Miuz: measuring the impact of disconnecting a node

Ivana Bachmann, Patricio Reyes, Alonso Silva, Javier Bustos-Jiménez

Miuz: measuring the impact of disconnecting a node

Ivana Bachmann [*1], Patricio Reyes [†2], Alonso Silva [‡3], and Javier Bustos-Jiménez [§4]

[1,4]NICLabs, Computer Science Department (DCC), Universidad de Chile, Chile
[2]Technological Institute for Industrial Mathematics (ITMATI), Santiago de Compostela, Spain
[3]Nokia Bell Labs, Centre de Villarceaux, Route de Villejust, 91620 Nozay, France

Abstract

In this article we present *Miuz*, a robustness index for complex networks. *Miuz* measures the impact of disconnecting a node from the network while comparing the sizes of the remaining connected components. Strictly speaking, *Miuz* for a node is defined as the inverse of the size of the largest connected component divided by the sum of the sizes of the remaining ones.

We tested our index in attack strategies where the nodes are disconnected in decreasing order of a specified metric. We considered *Miuz* and other well-known centrality measures such as betweenness, degree, and harmonic centrality. All of these metrics were compared regarding the behavior of the robustness (R-index) during the attacks. In an attempt to simulate the internet backbone, the attacks were performed in complex networks with power-law degree distributions (scale-free networks).

Preliminary results show that attacks based on disconnecting a few number of nodes *Miuz* are more dangerous (decreasing the robustness) than the same attacks based on other centrality measures. We believe that *Miuz*, as well as other measures based on the size of the largest connected component, provides a good addition to other robustness metrics for complex networks.

*Email: ivana@niclabs.cl To whom correspondence should be addressed.
†Email: preyes@usc.es
‡Email: alonso.silva@nokia-bell-labs.com
§Email: jbustos@niclabs.cl

1 Introduction

Networks are present in human life in multiple forms from social networks to communication networks (such as the Internet), and they have been widely studied as complex networks of nodes and relationships, describing their structure, relations, etc. Nowadays, the studies go deep into network knowledge, and using standard network metrics such as degree distribution and diameter one can determine how robust and/or resilient a network is.

Even though both terms (robustness and resilience) have been used with the same meaning, we will consider *robustness* as the network inner capacity to resist failures, and *resilience* as the ability of a network to resist and recover after such failures. However, both terms have in common the methodology for testing robustness and/or resilience. Usually, they consist on planned attacks against nodes failures or disconnections, from a random set of failures to more elaborated strategies using well known network metrics.

We consider that an "adversary" should plan a greedy strategy aiming to maximize damage with the minimum number of strikes. Under this new philosophy of "adversary", we first present a new network

impact metric called *Miuz*, which is the inverse of the size of the largest connected component, divided by the sum of the sizes of the remaining ones. Then, we plan a greedy strategy based on recalculating the network *Miuz-ness* after each node disconnection. We discuss the performance of attacks based on *Miuz* and other centrality measures[1] (in particular, betweenness, degree, harmonic), compared by the robustness index (*R*-index). Our main conclusion is that the first strikes of a *Miuz* strategy causes more "*damage*" than the classical betweenness, degree, and harmonic metrics.

The article is organized as follows, next section presents related work, followed by the definition of *Miuz*, its attacking strategy, and its simulation results in section 3. Discussions about the main results and conclusions are presented in sections 4 and 5 respectively.

2 Related Work

Over the last decade, there has been a huge interest in the analysis of complex networks and their connectivity properties [2]. During the last years, networks and in particular social networks have gained significant popularity. An in-depth understanding of the graph structure is key to convert data into information. To do so, complex networks tools have emerged [3] to classify networks [4], detect communities [5], determine important features and measure them [1].

The idea of planning a "network attack" using centrality measures has been catching the attention of researchers and practitioners nowadays. For instance, Sterbenz et al. [6] used betweenness-centrality (*bcen*) for planning a network attack, calculating the *bcen* value for all nodes, ordering nodes from higher to lower *bcen*, and then attacking (discarding) those nodes in that order. They have shown that disconnecting only two of the top *bcen*-ranked nodes , their packet-delivery ratio is reduced to 60%, which corresponds to 20% more damage than other attacks such as random links or nodes disconnections, tracked by link-centrality and by node degrees.

A similar approach and results were presented by Çetinkaya et al. [7]. They show that after disconnecting only 10 nodes the packet-delivery ratio is reduced to 0%. Another approach, presented as an improved network attack [8, 9], is to recalculate the betweenness-centrality after the removal of each node [10, 11]. They show a similar impact of non-recalculating strategies but discarding sometimes only half of the equivalent nodes.

Concerning centrality measures, betweenness centrality deserves special attention. Betweenness has been studied as a resilience metric for the routing layer [12] and also as a robustness metric for complex networks [13] and for internet autonomous systems networks [14] among others.

