Robustness Metrics for Cascading Failures

Inês Ferreira (ist190395) and Ricardo Santos (ist190178)

***Abstract*— In networks that act as transportation systems, a local failure propagates to the surrounding nodes, possibly leading to cascading events. Motter and Lai [1] have shown that heterogeneous networks are susceptible to random breakdowns and targeted attacks. Here we extend their analysis, considering several strategies to assess robustness that might result in divergent conclusions - a network can be more or less vulnerable to attacks, depending on the indicators used. Our work may guide the design of defense strategies to halt the propagation of cascading failures.**

I. Introduction

It is well-known that real-world networks are robust to random failures, considering that we must remove almost all its nodes to fragment a scale-free network. We also recognize that, regarding targeted attack (to nodes with the highest degree, for example), we only need to remove a minimal amount of hubs to cripple a scale-free network. How about when the failure of a node depends on those around it? Can the removal of a single node trigger other nodes' failures? And can this effect propagate to the extreme limit in which the network is entirely fragmented?

In this paper, we use the Motter-Lai congestion model (2002) [1] to simulate cascading events. Motter-Lai's model is applied to networks that act as a transportation system, for which there's a constant flow of physical quantities, like electric power in a power grid or data packets on the Internet. Supposing that the quantities travel between nodes through the shortest path connecting them, the load on a given node is the number of shortest paths passing through it, which is directly linked to its betweenness centrality[1]. We define the maximum load a node can take before it collapses as its capacity, given by:

$$C_i = (1+\alpha)L_i \ , \qquad i = 1, 2, ..., N \ . \tag{1}$$

L_i is the load of a node and α is a tolerance parameter. When the current load of a node surpasses its capacity, it is removed from the network, leading to a redistribution of its load through other nodes. Consequently, these might also fail due to the extra load, leading to a cascading event that can propagate throughout the entire network.

In this paper, we study random breakdowns and targeted attacks using 3 different criteria: highest degree, highest betweenness centrality and highest clustering coefficient. We analyse in detail two scale-free, heterogeneous models - the power law model and the DMS minimal model - both of which have the following degree distribution, P, of the form:

$$P(k) \sim k^{-\gamma} \ . \tag{2}$$

We will start analysing the robustness of the network using

$$G = \frac{N'}{N} \ , \tag{3}$$

where N' is the size of the final largest connected component, after a cascading of failures, and N is the initial size of the largest connected component, which coincides with the total number of nodes.

We also define other robustness metrics to be used: the final number of nodes in the network; the final number of components in the network; and the final fraction of unconnected pairs of nodes in the network.

II. Methods

The cascading effects were studied in the following model-based networks:

- Power Law Model, generated using the IGRAPH (C++) function IGRAPH_STATIC_POWER_LAW_GAME.
- Random Graph (Erdos-Rényi Model), generated using the IGRAPH (C++) function IGRAPH_ERDOS_RENYI_GAME [2].
- DMS Minimal Model, generated using NETWORKX (PYTHON3) in the following way: we start with a fully connected network with 3 nodes. At each iteration, a new node is added by connecting it to the ends of a randomly selected edge. The process is repeated until the desired number of nodes is reached.

All networks are unweighted, undirected, have no multiedges or selfedges and comprehend only one connected component, meaning there is a path between any given pair of nodes in the network. For each network model, 10 networks were generated with different seeds.

To create the cascading failures, algorithm 1 was used.

Algorithm 1 Cascade Failure

```
Compute the capacity for each node
Choose an initial node according to a given criteria
Enqueue the initial node in the deletion list
while deletion list not empty do
    while deletion list not empty do
        Dequeue node from the deletion list
        Enqueue node in the deleted nodes list
        Delete all edges incident in that node
    end while
    Recompute the betweenness centrality of all nodes (current load)
    for all nodes do
        if current load > capacity then
            Enqueue node in the deletion list
        end if
    end for
end while
Delete all nodes in the deleted nodes list
```

[1] Throughout this paper, load and betweenness centrality will be used interchangeably.

[2] The functions used for both the power law and the random graph models can generate networks with nodes with degree 0. For that reason, the parameters were selected such that the largest connected component of these graphs had the desired number of nodes and average degree.

The initial capacity for each node, C_i, is computed according to equation 1, where L_i, the initial load, is the starting betweenness centrality of each node, computed by the IGRAPH (C++) function IGRAPH_BETWEENNESS.

The *initial node* (trigger) can be chosen either randomly, simulating a random breakdown, or, to simulate a targeted attack, based on one of the following criteria:

- Highest Degree, computed with the IGRAPH (C++) function IGRAPH_DEGREE;
- Highest Betweenness Centrality, obtained likewise the initial load;
- Highest Clustering Coefficient, given by the IGRAPH (C++) function IGRAPH_TRANSITIVITY_LOCAL_UNDIRECTED.

For each network, and for each value of α, 5 triggers were used. For the targeted attacks the triggers are the 5 nodes with the highest value in the selected metric.

The *deletion list* contains the nodes to be eliminated in each iteration. This list is initialized in line 3 with the chosen trigger.

The main cycle (lines 4 to 16) runs until there are no more nodes to be deleted. Inside it, there is a first cycle (lines 5 to 9) where, for each node dequeued from the *deletion list*, all the edges incident in it are eliminated. The node is also added to the *deleted nodes list*, that stores all nodes that were deleted throughout all iterations. We decided to only delete edges at this point since deleting the nodes themselves would lead to a rearrangement in the remaining nodes numeration, making it more difficult to process the results. Note that, if all the edges incident to a node are removed, its load will be zero, so, in practice, it is as if it was deleted. We refer to such nodes as deleted, for simplicity. After deleting all nodes in a given iteration the betweenness centrality is recomputed for the remaining nodes, which gives a measure of the current load in each node. A new *deletion list* is then created, with all the nodes whose load exceeds their capacity (line 12), and that are to be removed in the next iteration. When a state where the load of each node is constant and within capacity is reached, the cycle ends (there are no more node failures, that is, the cascade ended). All nodes in the *deleted nodes list* are then actually deleted from the network.

