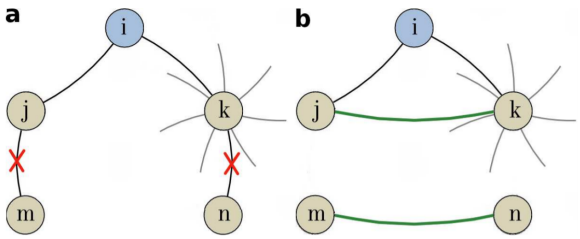

Figure 2.9: Adapted from [14]: Visual representation of the smart rewiring method.

The main motivation for developing this method was to encourage the creation of alternative connections between parts of the network that would otherwise be split upon the failure of a hub. The experiments conducted showed promising results. The new method shows, in Figure 2.10, that it can improve robustness as much as previous work, but with up to 20% less swaps than previous work, like in [13].

Another consequence of this new rewiring method is the increase of modularity of the network, because it deliberately creates triangles of connections, reducing the importance of the hubs, which are now connected to leaves (nodes with low degree), and their removal does not have huge impact on global connectivity.

- **Using multi-objective optimization with conflicting robustness measures**

In [23], Mingxing Zhou and Jing Liu take a new approach on network robustness optimization. They acknowledge the fact that there are many different types of attacks, and a network that is robust to a specific attack may not be robust to others, and formulate four different types of attacks: attack the nodes based on the highest degree (NA_{HDA}), attack the nodes based on the highest betweenness centrality (NA_{HBCA}), attack the links based on the highest degree(LA_{HDA}) and attack the links based on the highest betweenness centrality(LA_{HBCA}). The authors create 4 measures of robustness based on the type of attacks and Schneider's robustness measure[13], R_n^D, R_n^{BC} , R_l^D, and R_l^{BC}, and use Pearson's correlation coefficient to analyse relationships between the different measures.

A positive correlation coefficient indicates that the two measures can be optimized together, therefore single-objective optimization would be appropriate. A negative correlation coefficient indicates that the two measures cannot be optimized simultaneously using single-objective optimization, and a multi-objective optimization algorithm would be more appropriate. R_n^D and R_l^{BC} have the smallest Pearsonâs correlation coefficient, so the re-

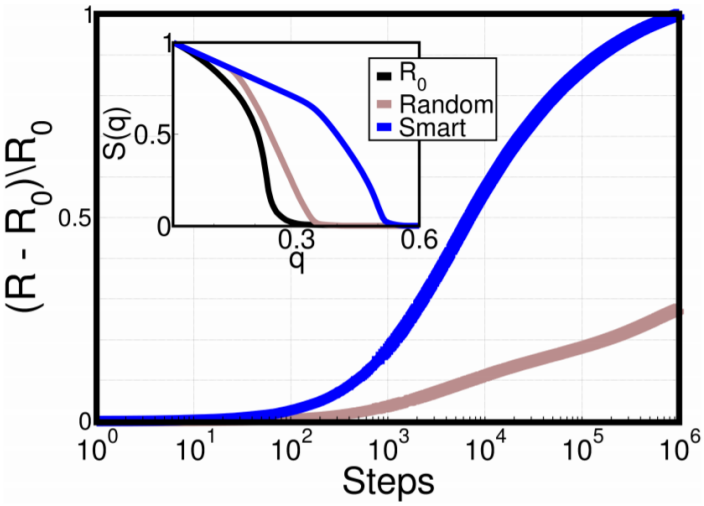

Figure 2.10: Adapted from [14]: Results showing the considerable improvement with new rewiring method against random rewiring.

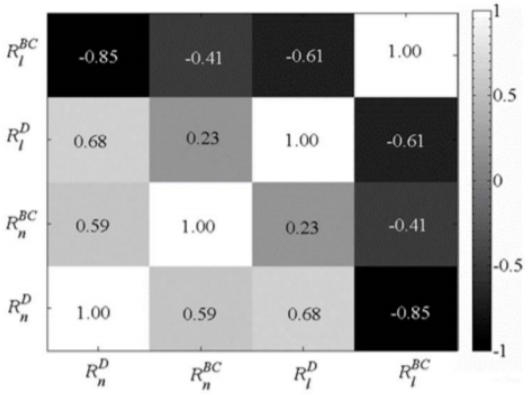

Figure 2.11: Adapted from [23]: Pearson's correlation coefficients of the different measures of robustness.

searchers focus on optimizing these two using a two-phase multi-objective evolutionary algorithm, labelled $MOEA - RSF_{MMA}$, to try and find a network that can be robust in terms of both measures. The first phase of the algorithm, labelled R_n^D -Sampling Phase, generates numerous networks with both high and low R_n^D, all with the same degree distribution(scale-free) and number of nodes and links. The second phase, labelled $R_n^D - R_l^{BC}$ - Optimization Phase, the multi-objective algorithm NSGA-II [24] is employed. The obtained Pareto fronts are plotted in Figure 2.12.

The obtained networks were analysed in terms of some structural parameters. Results showed that the average path length decreased with the optimization of R_n^D, but the optimization of $R_l^B C$ improves it. Also, assortativity of the networks improve with R_n^D but fluctuate when R_n^D is low, while the opposite is observed for $R_l^B C$.

- **Comparing different robustness measures**

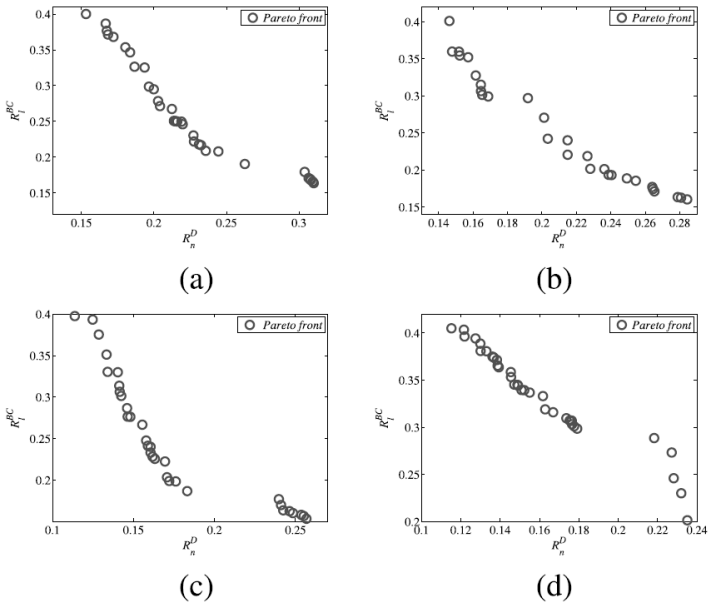

Figure 2.12: Adapted form [23]: Pareto's fronts.

In [25], Jing Liu , Mingxing Zhou, Shuai Wang and Penghui Liu compare different measures of robustness, analyze if they can properly evaluate the network robustness and if optimizing a network regarding one of the measures also lead to an improvement of robustness according to the other measures. In total, 9 different robustness measures were presented, some regarding node robustness and others edge robustness. 1. Edge connectivity, measures robustness as the number of edges that need to be removed form a network in order to disconnect it

$$v(G) = \min_{s,t \neq s \in V} \{v_{s-t}(G)\}. \tag{2.9}$$

Node connectivity, follows the same principle as edge connectivity, except itâs based on the number of nodes that need to be removed.

$$\omega(G) = \min_{s,t \neq s \in V \wedge e_{st} \notin E} \{\omega_{s-t}(G)\}. \tag{2.10}$$

Percolation threshold, p_c^r for random failures and p_c^t for targeted attacks, the critical number of nodes that need to be removed for the network to collapse into multiple smaller networks. p_c^t differs from p_c^r in the fact that it is calculated when, after simulating the attack process, the network is left disconnected.

$$p_c = 1 - \frac{1}{\kappa_0 - 1}. \tag{2.11}$$

Introduced by [13], this measure considers the size of the largest component.

$$R = \frac{1}{N} \sum_{Q=1}^{N} s(Q). \tag{2.12}$$

Similar to the previous one, but extended to consider attacks on edges

$$R_l = \frac{1}{M}\sum_{P=1}^{M} s(P). \tag{2.13}$$

Introduced in [26], this measure on the communication efficiency of the network

$$IntE = \frac{1}{N}\sum_{Q=1}^{N} E(Q). \tag{2.14}$$

The algebraic connectivity, which reflects how well a network is connected

$$\alpha(G) = \lambda_2 \leq \lambda_1 \leq \lambda_2 \leq \lambda_3 \leq ... \leq \lambda_N. \tag{2.15}$$

The natural connectivity, which characterizes the redundancy of alternative routes in a network

$$\overline{\lambda} = ln\left(\frac{1}{N}\sum_{i=1}^{N} e^{\lambda_i}\right). \tag{2.16}$$

The sensitivity of these 9 measures was analysed in both non-optimized and optimized networks. The higher the sensitivity of a measure, the better it can detect changes on the network, therefore it is a better measure of robustness. For the non-optimized networks, random BA networks were generated and different operations of adding and removing nodes were executed. The robustness was recalculated in each step, for every different measure. For the optimization part, the hill climbing algorithm was used. During the optimization process, p_c^t, R, R_l, IntE, $\alpha(G)$, and $\overline{\lambda}$ are used as the optimization objectives, generating six different types optimized networks. For each type, the sensitivity of above robustness measures is analysed. The results showed that v(G) and $\omega(G)$ canât properly detect changes in the networks, while R_l and $\alpha(G)$ showed a good response to those changes, in both the non-optimized and optimized networks. The other measures detected those changes to some degree. Another experiment was conducted to test if improving the robustness in terms of a measure also increases in terms of other measures. The results showed that none of the generated networks were robust in terms of all measures. For example, networks optimized for the objective function $\overline{\lambda}$ show very little robustness in terms of v(G), $\omega(G)$ and $\alpha(G)$. This suggests that there are measures that have a negative correlation, which indicate that multi-objective optimization may be useful to generate networks that are robust in terms of multiple measures.

