Optimized network robustness and dismantling

Bruno Diogo Mesquita de Sousa

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.

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

The most common robustness measures on complex networks include the percolation threshold and the R measurement [13]. The R measurement, equation 1, quantifies robustness by sequentially removing the highest degree node of the network and summing the relative size of the GCC after each removal. In the equation, N represents the total number of nodes of the network, Q represents the number of removed nodes, and s(Q) represents the size of the largest connected component of the network when Q nodes are removed.

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

The degree distribution of a network is the probability distribution of node degrees over the network. This paper studies the impact of 3 different degree distributions on multiplex networks. First, 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 paper also studies the effects of using Lattices, a regular network with a single-point distribution, together with power-law 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.

Multi-layer networks can be split in two main categories, multiplex and interdependent. Multiplex networks, the focus of this paper, have no dependencies between layers, meaning that removing a node in one layer does not propagate to the remaining layers, while interdependent networks can incorporate different dependence links between layers.

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, using simple optimization algorithms. This paper focuses on two main algorithms, greedy and simulated annealing. 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. 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.

3 Methodology

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. 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.

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.

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.

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.

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.

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.

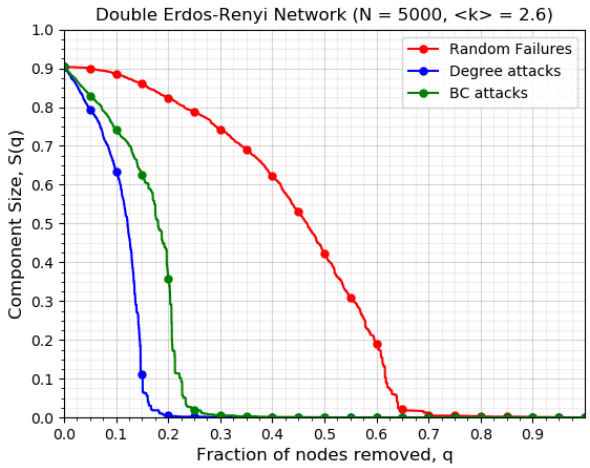

Figure 1: Robustness of ER-ER duplex networks under failures and attacks. $N = 5000, < k >= 2.6$

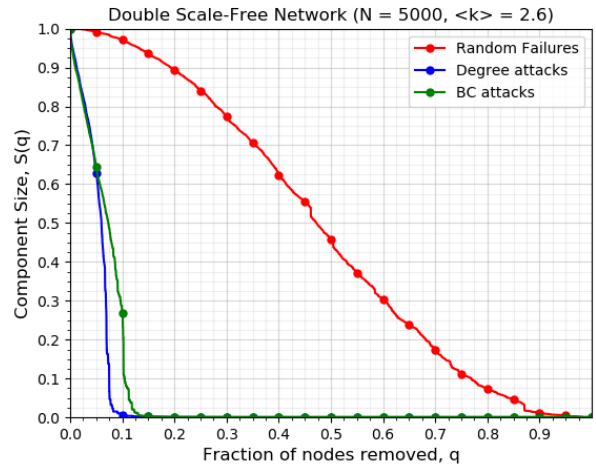

Figure 2: Robustness of SF-SF duplex networks under failures and attacks. $N = 5000, < k >= 2.6$

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.

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.

This paper studies 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.

4 Results

4.1 Degree distribution combination

The ER-ER duplex network behaves similarly to single-layer Erdös-Rényi networks. As shown in Figure 1, the robustness of ER-ER networks against targeted attacks is almost identical as in single-layer networks, 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

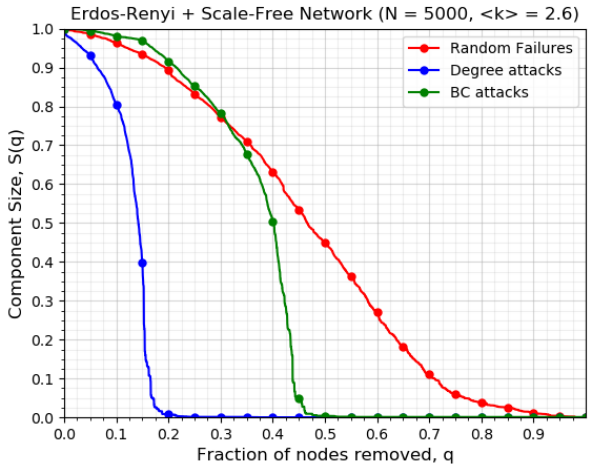

Figure 3: Robustness of ER-SF duplex networks under failures and attacks. $N = 5000, < k >= 2.6$

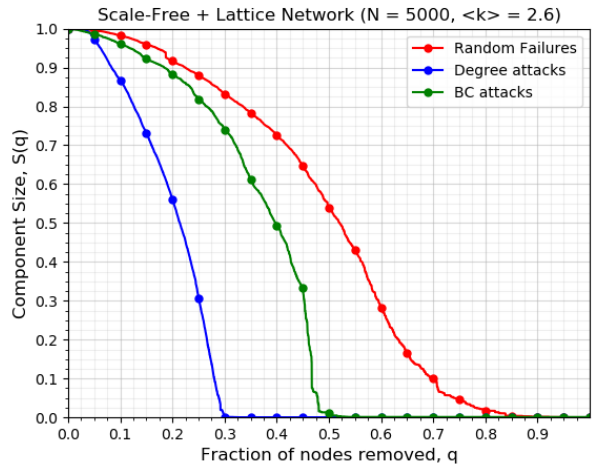

Figure 4: Robustness of SF-L duplex networks under failures and attacks. $N = 5000, < k >= 2.6$

failures (red), the ER-ER network continues to be more fragile than the SF-SF network (Figure 2). 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-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 observed robustness behaviour.

The combination of an ER layer with a SF layer shows some interesting properties. Figure 3 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.

The L-SF combination, although similar to ER-SF,shows some slight differences (Figure 4). 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.

4.2 Optimization of network robustness

4.2.1 Layer robustness optimization

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 improvement of 8.75% with the greedy algorithm and 7.54% with the simulated annealing algorithm. The best 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. Table 1 summarizes the results, showing the obtained improvements of robustness in percentage.

4.2.2 Global robustness optimization

The optimization procedure is now repeated, but using the R_d measure, the robustness of the duplex network. 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. Table 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, 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. 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 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.

4.2.3 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. Table 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.

	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 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 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 3: Robustness optimization guided by R_l and R_d

5 Conclusions and Future Work

This paper showed the behaviour of multiplex networks with two layers, incorporating different degree distributions such as exponential, scale-free and single-point, under random attacks and targeted attacks. It introduced a novel robustness measure adapted to multi-layer networks, originally introduced in [13], and showcased the performance of simple optimization algorithms (single and multi-objective) on improving robustness of multiplex networks. For future work, 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]. It could also be interesting to study how impactful the degree distribution of one layer is in multiplex networks with more than two layers. It would be interesting to study how well the optimization results scale 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, 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.

References

[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, 17–60 (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).