To evaluate the robustness of the networks, the following quantities are computed: number of remaining nodes in the network, size of the largest component, number of connected components and number of unconnected pairs of nodes. Both the size of the largest component and the number of components are computed with the IGRAPH (C++) function IGRAPH_CLUSTERS, and the number of unconnected pairs with IGRAPH (C++) function IGRAPH_SHORTEST_PATHS.

All the developed code can be accessed through [6].

III. Results and Discussion

A. Power Law Model with $\langle k \rangle \approx 2$

We now present the simulated results, starting with the study of random breakdowns and targeted attacks for a scale-free network with degree distribution according to (2) and an average degree of $\langle k \rangle \approx 2$.

It is clear in figure 1 that random breakdowns have almost no effect on the network. On the other hand, targeted attacks, especially to the nodes with the highest degree or load, have a notorious effect on the final size of the giant component. For these, even with a tolerance value of $\alpha = 1$, that is, each node has two times the capacity needed when the system is functioning normally, the giant component still gets reduced by 20% for degree-targeted attacks. This value is even larger if we target nodes with the highest betweenness centrality - a reduction of around 35% is observed.

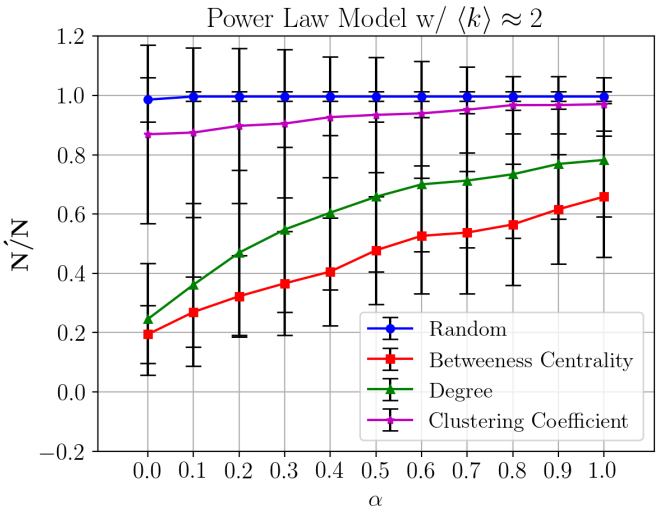

Fig. 1. Ratio of the final and initial largest components' sizes as defined in (3) as a function of the tolerance parameter α, to four different criteria for the selection of the trigger node. These results were obtained by, for each value of α, averaging over 10 different networks with 5 triggers each. The error bars represent the standard deviation of every set of data. For the targeted attacks, the 5 triggers are the 5 nodes with the highest value in each of the criteria. In the case of random breakdowns, the triggers are chosen at random. Each network has $\gamma = 3$, $1.985 < \langle k \rangle < 2.015$ and $4950 < N < 5050$.

These results are in accordance with intuition: random breakdowns are more likely to affect nodes that carry a small load, since these are the most numerous in the network, and their removal won't have any effect on the remaining network. In contrast, nodes with a high degree and betweenness centrality are likely to carry large loads that need to be diverted when these are attacked, overloading other nodes in the network. The similarity observed for these two criteria is understandable, since nodes with a higher degree (hubs) tend to also have a high betweenness centrality.

The damage is also larger for lower tolerance values. For $\alpha = 0$, the size of the final largest connected component for degree and load-based attacks is reduced to about 20%. This means that, for a network with 5000 nodes, ~ 3000 either shut down or get disconnected after an attack to a single node.

These results are also in line with the findings in [1], validating our algorithm.

We also study the effect of clustering coefficient based attacks. From figure 1 we conclude that the considered network model is quite robust to such attacks. Even for a tolerance value of $\alpha = 0$, about 90% of the network remains connected following the attack. Usually, the nodes with a higher clustering coefficient are those that have few neighbours, all connected in-between themselves. So, these nodes will carry close to no load, since their neighbours can use each other to traverse their loads. It is, then, expected for attacks based on this metric to have little to no effect on the network.

B. Power Law Model with $\langle k \rangle \approx 4$

The average degree was increased to 4 to analyze its impact on the robustness of networks generated with the same model.

From figure 2 we can infer that, in general, an increase in the average degree results in a more robust network.

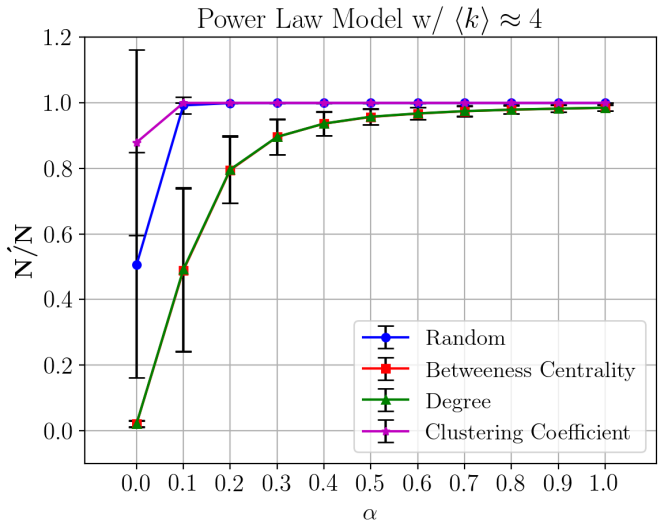

Fig. 2. Ratio of the final and initial largest components' sizes as defined in (3) as a function of the tolerance parameter α, to four different criteria for the selection of the trigger node. These results were obtained by, for each value of α, averaging over 10 different networks and 5 triggers each. The error bars represent the standard deviation for every set of data. The triggers are chosen in the same way as described in figure 1. Each network has $\gamma = 3$, $3.985 < \langle k \rangle < 4.015$ and $4950 < N < 5050$.