2.2.3 Multi-layer networks

Multi-layer networks are a specific type of complex networks that have multiple layers, each layer representing a different kind of relation between the nodes of the network. The nodes are the same on all layers, but interact differently within each layer. These networks are more adequate to accurately model key complex systems of our world like transportation systems and online social networks, and therefore it is relevant to study the mechanisms of robustness that underline these networks. The following papers study some aspects of robustness in these type

of networks.

- **Network robustness of multiplex networks with degree correlation between layers**

  In [27], Byungjoon Min, Su Do Yi, Kyu-Min Lee, and K.-I. Goh study the network robustness of multiplex networks with two layers (duplex), more specifically, the importance of correlations between degrees of a node in different networks. The motivation for this research was the fact that many real world multi-layer networks have degree correlation between its layers. A good example of this is the transportation network, where each layer represents a different kind of transportation. If a city in the highway layer has a high degree, it will most likely also have a high degree for other transportation layers, like trains or airports. Three types of correlation are taken into consideration: maximally-positive (MP), maximally-negative (MN) and uncorrelated (UC) [31]. Maximally-positive means that a node that is a hub in a layer, will also be a hub in the other layers. Maximally-negative means a node that is a hub in a layer will be a low degree node in other layers.

  The first measure studied was the biconnectivity. Two nodes that are connected through two disjoint paths are said to be biconnected. If we attack one of this paths, the two nodes remain connected through the alternative path, therefore it is seen as a property that improves robustness. We can then define the greatest connected bicomponent as a measurement of robustness of a network. The results showed that MP networks were able to achieve a larger bicomponent for lower mean degrees, whereas MN networks have a very small bicomponent for small mean degrees. MN also shows a percolation threshold for a mean degree of z = 0.838, where the size of the bicomponent exponentially grows, and stabilizes at the maximum value of 1 for z = 1.146, meaning that the whole network becomes part of the giant bicomponent.

  Next, the robustness of these duplex networks were studied against random failures and targeted attacks, in terms of the percolation threshold. The results showed that MP networks are more resilient to random failures than MN and UC, having a delayed percolation threshold in comparison with the competitors. This means we have to remove a larger fraction of nodes in MP for the network to collapse. One explanation for the increased robustness in MP networks is the skewness of the total degree distribution, while the MN networks have an evenly distributed degree distribution. This explanation is in conformity with the works of [2]. Another interesting result is that the effect of correlation becomes less significant when the network is sparse. For targeted attacks, when the networks are sparse, MP is more robust than UC. But for denser networks, MP is more vulnerable than UC. For MN, the results were the complete opposite of MP. MN is more vulnerable if the network is sparse and more robust if it is dense.

  For interdependent duplex networks, similar experiments were conducted. Results showed that MP networks are still more robust than MN for lower mean degrees, and is more robust against random failures. As for targeted attacks, the networks exhibit more complex behaviour. For sufficiently low density, MP is more robust than MN and UC. For an

intermediate density, MN is the most robust and UC the least. For high density, MN is the most robust, while MP is the most vulnerable.

An additional analysis for non-maximal correlation was made, with results showing that there is still some impact on the robustness, although not as significant as maximum correlation.

- **Comparing different attack methods on multiplex networks**

In this article [28], Da-wei Zhao, Lian-hai Wang, Yong-feng Zhi, Jun Zhang and Zhen Wang study the robustness of multiplex networks under random and targeted attacks. More specifically, they study layer node-based attacks. This means that when a node is attacked, only the edges of the selected layer are removed, and not all the edges of that node on all layers. For example, attacking a city on the train layer, will only disable the train connections of that city, but airports, highways, etc remain unaffected. With the goal of calculating the critical threshold of network collapse and the size of the giant connected component when a fraction of layer nodes are removed, a theoretical method is proposed, using the framework of generating function method [30]. When talking about GCC in multi-layer networks, it is more correct to label it as mutually connected giant component (MCGC). It is then defined as the largest component that remains after the removal propagates back and forth in the different layers, meaning that a node must connect to the giant connected component thorough at least one of the layers. All nodes in the MCGC are labeled multiplex nodes, and a pair of multiplex nodes are connected if there exists a connection between them in at least one layer. Four different formulas were derived, for the critical threshold and MCGC, for random and targeted attacks. The results obtained from the conducted experiments showed that the theoretical critical threshold can accurately predict the impact of layer node-based attacks on the robustness of multiplex networks and the theoretical prediction of the size of the MCGC also matches the obtained results. This was observed for both the random attacks and the targeted attacks. A final experiment was conducted to compare the used layer node-based attacks with multiplex node-based attacks, which lead to an interesting conclusion. A multiplex network is more vulnerable to layer node-based attacks than multiplex node-based attacks. Meaning, if the attacker focuses on attacking a node on each layer separately, instead of attacking the node on all layers simultaneously, the network will collapse at a faster rate. The proposed explanation from the researchers was that when layer node-based attacks is used, more multiplex nodes are subject to attack and lose more connections with other multiplex nodes.

- **Topological impacts of robustness optimization in interdependent networks**

  From the previous works, we can infer that increasing inter-layer degree correlation on multiplex networks is a good strategy to optimize robustness. In this paper [29], Ivan Kryven and Ginestra Bianconi show that such an optimization procedure might cause previously unforeseen consequences on interdependent multiplex networks. For instance, they show that these networks may be decomposed during percolation by multiple discontinuous phase transitions into sub-multiplexes that span across all layers. However, the introduction of these phase transitions can be mitigated by reducing the total number of layers. It was also shown that when modeling real world systems that have a multiplex like structure with a large amount of layers, trying to use a smaller number of layers can lead to a loss in the qualitative structure of the phase space.

2.2.4 Summary of Related Work

As we saw in this section, there is extensive research on the subject of network robustness. The following bullet points summarize some of the key aspects of network robustness.

Single-layer networks

- Scale-free networks are resilient to random failures but weak to targeted attacks.
- Exponential networks are resilient to targeted attacks but weak to random failures.
- Networks with a degree distribution with two and three peaks (nodes can only have two or three different degrees) show resilience to both random failures and targeted attacks.
- It is possible to improve robustness of a network by rewiring it, together with optimization methods such as hill-climbing or simulated annealing.
- Structural parameters, such as network efficiency or clustering coefficient, are affected by rewiring processes aimed at optimizing robustness.
- There are several metrics to measure network robustness, such as edge connectivity, node connectivity, percolation threshold, size of GCC, communication efficiency, algebraic connectivity and natural connectivity.
- Some of this metrics are more sensible to changes in the network than others. In an optimization process, it is preferable that the function to optimize is sensitive to small changes of the input.
- Multi-objective optimization has been successfully used to improve robustness in terms of conflicting robustness metrics.

Multi-layer networks

- Degree correlation between layers of a multiplex network can influence its robustness, depending on the density of the network and if the network suffers random failures or targeted attacks.
- Multiplex networks are more robust against multiplex node-based attacks than layer node-based attacks.
- Metrics to measure robustness of multiplex networks include the size of the MCGC(mutually connected giant component) or the size of the bi-component of the network.

As seen in this short summary, there is extensive research on the subject network robustness, with many distinct approaches to this problem. This dissertation tackles some problems that haven't been addressed as extensively, including:

1. Study the impact of degree distributions on the robustness of multiplex networks, including the use of distinct degree distributions on a single multiplex network.
2. Study the relationship between layer robustness and global robustness of a multiplex network.
3. Adapt and apply optimization methods done in single-layer networks, on multiplex networks, including adapting previous robustness measures to a multi-layer context.
4. Apply simple multi-objective methods on layer robustness and global robustness, on multiplex networks.

3 Methodology and Implementation

This chapter details the development decisions regarding the development and programming section of this work, as well as the implementation details of the various algorithms used in each development stage. Section 3.1 details the broader decisions regarding the implementation. Section 3.2 describes the generation of the different network populations. Section 3.3 describes the process of simulating the different types of attacks and failures targeting the networks. Section 3.4 details the network optimization portion of this thesis and the algorithms used. Finally, Section 3.5 offers a summary of this chapter.

3.1 General aspects

The majority of this thesis was developed using the programming language Python, version 3.6. A high level programming language, such as Python, simplifies working with complex data structures and allows for a more flexible development process, not so focused on low level programming details, such as memory management. If the complexity of the problem at hands were to require a bigger necessity for memory efficiency or an overall faster computing speed, then a lower level language would have been more appropriate, such as C or C++. Together with Python, the PyCharm IDE was used. An IDE makes the programming environment easier to manage and configure, turning the development process smoother. Multiple public Python libraries were used, including NetworkX (creating and analysing network structures), NumPy (array and numerical computation) and Matplotlib (data visualization). The Gephi tool was also utilized to aid with the visualization and analysis of the used networks.

3.2 Network generation

The first development portion of this thesis was generating the network population. In total, 181 single-layer networks were created: 90 with an exponential distribution, 90 with a power-law distribution and 1 with a lattice distribution. All networks have 5000 nodes, with an average degree, <k>, of 2.6.

3.2.1 Power-Law

The networks with a power-law distribution were generated by sampling sequences with length n from a Pareto distribution. An element in that sample corresponds to the degree of a node in the network. Then, the network is generated by adding n nodes to the network and randomly assigning links in such a way that it follows the sample extracted from the power-law distribution. To extract the 90 different power-law samples, the function powerlaw_sequence from NetworkX was utilized.

3.2.2 Exponential

Networks with an exponential distribution were generated using Erdös-Rényi model, $G(n, M)$, where n is the desired number of nodes that the network should have, and M is the total number of links. This model variant works by generating all possible graphs with n nodes and M links, and uniformly choosing a random one. NetworkX's function gnm_random_graph implements this same model and was used to generate the 90 different networks.

3.2.3 Lattice

The lattice network, which is has a grid-like structure where every nodes connects to 4 adjacent nodes, was created using NetworkX's graph generator grid_2d_graph. Since a 5000 nodes network makes for an asymmetrical grid, some links had to be added to make sure all nodes have a degree of 4. Because all lattices would be identical, generating 1 network is sufficient.