In fact, for $\alpha \geq 0.2$, more than 80% of the network remains connected even after a targeted attack. Intuitively, a network with a higher average degree will have more connections and, therefore, more redundant paths between nodes that can share load. The curves for attacks based on the node's degree and load overlap, since the nodes with the highest degree are also the ones with the highest loads (this claim was confirmed via the network visualization tool, GEPHI).

We also studied the existence of cascading failures in a scale-free network generated from a Barabási-Albert model with average degree $\langle k \rangle \approx 4$. The results and conclusions are the same as for the power law model, so they are omitted, for brevity.

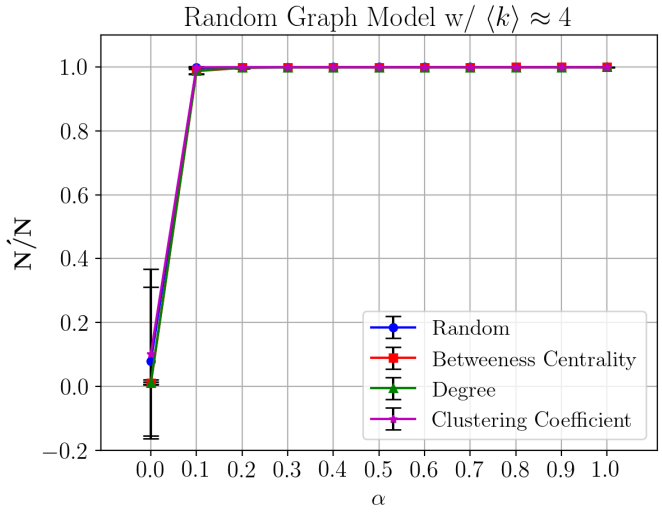

Fig. 3. Ratio of the final and initial largest components' sizes as defined in (3) as a function of the tolerance parameter α, to four different criteria for the selection of trigger node. These results were obtained as in figure 1. The error bars are as defined in figure 1 and the triggers are chosen in that same way. Each network has $3.985 < \langle k \rangle < 4.015$ and $4950 < N < 5050$ and was obtained with a Erdos-Rényi Model.

C. Random Graph with $\langle k \rangle \approx 4$

The same procedure was repeated for a homogeneous network, a random graph generated from an Erdos-Rényi model. It is clear from figure 3 that a homogeneous network is overall more robust either to random breakdowns as well as target attacks, independently of the criteria. The vulnerability of some real-world networks is due to their heterogeneity, which is also associated with a heterogeneous distribution of loads.

D. DMS Minimal Model with $\langle k \rangle \approx 4$

We also studied whether a network with nodes with a high clustering coefficient is more robust to cascades of failures. To make a fair comparison, a scale-free network was generated from the DMS Minimal model, which allows for networks with a heterogeneous distribution of clustering coefficients and with a high global clustering coefficient. It has the same degree distribution as in (2) and a naturally occurring average degree $\langle k \rangle = 4$.

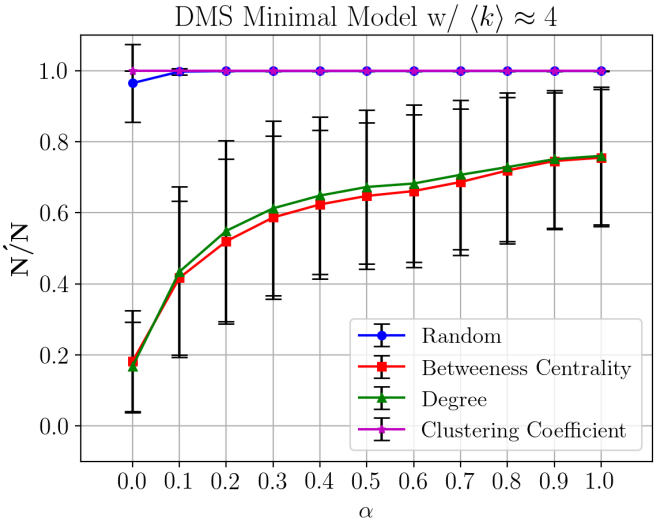

Fig. 4. Ratio of the final and initial largest components' sizes as defined in (3) as a function of the tolerance parameter α, to four different criteria for the selection of the trigger node. The results were obtained in the same way as in figure 1. The error bars represent the standard deviation for every set of data. The triggers are chosen in the same way as described in figure 1. Each network has $\gamma = 3$, $k \approx 4$, $N = 5000$ and was generated from a DMS Minimal model.

From figure 4 we can see that, for random breakdowns, this model of the network is as robust, if not, even more, than a simple power law network. However, for degree and load-based target attacks, the opposite effect seems to occur. Apart from when $\alpha = 0$, the final component is always smaller than that of a simple power law network. Even for $\alpha = 1$, more than 20% of the network gets disconnected after a targeted attack.

So, a network with a high clustering coefficient seems to be less robust to target attacks than a regular power law network, with the same scale-free distribution and average degree. This is somewhat counter-intuitive since a higher clustering coefficient is the resultant of a bigger interconnection between neighbouring nodes, which should add to network robustness.

E. Other robustness metrics

Now let's imagine the following scenario: if we have two same-sized communities linked by only one node that is attacked, the size of the network's giant component decreases by half

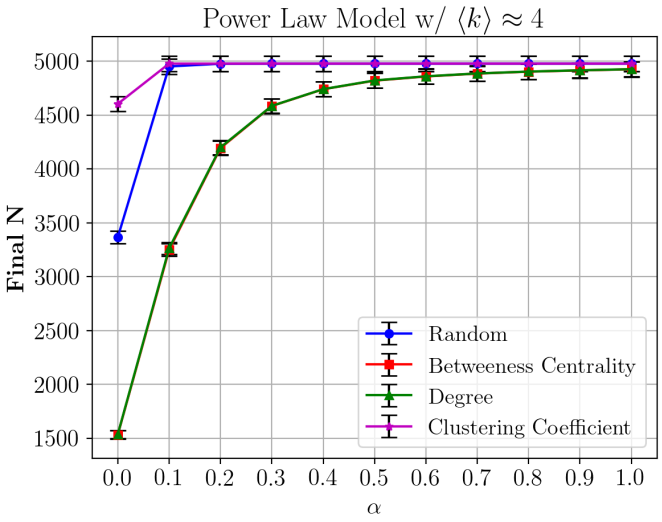

Fig. 5. Number of nodes in the network after the application of algorithm 1 for four different criteria for the selection of trigger node. These results were obtained using 10 networks and averaging over 5 iterations for each value of α where each network has $\gamma = 3$, $3.985 < \langle k \rangle < 4.015$ and $4950 < N < 5050$.

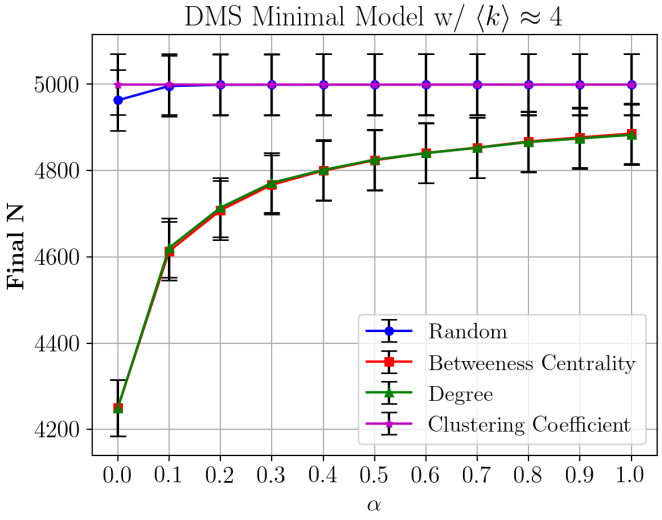

Fig. 6. Number of nodes in the network after the application of algorithm 1 for four different criteria for the selection of trigger node. These results were obtained using 10 networks and averaging over 5 iterations for each value of α where each network has $\gamma = 3$, $\langle k \rangle \approx 4$ and $N = 5000$.

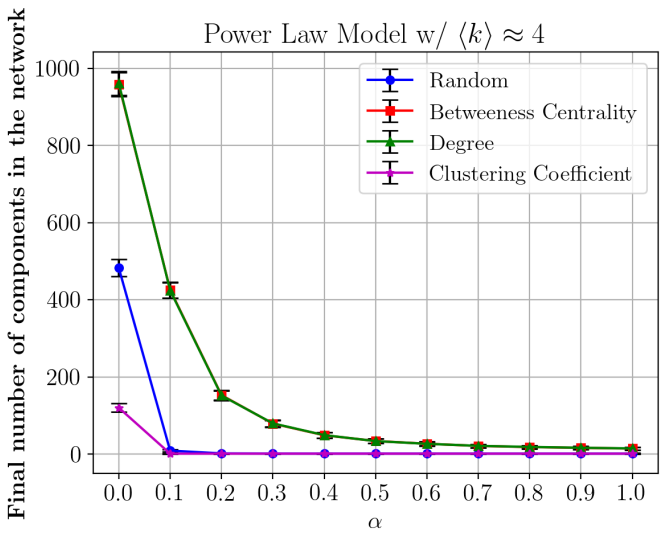

Fig. 7. Number of components in the network after the application of algorithm 1 for four different criteria for the selection of the trigger node. These results were obtained using 10 networks and averaging over 5 iterations for each value of α where each network has $\gamma = 3$, $3.985 < \langle k \rangle < 4.015$ and $4950 < N < 5050$.

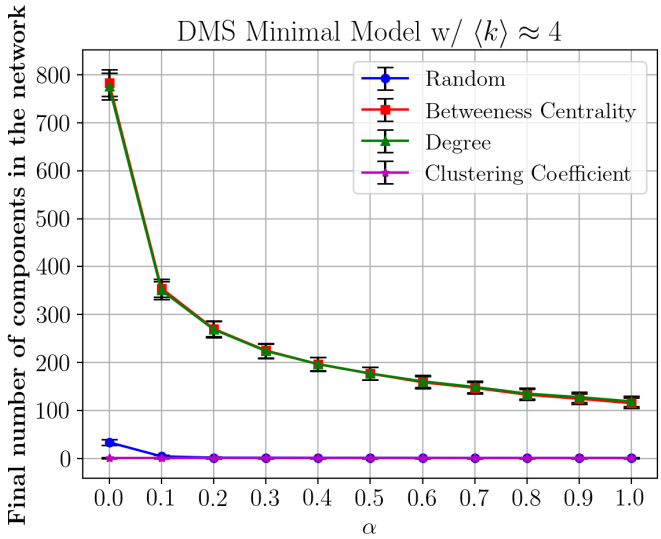

Fig. 8. Number of components in the network after the application of algorithm 1 for four different criteria for the selection of the trigger node. These results were obtained using 10 networks and averaging over 5 iterations for each value of α where each network has $\gamma = 3$, $\langle k \rangle \approx 4$ and $N = 5000$.

but the amount of nodes removed is minimal. We are linking robustness with the size of the giant component of the network but, depending on the shape of the network, other robustness metrics might be more adequate. So we will also look at the number of nodes, the number of connected components and the fraction of unconnected nodes after the cascading failures.

We will use these metrics to further compare a scale-free network with a high (global) clustering coefficient (DMS model) with one with a lower (global) clustering coefficient (power law model), and we will focus our analysis on degree and load-based attacks.

We start with the analysis of the final number of nodes in the network, presented in figures 5 and 6, for the power law and DMS models, respectively. From these, we can see that, for both models, for $\alpha \geq 0.3$, 90% of the networks' nodes outlast the cascading failures. Notice that, for the same α range, for the power law model, the G ratios (figure 2) are also in the same percentage values, hinting that most nodes remain in the giant component. For smaller values of α, the final number of nodes is significantly bigger for the DMS model: more than 80% of the nodes remain active, even for a tolerance value of 0.