3.2.4 Duplex networks

The generated single-layer networks were then coupled in 4 different sets of multiplex networks with two lawyers (duplex): 30 with 2 exponential layers, 30 with two power-law layers, 30 with one exponential layer and one power-law layer and 30 with one power-law layer and one with a lattice layer, totalling 120 duplex networks.

3.3 Measuring robustness of duplex networks

Robustness of single-layer networks is often measured by observing the behaviour of the largest cluster of the network, GCC, throughout an attack or failure event. The robustness of duplex networks was measured using an extended definition of the GCC, MCGC - mutually connected giant component. It follows the principle that if we remove a node in a layer, it may still be connected to the giant cluster through another layer, and therefore not isolated from the rest of the nodes. The relative size of the MCGC is calculated by adding temporary links between the equivalent nodes from the layers and performing a breadth-first search to find

the GCC of this network. Algorithm 1 describes, in more depth, the developed algorithm to calculate the MCGC size.

3.3.1 Random failures

To simulate node failures, caused by non-intentional behaviour, a layer is randomly selected, as well as one of its nodes to be removed, together with its links. This process is repeated until all nodes are removed. The pseudo-code is described in Algorithm 2.

3.3.2 Targeted attacks

3.3.2.1 Degree based attacks

Degree based attacks choose the node to attack in each iteration by ranking them by their degree. The node degrees are recalculated after a node is removed. The pseudo-code is described in Algorithm 3.

3.3.2.2 Betweenness based attacks

This attack ranks the nodes by the importance they have in connecting all other nodes of the network. More specifically, this metric counts the number of shortest paths that pass through a given node. The pseudo-code is described in Algorithm 4.

3.4 Optimization

The goal of the optimization section of this thesis is to study the impact that optimizing the robustness of a particular layer in a duplex network has on the robustness of the whole duplex network. This optimization method was first described in [13], and uses a rewiring mechanism as way of generating new neighbours in each iteration. It works as follows:

- Choose two distinct and disjoint links from the network, (i,j) and (k,l)
- Swap the links, by creating two new links (i,l) and (k,j) and deleting (i,j) and (k,l)

This mechanism generates child networks with slight variations and preserves the original degree distribution, minimizing structural and topological changes to the network that could otherwise undermine its functionality. The metric used to measure the robustness is the R measurement [13]. To measure the global robustness of the duplex networks, we extend the definition of the R metric from single-layer networks to multi-layer. The original R measure on single-layer networks works by sequentially removing the highest degree node of the network and summing the relative size of the GCC after each removal. To extend this measure to duplex networks, the GCC size is replaced by MCGC size, and the removed node is chosen between

both layers. The node with highest degree is chosen between the two layers, and removed only in the layer where it has the highest degree. To differentiate between both measures, the R measure is relabeled as R_l when measuring robustness of single-layer networks and R_d when measuring robustness of duplex networks. Algorithm 5 and Algorithm 6 show the pseudo-code for both R_l and R_d calculation, respectively. This thesis also compares the efficacy between a greedy approach, Algorithm 7, and simulated annealing, Algorithm 8.

The acceptance condition for this optimization algorithms changes accordingly to the following desired objects of study:

1. Optimize the robustness of one layer, R_l and study the impact on global robustness of the duplex network, R_d.
2. Optimize the global robustness of the duplex network, R_d, and measure the impact on the individual layers R_l.
3. Optimize both layer robustness and global robustness simultaneously (multi-objective).

For 1. and 2., the acceptance condition is based on R_l and R_d, respectively. For point 3), both R_l and R_d are used simultaneously, and it requires an improvement in both measures in order for the new network to be accepted.

3.5 Overview

This chapter described the technical work developed in this thesis. Section 3.1 described the design choices that went into the development. Section 3.2 presented the methods used to generate exponential networks, scale-free networks and lattice networks, to then be used as layers of duplex networks. Section 3.3 presented the algorithms used to simulate failures and attacks on duplex networks. Finally, section 3.4 presented the novel measure of robustness adapted from single-layer networks to duplex networks and the two algorithms used, greedy and simulated annealing.

Algorithm 1: Calculation of MCGC relative size

```
function calculate_mcgc(l1, l2);
Input  : Network layers l1 and l2
Output: mcgc size
Initialization;
# Disjoint union of both layers into one single network,nt
# Nodes from layer l2 get relabeled from [1, n] to [n+1, 2n]
nt = union(l1, l2);
for i in range(n) do
    # Add temporary links between equivalent nodes
    add_edge(i, i + n)
end
# Calculate mcgc as a standard gcc of the new network
gcc = list(max(connected_components(nt), key=len))
for i in range(len(gcc)) do
    # Relabel nodes to original id
    if gcc[i] > n-1 then
        gcc[i] = gcc[i] - n
    end
end
# Remove duplicate nodes
gcc = list(set(gcc))
# Divide mcgc absolute size by n, the network size;
mcgc_size = len(gcc) / n
return mcgc_size
```

Algorithm 2: Random failures

```
function random_failures(l1, l2);
Input  : Network layers l1 and l2
Output: Array of MCGC values
Initialization;
mcgc_array = []
while removed_nodes < total_nodes do
    # choose random layer
    layer = rd.choice(["l1", "l2"])
    # choose random node from layer
    node = rd.choice(layer.nodes)
    layer.remove_node(node) removed_nodes += 1
    # calculate mcgc size
    mcgc_array += [calculate_mcgc(l1, l2)]
end
return mcgc_array
```

Algorithm 3: Degree based attack

```
function degree_attack(l1, l2);
Input  : Network layers l1 and l2
Output: Array of MCGC values
Initialization;
mcgc_array = [];
while removed_nodes < total_nodes do
    # Calculate node degrees in each layer and choose max;
    max_node_l1 = max(l1.nodes, key=degree);
    max_nod_l2 = max(l2.nodes, key=degree);
    node = max(max_node_l1, max_node_l2);
    if max_node_l1 > max_node_l2 then
        l1.remove_node(node);
    else
        l2.remove_node(node);
    end
    removed_nodes += 1;
    # calculate mcgc size;
    mcgc_array += [calculate_mcgc(l1, l2)];
end
return mcgc_array
```

Algorithm 4: Betweenness centrality based attack

```
function betweenness_centrality_attack(l1, l2);
Input  : Network layers l1 and l2
Output: Array of MCGC values
Initialization;
mcgc_array = []
while removed_nodes < total_nodes do
    # Calculate betweenness centrality of every node in each layer and choose max
    max_node_l1 = max(l1.nodes, key=betweenness_centrality)
    max_node_l2 = max(l2.nodes, key=betweenness_centrality)
    node = max(max_node_l1, max_node_l2)
    if max_node_l1 > max_node_l2 then
        l1.remove_node(node)
    else
        l2.remove_node(node)
    end
    removed_nodes += 1
    # calculate mcgc size
    mcgc_array += [calculate_mcgc(l1, l2)]
end
return mcgc_array
```

Algorithm 5: Calculation of R_l

```
function calculate_R_l(l1);
Input  : Network layer l1
Output: Robustness value R_l for layer l1
Initialization;
gcc_sizes = []
while removed_nodes < total_nodes do
    # Choose node with highest degree
    node = max(l1.nodes, key=degree)
    # Remove node from network
    l1.remove_node(node)
    removed_nodes += 1
    # Calculate GCC relative size
    gcc = max(connected_components(l1), key=len)
    gcc_sizes.append(len(gcc) / (n-1))
end
# Sum all gcc_sizes and normalize by size of network, n
return sum(gcc_sizes)/n
```

Algorithm 6: Calculation of R_d

```
function calculate_R_d(l1, l2);
Input  : Network layers l1 and l2
Output: Robustness value R_d for duplex network
Initialization;
mcgc_sizes = []
while removed_nodes < total_nodes do
    # Choose node with highest degree between both layers
    max_node_l1 = max(l1.nodes, key=degree)
    max_node_l2 = max(l2.nodes, key=degree)
    node = max(max_node_l1, max_node_l2)
    # Remove node from network
    if max_node_l1 > max_node_l2 then
        l1.remove_node(node)
    else
        l2.remove_node(node)
    end
    removed_nodes += 1
    # Calculate MCGC relative size
    mcgc_size += calculate_mcgc(l1, l2)
    mcgc_sizes.append(mcgc_size / (n-1))
end
# Sum all gcc_sizes and normalize by size of network, n
return sum(gcc_sizes)/n
```

Algorithm 7: Greedy optimization algorithm

```
function greedy_optimization(max_iteration, l1, l2);
Input  : Network layers l1 and l2
Output: Rewired network layers l1 and l2
Initialization;
r_l = calculate_r_l(n, l1);
r_d = calculate_r_d(n, l1, l2);
while iteration < max_iteration do
    # Choose two different edges to rewire;
    edges = list(l1.edges());
    e_1 = rd.choice(edges);
    e_2 = rd.choice(edges);
    # Create new edges;
    n_e_1 = (e_1[0], e_2[1]);
    n_e_2 = (e_2[0], e_1[1]);
    # Add new edges and remove old edges;
    l1.remove_edges_from([e_1, e_2]) ;
    l1.add_edges_from([n_e_1, n_e_2]) ;
    # Calculate new R_l value;
    r_l_new = calculate_r_l(n, l1) ;
    r_d_new = calculate_r_d(n, l1, l2) ;
    # If new layer is more robust ;
    if r_l_new > r_l then
        # Keep new layer and save robustness values;
        r_l = r_lnew r_d = r_dnew else
            # If not, undo changes to layer;
            l1.remove_edges_from([n_e_1, n_e_2]);
            l1.add_edges_from([e_1, e_2]);
        end
        iteration += 1 ;
    end
    return l1, l2
```

Algorithm 8: Simulated annealing optimization algorithm

function simulated_annealing_optimization($max\_iteration, l1, l2$);
Input : Network layers $l1$ and $l2$
Output: Rewired network layers $l1$ and $l2$
Initialization;
r_l = calculate_r_l(n, l1);
r_d = calculate_r_d(n, l1, l2);
temperature = 1;
while *iteration* < *max_iteration* **do**
    temperature = temperature * 0.999;
    # Choose two different edges to rewire;
    edges = list(l1.edges());
    e_1 = rd.choice(edges);
    e_2 = rd.choice(edges);
    # Create new edges;
    n_e_1 = (e_1[0], e_2[1]);
    n_e_2 = (e_2[0], e_1[1]);
    # Add new edges and remove old edges;
    l1.remove_edges_from([e_1, e_2]) ;
    l1.add_edges_from([n_e_1, n_e_2]) ;
    # Calculate new R_l value;
    r_l_new = calculate_r_l(n, l1) ;
    r_d_new = calculate_r_d(n, l1, l2) ;
    # If new layer is more robust ;
    if *r_l_new > r_l or exp((r_l_new - r_l) / temperature) ≥ random()* **then**
        # Keep new layer and save robustness values;
        $r_l = r_{ln}ew$ $r_d = r_{dn}ew$ **else**
            # If not, undo changes to layer;
            l1.remove_edges_from([n_e_1, n_e_2]);
            l1.add_edges_from([e_1, e_2]);
        end
        iteration += 1 ;
    end
    return $l1, l2$

4 Results

This chapter presents the results obtained from the generated networks and the methods described in the previous chapter, Section 4.1 presents the results obtained when simulating random failures and targeted attacks on single layer networks, serving as a control subject. Next, on Section 4.2, the results for random failures and targeted attacks on duplex networks are presented. Lastly, Section 4.3 presents the results of the optimization procedures done on duplex networks, including single objective optimization on R_s and R_m separately (Section 4.3.1) and a simple multi-objective procedure on both R_s and R_m measures (Section 4.3.2), using the greedy algorithm the simulated annealing algorithm.