This more recent analysis leads to an opposite conclusion to the one we had before. Although the power law model has fewer nodes in the final network than the DMS model, they remain in one big component. To verify this idea, we studied the final number of connected components in the network together with the number of unconnected pairs of nodes, since they are intimately related (nodes in different connected components are unconnected). The results for both models are present in figures 7, 8, 9 and 10. The conclusions obtained from both metrics are the same so we will focus on the number of connected components.

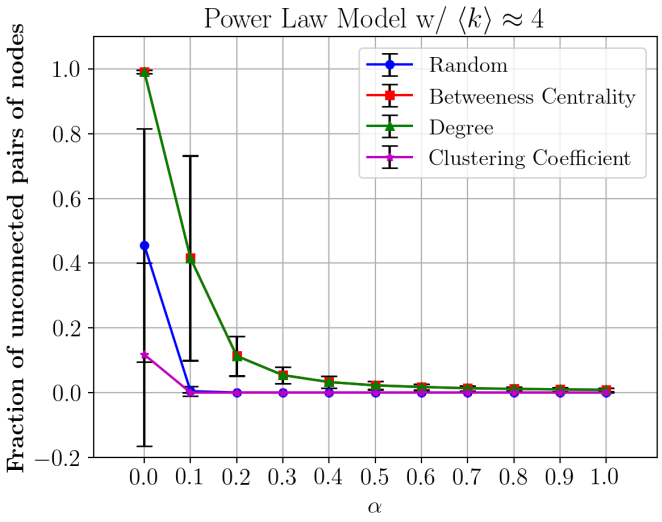

Fig. 9. Ratio of unconnected pairs in the network after the application of algorithm 1 for four different criteria for the selection of the trigger node. These results were obtained using 10 networks and averaging over 5 iterations for each value of α where each network has $\gamma = 3$, $3.985 < \langle k \rangle < 4.015$ and $4950 < N < 5050$.

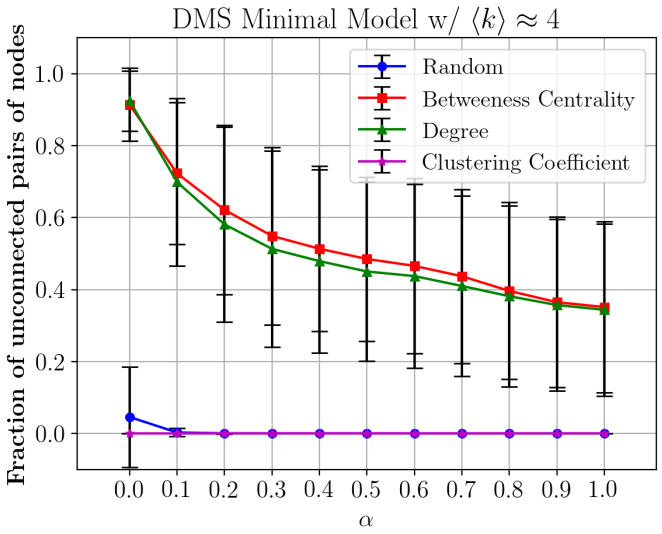

Fig. 10. Ratio of unconnected pairs in the network after the application of algorithm 1 for four different criteria for the selection of the trigger node. These results were obtained using 10 networks and averaging over 5 iterations for each value of α where each network has $\gamma = 3$, $\langle k \rangle \approx 4$ and $N = 5000$.

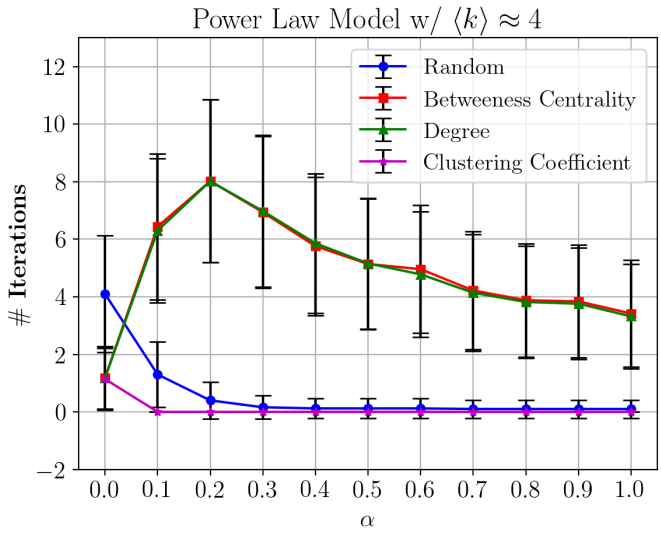

Fig. 11. Number of iterations of the main loop (lines 4 to 16) of algorithm 1 for the trigger node selection criteria of the highest betweenness centrality as a function of alpha. These results were obtained using 10 networks and averaging over 5 iterations for each value of α where each network has $\gamma = 3$, $3.985 < \langle k \rangle < 4.015$ and $4950 < N < 5050$.

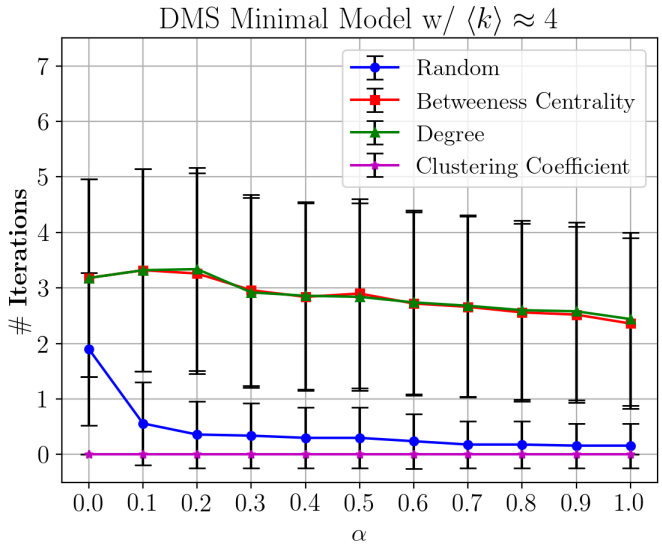

Fig. 12. Number of iterations of the main loop (lines 4 to 16) of algorithm 1 for the trigger node selection criteria of the highest betweenness centrality as a function of alpha. These results were obtained using 10 networks and averaging over 5 iterations for each value of α where each network has $\gamma = 3$, $\langle k \rangle \approx 4$ and $N = 5000$.

For the DMS model, the final number of components (figure 8) is, in general, greater than in the power law model (figure 7), meaning that the nodes' failures result in the breakdown of the network into several components. That's why the size of the giant component has a bigger decrease when compared with the power law model, even though the final number of nodes remains high.

The analysis of all of these robustness metrics together gives us more insight into what exactly is happening during the cascading failures. For the power law model, the deleted nodes are taken from the giant component, making it decrease in size, but the network is not separated into several large components (except for $\alpha = 0$, where the network is completely dismantled and the remaining nodes are alone or connected in very small groups). For the DMS model, the removed nodes break the network into several large pieces, due to this model's higher clustering coefficient - the nodes form connected groups that are more resilient towards attacks, due to the characteristically high redundancy in links observed in smaller components.

With the formation of these components, the propagation of the failures is halted faster. To corroborate this last affirmation, we will now investigate how the number of iterations of algorithm 1 is related with the tolerance parameter using figures 11 and 12.

F. Cascading length

It can be seen in figure 11 that, for random breakdowns and clustering coefficient based attacks, the number of iterations is, on average, smaller than one, that is, there is almost no cascade effect, in agreement with previous conclusions. The targeted attacks using the highest degree and betweenness centrality behave

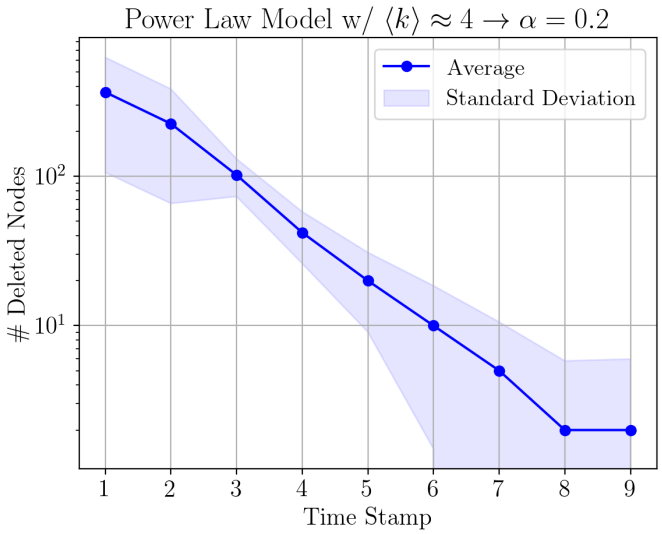

Fig. 13. Number of deleted nodes in each iteration of the main loop of algorithm 1. Note that iteration 0 is not shown in the plot since it only contains the trigger node (chosen with the highest betweenness centrality criteria). These results were obtained using 10 networks and averaging over 5 iterations for $\alpha = 0.2$ where each network has $\gamma = 3$, $3.985 < \langle k \rangle < 4.015$ and $4950 < N < 5050$.

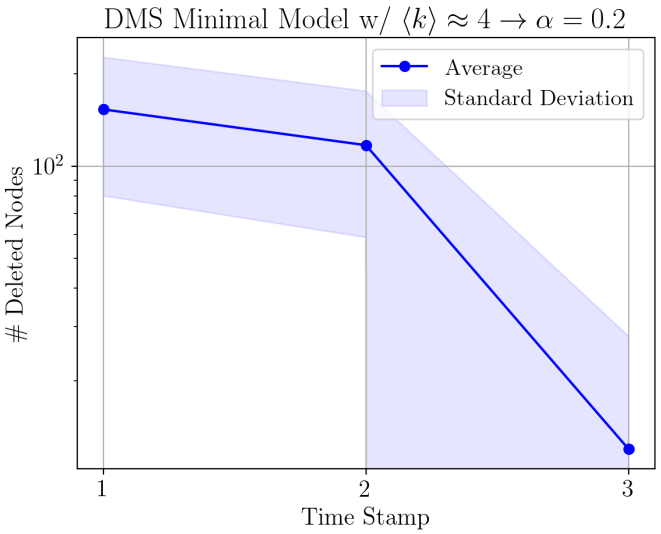

Fig. 14. Number of deleted nodes in each iteration of the main loop of algorithm 1. Note that iteration 0 is not shown in the plot since it only contains the trigger node (chosen with the highest betweenness centrality criteria). These results were obtained using 10 networks and averaging over 5 iterations for $\alpha = 0.2$ where each network has $\gamma = 3$, $\langle k \rangle \approx 4$ and $N = 5000$.

differently. For low α, the number of iterations is very low but, as we observed before, the effects in the network are the largest. This means that in just a few iterations the network completely breaks apart. When α increases slightly, the number of iteration also increases, showing a bigger propagation of the cascading effect throughout the network, until a peak is attained in $\alpha = 0.2$. For this value, thought figure 13, we can see that the number of affected nodes also decreases exponentially with each iteration. Increasing the tolerance past the peak number of iterations, the cascade effect gets shorter in time, since the network becomes more robust, interrupting the propagation of nodes' failures. The behaviour following these two targeted attacks is much simpler for the DMS model networks (figure 12), where the average number of iterations is almost constant with α, decreasing slightly as the tolerance increases. This value is, in general, smaller than for the power law model (the only exception being $\alpha = 0$). The amount of nodes removed per iteration is also fairly low, as it can be observed in figure 14. For random breakdowns and clustering coefficient based attacks the pattern is the same as in the power law model.

G. Real-World Networks

Finally, we decided to apply algorithm 1 to two real-world networks to try to understand which features in each make them more or less resilient to attacks and what models might be more accurate to describe them. As real-world networks tend to be heterogeneous, it is expected that the two networks behave in a similar way to the previously discussed scale-free models.