4.1 Single Layer networks

Previous results have shown that single-layer networks with an exponential degree distribution are robust against targeted attacks, whether it be degree based or betweenness centrality based, and fragile against random failures, while networks with a power-law degree distribution are robust against random failures but fragile against targeted attacks. To simulate these results, 30 Erdös-Rényi networks and 30 Scale-Free networks were generated using the methods described in Chapter 3. Figure 4.1 and Figure 4.2 show the behaviour of the Erdös-Rényi network and the Scale-Free network, respectively, under random failures (red), degree attacks (green) and betweenness centrality attacks (yellow). The results show a noticeable difference in behaviour between the two networks. The scale free network is noticeably more robust against random failures, showing a slow and delayed reduction of the size of its largest connected component and requires $\approx 90\%$ of its nodes to be removed for it to completely collapse. In contrast, the largest connected component of the Erdös-Rényi network shows a much steeper drop of its size. As for targeted attacks, scale-free networks collapse much easier than Erdös-Rényi network do, with the largest connected component collapsing when only $\approx 5\%$ of its nodes are removed. Both types of attacks, degree based and betweenness centrality based, lead to similar behaviour, with degree based attacks being slightly more destructive for both type of networks.

4.2 Distribution Combination

This section aims to ascertain whether the behaviour of single-layer networks carries over when these layers are combined into duplex networks. For example, if an Erdös-Rényi network

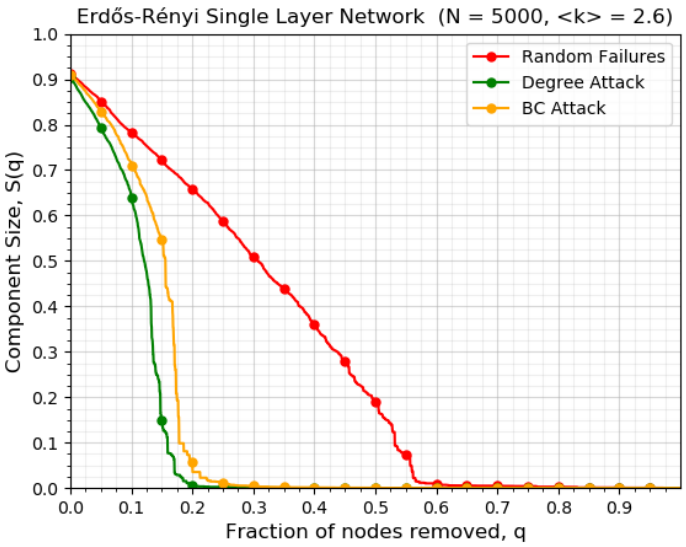

Figure 4.1: Robustness of single-layer Erdös-Rényi network. $N = 5000, < k >= 2.6$.

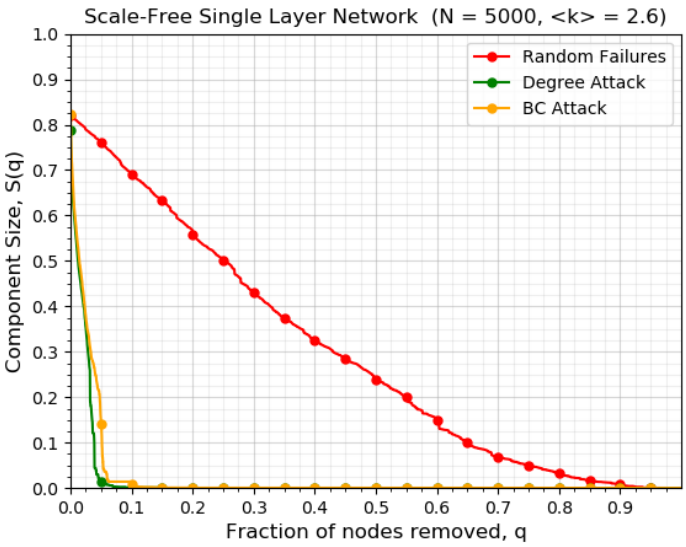

Figure 4.2: Robustness of single-layer scale-free network. $N = 5000, < k >= 2.6$.

is more robust against targeted attacks, is this also true when two Erdös-Rényi networks are combined into one duplex network? Also, what happens when a layer that is robust against targeted attacks is coupled with a layer that is fragile to these attacks? Which distribution is more impactful in the global robustness of the duplex network? In total, 4 different configurations of duplex networks were created, by arranging single-layer networks in groups of two: two Erdös-Rényi layers (ER-ER), one Erdös-Rényi layer with one scale-free layer (ER-SF), two scale-free layers (SF-SF) and one lattice layer with one scale-free layer (L-SF). Every layer has 5000 nodes and an average degree of $< k >= 2.6.$, except for the lattice layers that have an average degree of $< k >= 4$.

4.2.1 ER-ER and SF-SF Networks

The ER-ER duplex network behaves similarly to single-layer Erdös-Rényi networks. As shown in Figure 4.3, the robustness of ER-ER networks against targeted attacks is almost identical as for the single-layer network in Figure 4.1, with the largest connected component completely collapsing when 20% of the nodes are removed in a degree based attack (blue) and 25% in a betweenness centrality attack(green). When suffering random failures (red), the ER-ER network continues to be more fragile than the SF-SF network (Figure 4.4). The ER-ER network shows a more delayed reduction of its largest component size when compared to the single-layer Erdös-Rényi network, even though they both collapse at around the same fraction of removed nodes. This delay could be explained by the general behaviour of multiplex networks, seeing that when a node is removed from one layer, it may still be connected to the connected component through the alternative layer, therefore causing the delayed reduction of the connected component, particularly when the connected component is still significantly large.

The SF-SF duplex network also displays the behaviour observed in the single-layer Scale-

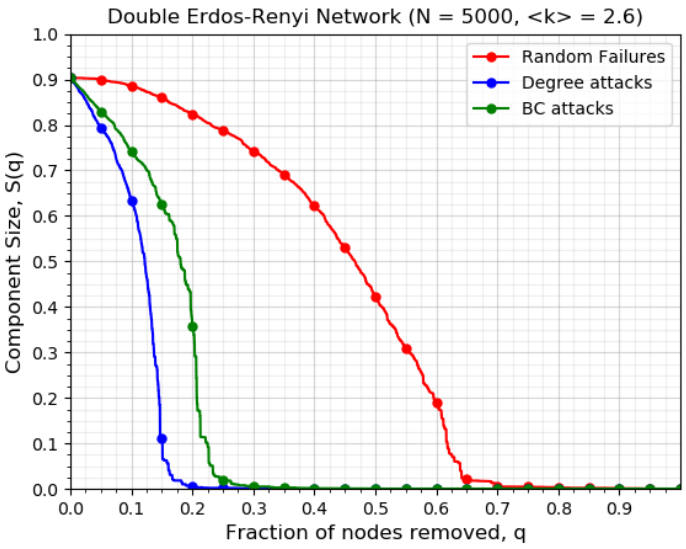

Figure 4.3: Robustness of ER-ER duplex networks under random failures and targeted attacks. $N = 5000, < k >= 2.6$.

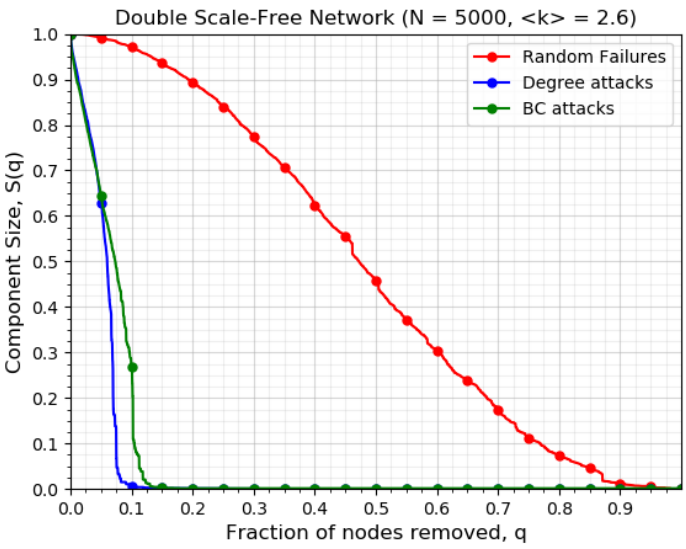

Figure 4.4: Robustness of SF-SF duplex networks under random failures and targeted attacks. $N = 5000, < k >= 2.6$.