1) Internet: The first real-world network is the Internet at the level of autonomous systems [5]. It has a degree distribution according to that of (2) - see figure 18 in Appendix - and an average degree of approximately 4.

As it can be seen by figure 15, this network exhibits very similar behaviour to the power law model networks in section III-B and as theorized above: it is very robust to random breakdowns and clustering coefficient based attacks, but attacks targeting nodes

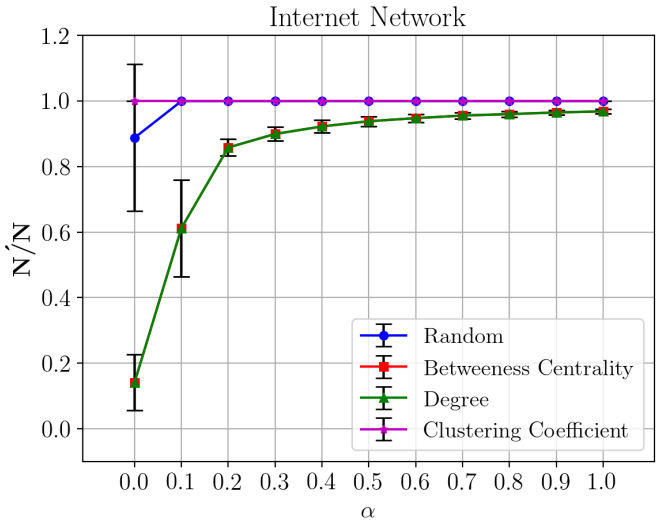

Fig. 15. Ratio of the final and initial largest components' sizes as defined in (3) as a function of the tolerance parameter α, to four different criteria for the selection of the trigger node. These results were obtained by, for each value of α, averaging over 5 triggers. The error bars represent the standard deviation for every set of data. For the targeted attacks, the 5 triggers are the 5 nodes with the highest value for each of the criteria. In the case of random breakdowns, the triggers are chosen at random. The network has $\langle k \rangle \approx 4.22$ and $N = 22963$.

with higher load and degree are more damaging, especially for lower tolerance values.

2) Power Grid: The second real-world network is the western US power grid [4]. This network has an exponential degree distribution - see figure 19 in Appendix - which is relatively homogeneous.

The loads' distribution, however, is still fairly heterogeneous. This results in the fact that load-based attacks can trigger cascading effects in the network - over 50% of the network's largest component gets disconnected, even for the higher value of α.

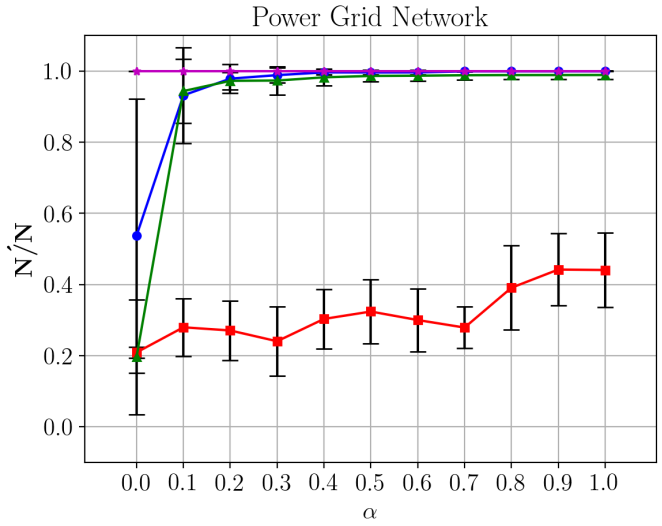

Fig. 16. Ratio of the final and initial largest components' sizes as defined in (3) as a function of the tolerance parameter α, to four different criteria for the selection of the trigger node (the curves for each criterion are according to the legend of (3)). These results were obtained by, for each value of α, averaging over 5 triggers. The error bars represent the standard deviation for every set of data. For the targeted attacks, the 5 triggers are the 5 nodes with the highest value for each of the criteria. In the case of random breakdowns, the triggers are chosen at random. The network has $\langle k \rangle \approx 2.67$ and $N = 4941$.

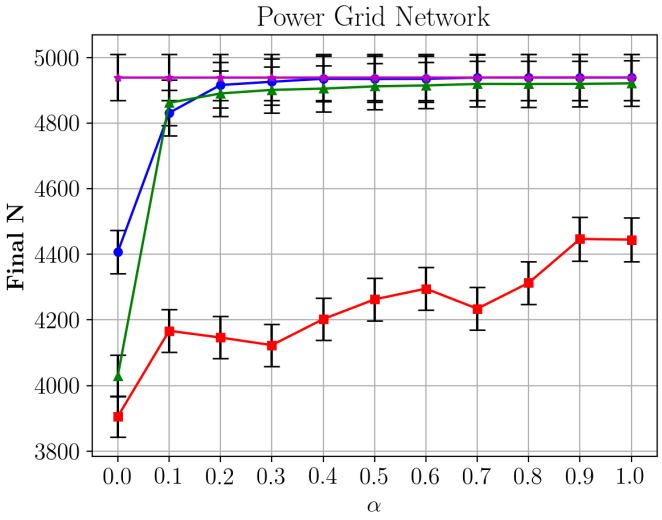

Fig. 17. Number of nodes in the network after the application of algorithm 1 for four different criteria for the selection of trigger node (the curves for each criterion are according to the legend of (3)). The network has $\langle k \rangle \approx 2.67$ and $N = 4941$.

But, analogous to the analysis with the DMS model, although the giant component gets severely diminished, this might not mean that the nodes not belonging to it were removed. It is deducible from figure 17 that the number of final nodes in the network remains between 79% and 89% for this kind of attack.

For both random breakdowns and degree-based attacks, however, the network appears very robust, seeing that these types of attacks culminated in similar behaviour to that of a random network as described in section III-C.