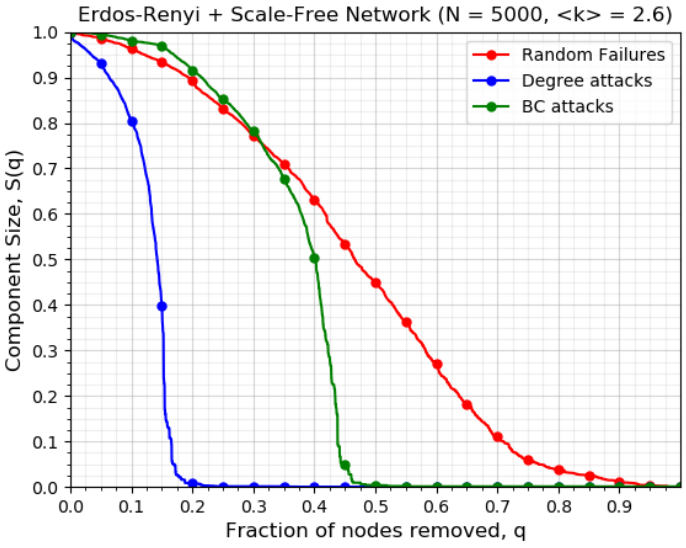

Figure 4.5: Robustness of ER-SF duplex networks under random failures and targeted attacks. $N = 5000, < k >= 2.6$.

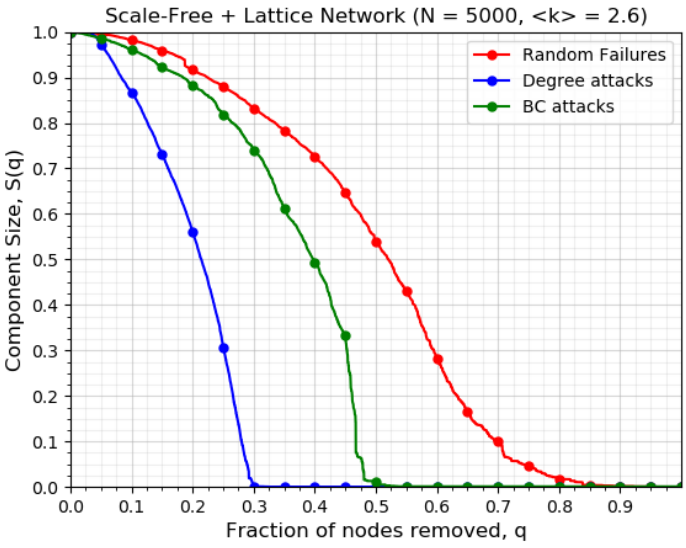

Figure 4.6: Robustness of SF-L duplex networks under random failures and targeted attacks. $N = 5000, < k >= 2.6$.

Free network. It remains fragile against targeted attacks, requiring only 10% (degree attacks, blue) and 15% (betweenness centrality attacks, green) of nodes to be removed to cause the collapsing of the connected component. It also keeps the strong robustness against random failures (red), requiring 90% of node removal to collapse the connected component. Once again, the delayed reduction of the largest component size observed in the ER-ER networks, under random failures, is present in SF-SF networks as well, which is particularly noticeable when the largest component is larger than 70%.

Comparing ER-ER networks against SF-SF networks, the strengths and weaknesses observed in single-layer networks manifest themselves in the duplex configurations. The SF-SF networks are significantly more robust against random failures than ER-ER networks, but also significantly more fragile against targeted attacks than ER-ER networks. Given these results, it possible to conclude that, in fact, the robustness properties of ER and SF single-layer networks carry over to duplex networks, and the degree distributions remain as the main contributors for the observed robustness behaviour.

4.2.2 ER-SF Networks

The combination of an ER layer with a SF layer shows some interesting properties. Figure 4.5 shows that these ER-SF networks exhibit the robust behaviour that each of its layers provide individually. They show high robustness to random failures (red), which are characteristic of scale-free networks and, simultaneously, show high robustness to targeted attacks (blue and green), which are characteristic of Erdös-Rényi networks. It shows the same high robustness to targeted attacks as ER-ER networks do, as well as high robustness to random failures observed in SF-SF networks. It can be concluded, then, that this configuration can take advantage of the best characteristics of each layer and make a duplex network that showcases robustness against both random failures and targeted attacks.

4.2.3 L-SF Networks

This combination of distributions, although similar to ER-SF, shows some slight differences (Figure 4.6). The first aspect to notice is the improved robustness in both random failures (red) and targeted attacks(blue and green) for smaller fractions of removed nodes. This can be explained by the geometrical property of the lattice. By acting as a regular grid, it guarantees that even if all nodes are removed from the scale-free layer, the largest connected component will remain fully connected on the lattice layer. The most noticeable behaviour in this L-SF configuration is the improved robustness when facing degree based attacks, when compared with the ER-SF network. Again, the topological properties of the lattice explain this phenomenon. Because all nodes in the lattice have a degree of 4 and in each iteration of the attack, the node to be removed is only removed in the layer where it has the highest degree. Therefore, only when all nodes with a degree above 4 are removed from the scale-free network, can the attack algorithm start to remove nodes from the lattice layer. Until that point, the largest connected component remains fully connected.

4.3 Optimization of network robustness

4.3.1 Layer robustness optimization

As it has been shown in single-layer networks[13,14,17,19,23], it is possible to increase the robustness of a network by using optimization methods, together with rewiring mechanisms. This section aims to find if optimizing the robustness of a single layer, R_l leads to an increase on the global robustness of a duplex network, R_d. Figures 4.7 to 4.12 are example samples from the the results obtained from both greedy and simulated annealing on ER-ER, SF-SF and ER-SF duplex networks. Table 4.1 summarizes the results, showing the obtained improvements of robustness in percentage.

$$\%\, of change = \frac{new\, robustness - old\, robustness}{old\, robustness} * 100. \tag{4.1}$$

The results show that optimizing the robustness of one of the layers, R_l, of a duplex network leads to an improvement in the global robustness R_d of the duplex network, in all the different distribution configurations. The ER-SF duplex network shows the best results, with an average R_d improvement of 8.75% with the greedy algorithm and 7.54% with the simulated annealing algorithm. The best R_d improvement obtained from the whole population happened on an ER-SF network when using simulated annealing, showing an improvement of 17.33% in the global robustness of the duplex network. The results also show that the greedy algorithm is able to achieve better results than the simulated annealing algorithm. A possible explanation for this outcome could be that the early iterations of the simulated annealing algorithm, that allow for worse states to be accepted, lead to network configurations that strongly decrease the robustness of the network.

4.3.2 Global robustness optimization

The optimization procedure is now repeated, but using the R_d measure, the robustness of the duplex network, as the optimization goal. The aim of this method is to find if guiding the optimizing algorithm using a global robustness measure leads to an increase in the robustness measure of the independent layers. Figures 4.13 to 4.18 are example samples from the results obtained from both greedy and simulated annealing on ER-ER, SF-SF and ER-SF duplex networks. Table 4.2 shows that although the algorithms can successfully optimize R_d, up to 26.82% improvement, R_l doesn't necessarily go along with this improvements. In some cases, like the one plotted in Figure 4.14, although R_d improves by 15.34%, R_l actually decreases by -4.6%. This phenomenon was observed in all three different network configurations. However, there exist cases where the optimization of R_d does lead to the increase of R_l, as seen in Figure 4.13%. The average results are relatively low, for both greedy and simulated annealing. In some cases, like for SF-SF and ER-ER networks, using simulated annealing, the average variation of robustness is actually negative, as seen in Table 4.2. This results lead to the conclusion that optimizing the robustness of a duplex network using a global robustness measure, doesn't necessarily lead

to an improvement of the robustness of its layers and can, in fact, make them more fragile.

4.3.3 Multi-objective optimization on layer and global robustness

The previous results seem to indicate that 1) Optimizing the robustness of one layer leads to a consistent improvement in the robustness of the whole duplex network and 2) optimizing the robustness of the whole duplex network does not necessarily improve the robustness of the individual layers, and can make them more fragile. This section aims to find whether R_l and R_d can be optimized simultaneously or if there is a conflict between them. The greedy algorithm and simulated annealing algorithm from the two previous sections are modified in order to only accept the new rewired network if both R_l and R_d have improved compared to the previous network. Figures 4.19 to 4.24 show some examples for both algorithms and duplex configurations. Table 4.3 showcases the obtained results, which show a positive increment of both R_l and R_d for all different duplex networks and for the two algorithms. It seems, then, that it is possible to simultaneously improve the global robustness of a duplex network and the robustness of its layers.

4.4 Overview

This chapter presented the results obtained from the proposed methods in chapter 3 and from the generated network population. After successfully replicating the literature results on single-layer networks robustness [2,32], the results on duplex networks showed some interesting behaviour. First, the proposed theory that the degree distributions of the individual layers impact the duplex in similar ways, is true. While the ER-ER duplex network is robust to targeted attacks and fragile to random failures, just like its ER layers, the SF-SF network is robust to random failures and fragile against targeted attacks, just like its SF layers. The ER-SF network, incorporating an Erdös-Rényi layer and a Scale-Free layer, shows improved robustness against targeted attacks, when compared with SF-SF networks, and also shows improved robustness against random failures, when compared with ER-ER networks. Therefore, it seems that ER-SF networks inherit the strengths from both of its layers. The L-SF network, which incorporates a lattice layer and a scale-Free layer, shows similar behavior as the ER-SF networks, with an improved robustness for small-scale attacks and failures, which is attributed to the particular single-point distribution of the Lattice Layer. The results from chapter 4.3 show that optimizing the robustness of the individual layers, R_l, also leads to an improvement in the global robustness of the duplex network, R_d, for the 3 different studied duplex configurations. However, when the global robustness is optimized, it does not necessarily lead to an improvement of the robustness of the individual layers, and can cause them to become more fragile. Multi-objective optimization on R_l and R_d showed that it is possible to substantially and simultaneously improve the robustness of the individual layers and the global duplex network.

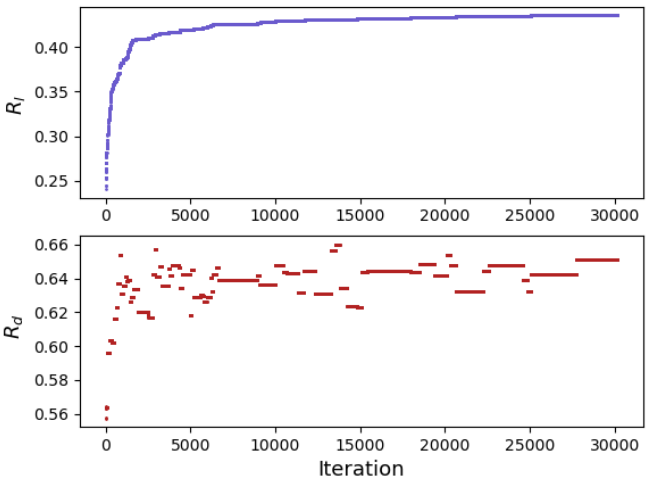

Figure 4.7: Greedy optimization of layer robustness on an ER-ER network.

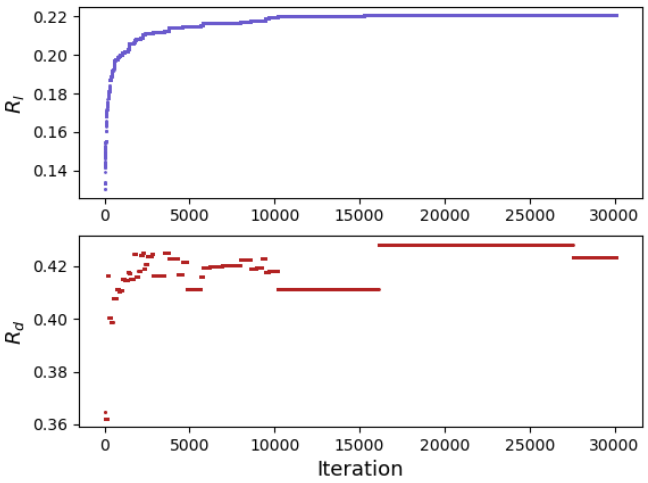

Figure 4.8: Greedy optimization of layer robustness on an SF-SF network.

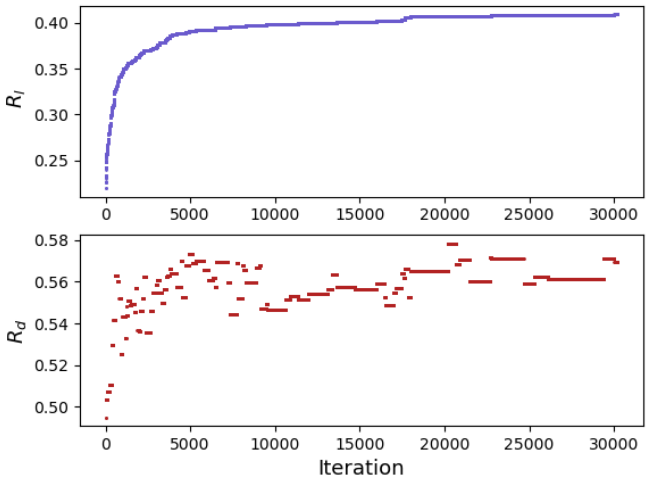

Figure 4.9: Greedy optimization of layer robustness on an ER-SF network.

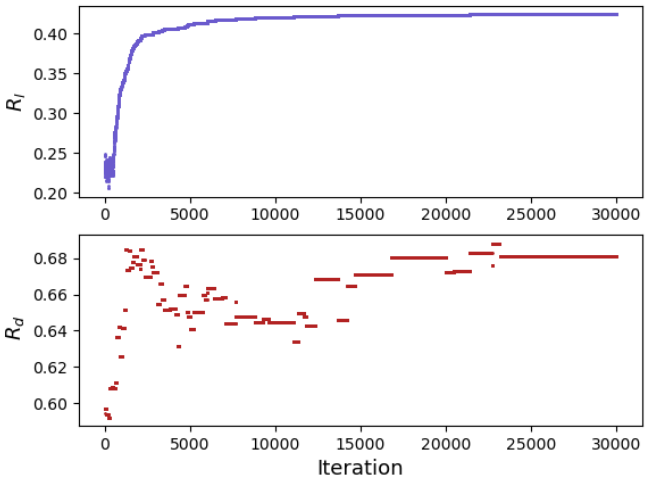

Figure 4.10: Simulated annealing optimization of layer robustness on an ER-ER network.

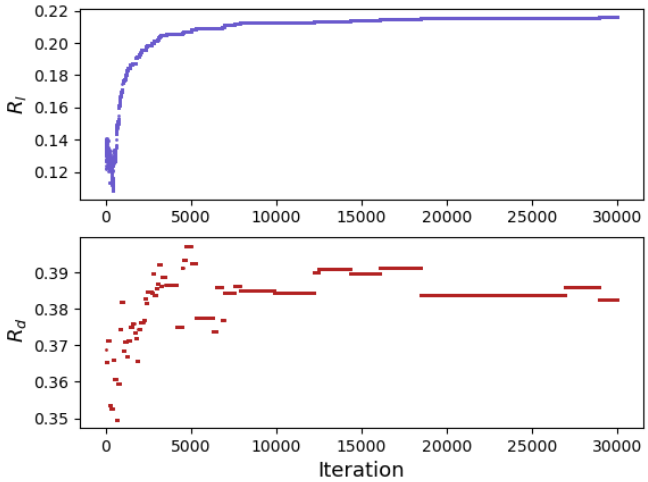

Figure 4.11: Simulated annealing optimization of layer robustness on an SF-SF network.

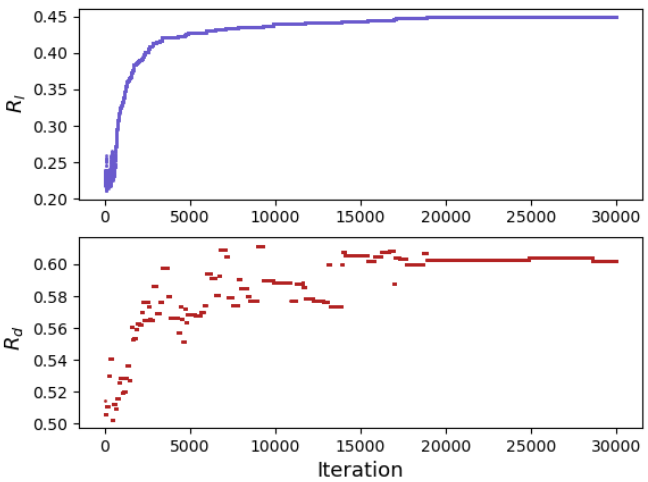

Figure 4.12: Simulated annealing optimization of layer robustness on an ER-SF network.

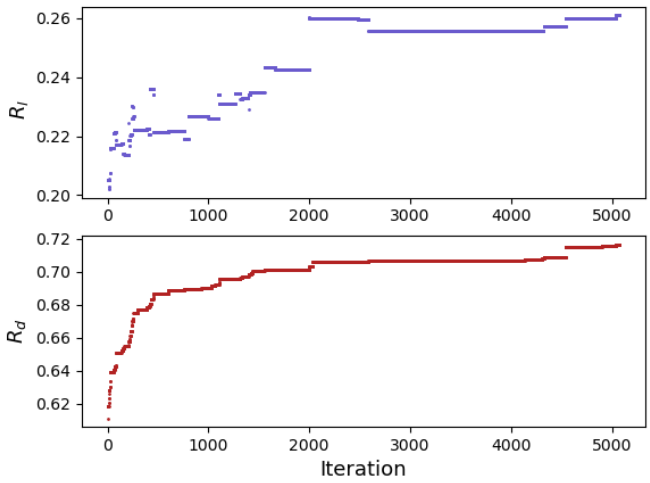

Figure 4.13: Greedy optimization of duplex robustness on an ER-ER network.

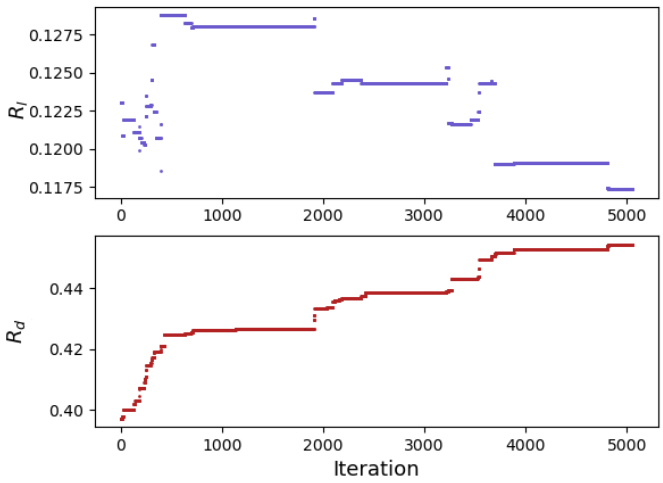

Figure 4.14: Greedy optimization of duplex robustness on an SF-SF network.

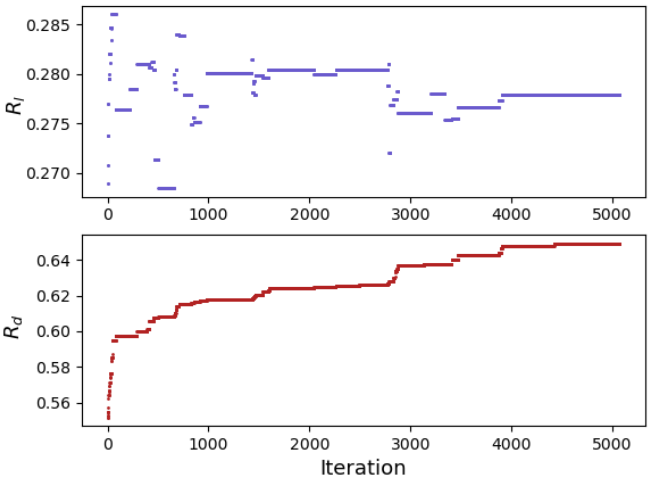

Figure 4.15: Greedy optimization of duplex robustness on an ER-SF network.