IV. Conclusion

Scale-free networks are, in general, robust to random breakdowns but targeted attacks may yield devastating consequences to their connectivity. This is mainly due to their heterogeneity, either in the distribution of degree or in the distribution of loads, since these effects were not observed on homogeneous networks like random graphs. The latter are highly robust either to random breakdowns or targeted attacks. The former type of network is the most susceptible to attacks targeting nodes with high loads. Degree based attacks may also be devastating, since, for this type of network, nodes with a higher degree tend to also have higher loads. Attacks based on other criteria, like the clustering coefficient, usually have no effects on the network. Real-world networks tend to also be highly heterogeneous, and many are scale-free. So, the conclusions for these networks are the same: random breakdowns have no noticeable effect, but target attacks can cripple the entire network, as it was observed for the Internet. Some networks, however, have some characteristics that may not be fully captured by any of the studied models, like the Power Grid. Nonetheless, our conclusions also apply: robustness to random breakdowns is still high; robustness to degree-based attacks is also high, due to the fairly homogeneous degree distribution (exponential); robustness to load-based attacks is still low, due to the highly heterogeneous distribution of loads, as in a scale-free network.

Depending on the robustness metric chosen, one may consider one type of network more resilient than the other. A network following a DMS model might be preferred when (i) the focus of robustness is the number of nodes that remain unaffected resulting in an attack - if we don't care as much for broken connections as for nodes that go offline and the few removed nodes ate the ones that separate the network into several communities, connecting them again is simple if links between communities are cheap and easily deploy-able - or (ii) there are severe cost limitations that don't allow for a node's capacity to be much larger than its load (small α). A simple power law with a smaller clustering coefficient seems to do better if (i) it is preferred that the network remains connected in one big component or (ii) it can be allowed to have higher capacities values.

Even though a higher average degree makes a network more robust to targeted attacks, in a real-world network, like the power grid, the number of links may be limited by cost. Nonetheless, it would be interesting to see if this conclusion would remain for bigger average degrees since we only studied this effect for average degrees of $\langle k \rangle \in \{2, 4\}$. Intuition says so, but it could also be the case that the added links would allow for the formation of smaller communities, similarly to the DMS model. This study is left for future work.

We also leave for future work the study of cascading effects in scale-free networks with well-defined communities, more specifically if a network with this topology is more or less robust than the ones considered here.

APPENDIX

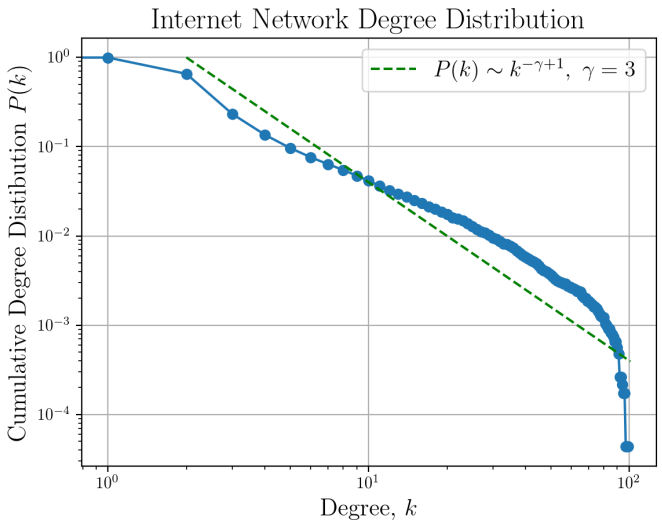

Fig. 18. Cumulative degree distribution of the internet at the level of autonomous systems, with $N = 22963$ and $\langle k \rangle \approx 4.22$. The dashed, green, line is the expected slope for the cumulative degree distribution of a network whose degree distribution follows (2), with $\gamma = 3$. It can be seen that this network is, in fact, scale-free. A *cutoff* for higher degrees can be observed, characteristic of real-world, finite, networks. The maximum presented degree is 100 but there are nodes in the network with a higher degree, which also shows the heterogeneity of the network.

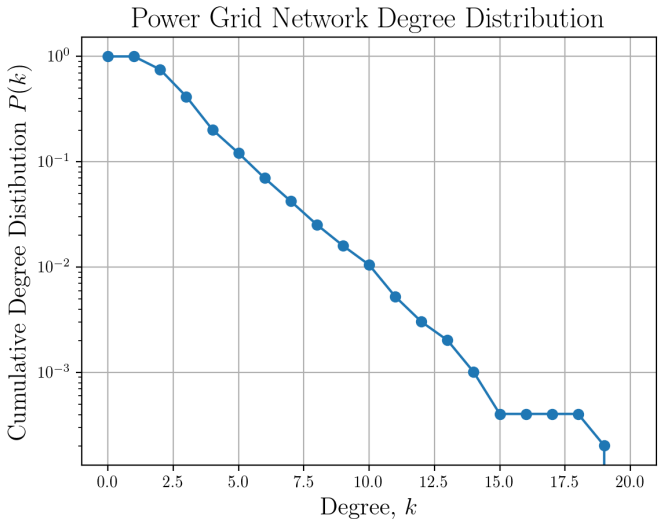

Fig. 19. Cumulative degree distribution for the western US power grid network, with $N = 4941$ and $\langle k \rangle \approx 2.67$. The degree axis is in linear scale while the $P(k)$ axis is in logarithmic scale. The fact that the degree distribution forms an almost straight line hints towards a more exponential degree distribution, which is a relatively homogeneous distribution. The fact that the maximum degree of the network is 19 also shows said homogeneity.

REFERENCES

[1] Motter, Adilson E. and Lai, Ying-Cheng (2002). "Cascade-based attacks on complex networks"

[2] igraph C library - `https://igraph.org/c/`

[3] NetworkX - `https://networkx.org`

[4] Western US Power Drig Network Data - `https://icon.colorado.edu/#!/networks`

[5] Internet Network Data - `http://www-personal.umich.edu/~mejn/netdata/`

[6] Developed Code - `https://drive.google.com/drive/folders/1Krc-8Oac-pMx3ynFqlVogAp9VDoo1zu_?usp=sharing`