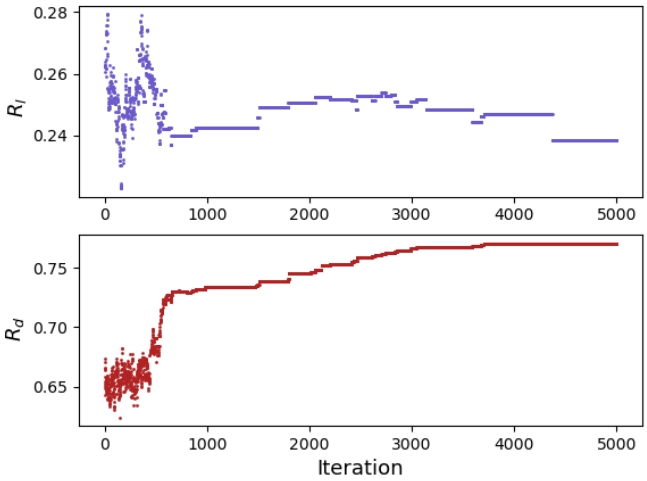

Figure 4.16: Simulated annealing optimization of duplex robustness on an ER-ER network.

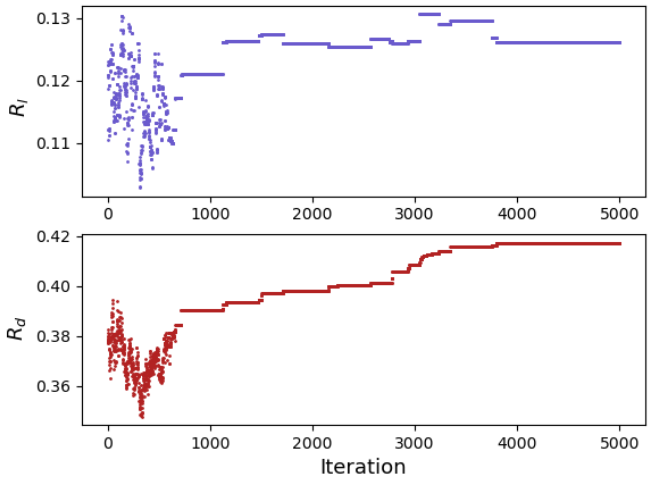

Figure 4.17: Simulated annealing optimization of duplex robustness on an SF-SF network.

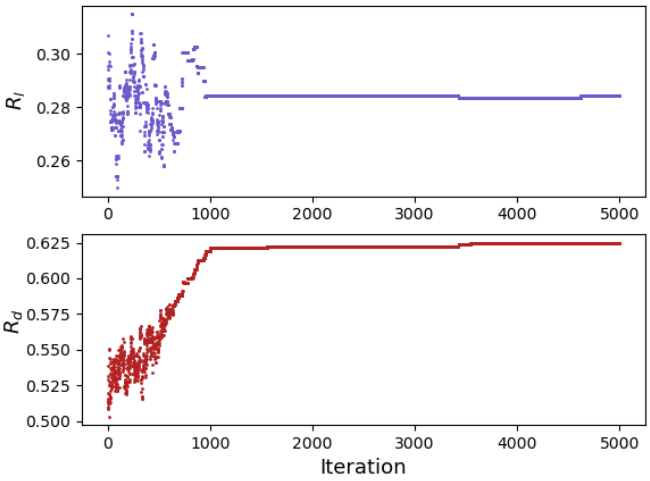

Figure 4.18: Simulated annealing optimization of duplex robustness on an ER-SF network.

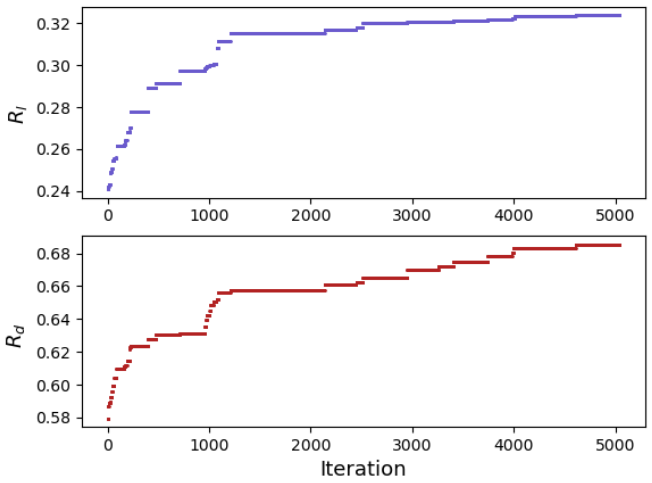

Figure 4.19: Greedy multi-objective optimization of R_l and R_d on an ER-ER network.

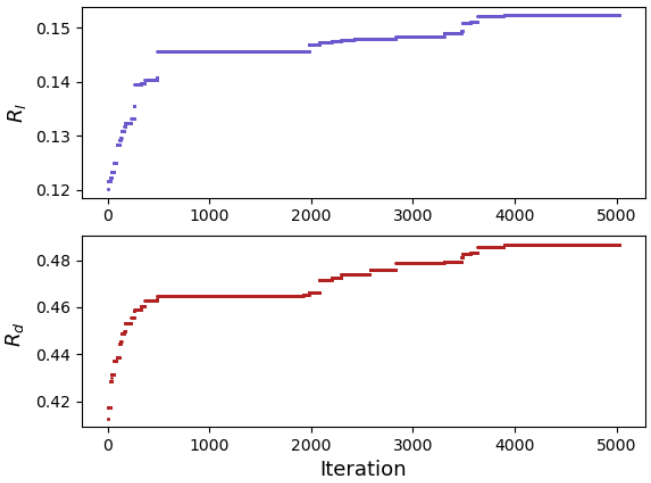

Figure 4.20: Greedy multi-objective optimization of R_l and R_d on an SF-SF network.

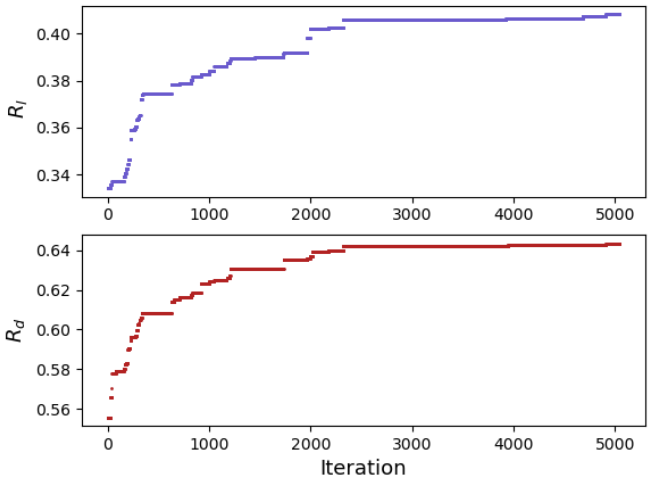

Figure 4.21: Greedy multi-objective optimization of R_l and R_d on an ER-SF network.

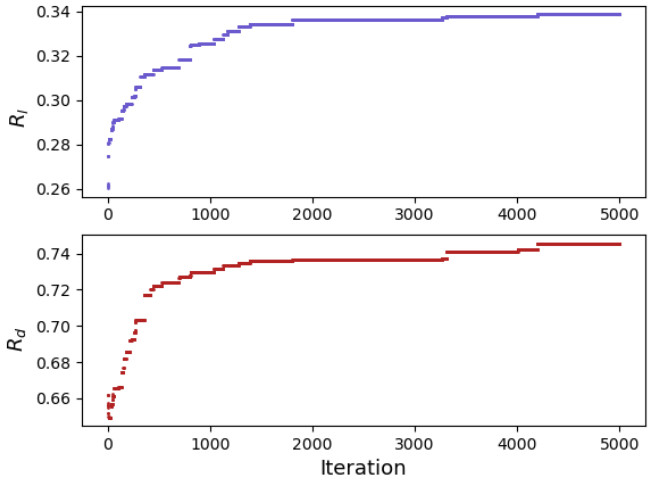

Figure 4.22: Simulated annealing multi-objective optimization of R_l and R_d on an ER-ER network.

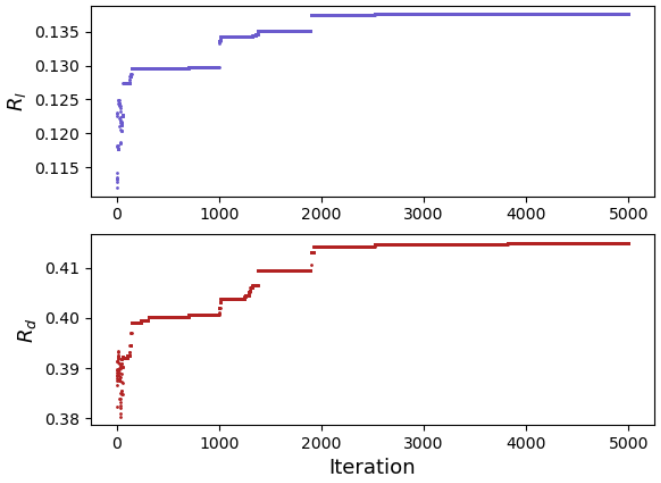

Figure 4.23: Simulated annealing multi-objective optimization of R_l and R_d on an SF-SF network.

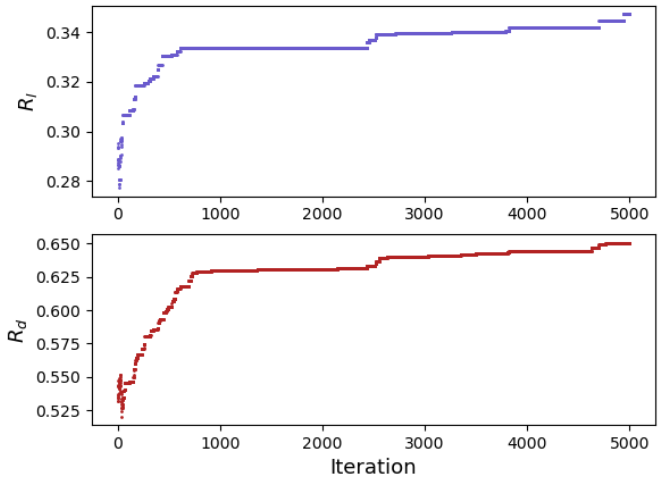

Figure 4.24: Simulated annealing multi-objective optimization of R_l and R_d on an ER-SF network.

	Greedy				Simulated Annealing			
	R_l		R_d		R_l		R_d	
	Best	Avg	Best	Avg	Best	Avg	Best	Avg
ER-ER	109.01%	69.02%	16.82%	7.59%	104.72%	68.58%	14.58%	6.91%
SF-SF	92.12%	66.20%	16.15%	4.92%	89.58%	62.98%	13.46%	2.91%
ER-SF	104.05%	75.62%	13.41%	8.75%	105.69%	65.56%	17.33%	7.54%

Table 4.1: Robustness optimization guided by R_l.

	Greedy				Simulated Annealing			
	R_l		R_d		R_l		R_d	
	Best	Avg	Best	Avg	Best	Avg	Best	Avg
ER-ER	11.31%	4.26%	20.57%	13.90%	10.53%	-0.96%	17.23%	13.99%
SF-SF	13.91%	0.21%	24.87%	13.66%	4.59%	-2.33%	18.12%	12.54%
ER-SF	18.77%	5.98%	26.82%	18.13%	11.48%	3.45%	17.33%	20.24%

Table 4.2: Robustness optimization guided by R_d

	Greedy				Simulated Annealing			
	R_l		R_d		R_l		R_d	
	Best	Avg	Best	Avg	Best	Avg	Best	Avg
ER-ER	34.49%	27.52%	18.53%	13.87%	49.85%	31.07%	17.47%	12.84%
SF-SF	46.94%	31.91%	22.80%	15.03%	43.04%	29.83%	15.54%	11.08%
ER-SF	38.92%	29.05%	23.58%	17.61%	52.03%	29.45%	24.76%	15.25%

Table 4.3: Robustness optimization guided by R_l and R_d

5 | Conclusion

This thesis focused on the study of robustness of multiplex networks. The main findings were as follows:

- Duplex networks with two layers of the same degree distribution behave similarly as a single-layer network with that same degree distribution. A duplex network with two power-law distributions is robust against random failures and fragile against targeted attacks. A duplex network with two exponential distributions is robust against targeted attacks and fragile against random failures.

- A duplex network with one power-law layer and one exponential layer is more robust against targeted attacks than a double power-law duplex network. It is more robust against random failures than a double exponential duplex network, making it an ideal duplex configuration when targeted attacks and random failures are present.

- A duplex network with one power-law layer and one lattice layer behaves similarly to a duplex network with one power-law layer and one exponential layer. However, it shows increased robustness for small-scale degree-based attacks and random failures. The improved robustness against degree-based attacks can be attributed to the particular single-point distribution of the lattice layer, that guarantees the integrity of the MCGC up until the point where all nodes of degree larger than four are removed. The improved robustness against random failures can be explained by the grid-like structure that the lattice layer provides to the duplex network, allowing the duplex network to be connected for small fractions of removed nodes.

- Optimizing robustness of individual layers in a duplex network leads to increased robustness in the whole duplex network. However, when the global robustness is optimized, it does not necessarily lead to an improvement of the robustness of the individual layers, and can cause them to become more fragile.

- Multi-objective optimization showed that it is possible to substantially and simultaneously improve the robustness of the individual layers and the global duplex network.

5.1 Future Work

Regarding the work done on experimenting with different degree distributions, it would be interesting to further investigate how other degree distributions behave when used in a multiplex configuration, such as the ones studied and introduced in [1,6]. Also, it could be interesting to study how impactful the degree distribution of one layer is in multiplex networks with more than two layers. The optimization portion of this thesis, although results showed that optimizing one layer leads to a global increase in robustness, it would be interesting to study how well this result scales with multiplex networks with more than two layers. Furthermore, it would be interesting to see if optimizing all layers separately leads to a significant improvement of global robustness, compared against only optimizing one layer. The work done on multi-objective optimization could be further studied by using other state-of-the art optimization algorithms such as the one used for single-layer networks in [23]. Lastly, as this thesis focused on multiplex networks with no degree correlation between layers, it would be interesting to understand if this results are also valid in interdependent networks, where layers are not fully independent, and in networks that have degree correlation, and study possible robustness properties that could emerge in these networks.

Bibliography

[1] André X. C. N. Valente, Abhijit Sarkar & Howard A. Stone, "Two-Peak and Three-Peak Optimal Complex Networks" Phisical Review Letters **92**(11) (2004)

[2] R. Albert, H.Jeong & A.-L. Barabási, "Error and Attack Tolerance of Complex Networks." Nature (London) **406**,378 (2000)

[3] Erdös, P. & Rényi, A., "On the evolution of random graphs." Publ. Math. Inst. Hung. Acad. Sci. 5, 17â60 (1960).

[4] Watts, D. J. & Strogatz, S. H., "Collective dynamics of 'small-world' networks." Nature 393, 440 - 442 (1998)

[5] Bunde, A. & Havlin, S. (eds), "Fractals and Disordered Systems." (Springer, New York, 1996)

[6] G. Paul, T. Tanizawa, S. Havlin & H. E. Stanley, "Optimization of Robustness of Complex Networks." (2004)

[7] A.-L. Barabási, and R. Albert, Science 286, 509 (1999).

[8] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "Computer Communications Review" 29, 251(1999).

[9] J. F. F. Mendes, S. N. Dorogovtsev, and A. F. Ioffe, "Evolution of Networks: From Biological Nets to the Internet and the WWW" Oxford University Press, Oxford, (2003).

[10] Sun, Yu, Peiyang Yao, Dongdong Shui and Yun Zhong, "Analysis of Robustness of Complex Networks based on Optimization Theory." (2016).

[11] Maslov, Sergei, Kim Sneppen and Alexei Zaliznyak, "Detection of topological patterns in complex networks: correlation profile of the internet." (2004).

[12] Mahendra, Piraveenan, Gnana Thedchanamoorthy, Mohammed Shahadat Uddin and Kon Shing Kenneth Chung, "Quantifying topological robustness of networks under sustained targeted attacks". Social Network Analysis and Mining 3 (2013): 939-952.

[13] Schneider, Christian M., André A. Moreira, José S. Andrade, Shlomo Havlin and Hans J. Herrmann, "Mitigation of Malicious Attacks on Networks." Proceedings of the National Academy of Sciences of the United States of America 108 10 (2011): 3838-41 .

[14] V. H. P. Louzada, F. Daolio, H. J. Herrmann and M. Tomassini, "Smart rewiring for network robustness." Journal of Complex Networks (2013), 1(2): 150-159.

[15] V. H. P. Louzada, F. Daolio and H. J. Herrmann et. al, "Propagation Phenomena in Real World Networks." (2015).

[16] Burke, Edmund K. and Graham Kendall, "Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques." (2005).

[17] Zeng, An and Weiping Liu, "Enhancing network robustness against malicious attacks." Physical review. E, Statistical, nonlinear, and soft matter physics 85 6 Pt 2 (2012): 066130 .

[18] Tran, Hoang Anh Q., Akira Namatame, Augie Widyotriatmo and Endra Joelianto, "An optimization procedure for enhancing network robustness against cascading failures." 2014 Seventh IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA) (2014): 1-7.

[19] Ma, Liangliang, Jing Liu, Boping Duan and Mingxing Zhou, "A theoretical estimation for the optimal network robustness measure R against malicious node attacks." (2015).

[20] Molloy M. and Reed B., Comb. Probab. Comput., 7 (1998) 295.

[21] Callaway D. S., Newman M. E. J., Strogatz S. H. and Watts D. J., Phys. Rev. Lett., 85 (2000) 5468.

[22] Newman M. E. J., Strogatz S. H. and Watts D. J., Phys. Rev. E, 64 (2001) 026118.

[23] Zhou, Mingxing and Jing Liu, "A Two-Phase Multiobjective Evolutionary Algorithm for Enhancing the Robustness of Scale-Free Networks Against Multiple Malicious Attacks." IEEE Transactions on Cybernetics 47 (2017): 539-552.

[24] K. Deb, A. Pratap, S. Agarwal, and T. Meyarivan, "A fast and elitist multiobjective genetic algorithm: NSGA-II." IEEE Trans. Evol. Comput., vol. 6, no. 2, pp. 182-197, Apr. 2002.

[25] Liu, Jing, Mingxing Zhou, Shuai Wang and Penghui Liu., " A comparative study of network robustness measures." Frontiers of Computer Science 11 (2016): 568-584.

[26] Louzada, Vitor H. P., Fabio Daolio, Hans J. Herrmann and Marco Tomassini, "Generating Robust and Efficient Networks Under Targeted Attacks." (2012)

[27] Min, Byungjoon, Su Do Yi, Kyumin Lee and K I Goh, "Network robustness of multiplex networks with interlayer degree correlations." Physical review. E, Statistical, nonlinear, and soft matter physics 89 4 (2014): 042811.

[28] Zhao, Dawei, Lianhai Wang and Zhen Wang, "The robustness of multiplex networks under layer node-based attack." Scientific reports (2015).

[29] Kryven, Ivan and Ginestra Bianconi, "Enhancing the robustness of a multiplex network leads to multiple discontinuous percolation transitions." Physical review. E 100 2-1 (2019): 020301 .

[30] Newman, M. E., Strogatz, S. H. & Watts, D. J., "Random graphs with arbitrary degree distributions and their applications." Phys. Rev. E 64, 026118 (2001).

[31] Lee, Kyu-Min, Jung Yeol Kim, Won-kuk Cho, K.-I. Goh and I.-M. Kim. , "Correlated multiplexity and connectivity of multiplex random networks." (2012).

[32] Guillaume, Jean-Loup & Latapy, Matthieu Magnien, Clémence. , "Comparison of Failures and Attacks on Random and Scale-Free Networks." Proc. OPODIS. 186-196. (2004).