3 Miuz Attacking Strategy

Given a network $\mathcal{N}$ of size N, we denote by $\mathcal{C}(\mathcal{N} \setminus n)$ the set of connected components in $\mathcal{N}$ after disconnecting node n. The *Miuz* index for a node n in $\mathcal{N}$ is defined as follows:

$$Miuz_{\mathcal{N}}(n) = \begin{cases} \frac{\sum_{c \in \mathcal{C}(\mathcal{N} \setminus n)} \|c\|}{max_{c \in \mathcal{C}(\mathcal{N} \setminus n)} \|c\|} - 1, \textit{ if } \|\mathcal{C}(\mathcal{N} \setminus n)\| \neq \|\mathcal{C}(\mathcal{N})\| + 1 \\ 0 \qquad\qquad\qquad\qquad \textit{otherwise} \end{cases} \tag{1}$$

where $\|c\|$, with $c \in \mathcal{C}(\mathcal{N} \setminus n)$, is the size of the connected component c of the network $\mathcal{N}$ after disconnecting node n (if connected, i.e. if there is an edge between node n and another node of the network). Notice that $Miuz_{\mathcal{N}}$(n) reflects the partition of a network in several sub-networks after the disconnection of node n and how these sub-networks remain interconnected. Strictly speaking, it compares in size the core network (the largest connected component) with the other remaining sub-networks. $Miuz_{\mathcal{N}}$ takes values between 0 (the whole network remains connected) to $N - 1$ (the whole network is disconnected). Figure 1 shows examples of three networks after disconnecting the node with either highest *Miuz*, degree, betweenness or harmonic centrality.

3.1 Network Attack Plan

If we plan a network attack by disconnecting nodes with a given strategy, it is widely accepted the use

of centrality measures (such as degree, betweenness, harmonic) because they reflect the importance of nodes in the network [13]. These attack strategies are compared by means of the *Unique Robustness Measure* (R-index) [15], defined as:

$$R = \frac{1}{N}\sum_{Q=1}^{N} s(Q), \tag{2}$$

where N is the number of nodes in the network and $s(Q)$ is the fraction of nodes in the largest connected component after removing Q nodes using a given strategy. Therefore, the higher the R-index, the better in terms of robustness. Our strategy is:

In each step, (re)compute the Miuz index for all the nodes and disconnect the node with the highest Miuz value.

Degree centrality is a simple, easy-to-compute local (myopic) metric. Despite its simplicity, it is the preferred metric for certain literature [13] under this kind of attacks. Basically, it ranks nodes in terms of their degree (number of edges or connections to other nodes). Betweenness centrality ranks nodes by the number of shortest paths passing throw them. Unlike degree, betweenness centrality is not a local (myopic) metric. It determines the importance of a node by looking at the paths between all of the pairs of remaining nodes. The harmonic centrality is a metric related to the distances to the remaining nodes. It is the sum of the reciprocal of distances to other nodes (with the convention of $1/\infty = 0$, used when two nodes are not connected by any path). This metric was widely studied in [16], mainly because of its good mathematical properties.

For a better understanding of network attacks and strategies, see [10, 11, 8, 9].

3.2 Simulations

In an attempt to study the behavior of the internet backbone, we test our strategy in simulated scale-free networks (it means, with power-law degree distributions, that is *dist(deg)* $\propto x^{-\alpha}$) with exponents $\alpha \in \{2.10, 2.15, 2.20, 2.25, 2.30\}$. For each α, we simulate 50 networks of size 1000 (i.e., with 1000 nodes). Then, we tested and compared strategies ranked with a multitude of centrality measures [1] in terms of the R-index. However, apart from *Miuz*, for this article we selected and reported the results for degree, betweenness and harmonic centrality.

Instead of just compare the robustness, after the removal of all of the nodes, we studied the behavior of the attacks after the only a few strikes. To do so, we define a variant of the R-index which takes into account only the first n strikes of an attack. Thus, for a simultaneous attack (where the nodes are ranked by a metric only once at the beginning), the R_a-index is defined as:

$$R_a = \frac{1}{a}\sum_{Q=1}^{a} s(Q). \tag{3}$$

For a sequential attack, the order of node disconnection is recomputed after each disconnection. Similar to the R-index, notice that the lower the R_a-index, the more effective the attack is, since that gives us a higher reduction of robustness.

Results are shown in Table 1. We tested sequential attacks: At each strike, the next node to disconnect was the one with the highest metric (whether it be *Miuz*, Degree, Betweenness or Harmonic centrality) in the current network. The table shows the behavior of the R_a-index as well as the R-index in 50 scale-free networks (generated as before) with exponent 2.1, 2.2 and 2.3. For each group of networks, we compute the R_a-index for $a \in \{5, 10, 20, 30\}$, it means, the variant of R-index after the first $5, 10, 20$ and 30 node disconnections. *Miuz* proves to be very effective in attacks with only a few disconnections. Moreover, *Miuz* shows that the effectiveness persists over the number of strikes in scale-free networks with lower exponent.

It is interesting to note that, no matter the metric used, the damage decreases in the long term with the number of strikes. Indeed, if we consider a complete attack, disconnecting all the nodes of the network, the R-index shows that an attack based on Harmonic centrality performs better. A comparison of the R-index is shown in Table 2. It is important to notice that R-index is a metric for a general view of robust-

ness, and it gives no information of how fast the network is disconnected (further details in Section 4.1).

4 Discussion

We start analyzing what would be the worst "attack". In the worst case, a "*malicious adversary*" will try to perform the maximum damage with the minimum number of strikes, that is, with the minimum number of node disconnections (made by the attacker). In terms of decreasing the size of the largest connected component, *Miuz* is the best attack strategy during the first strikes. It achieves the disconnection of more than half of the network only after nine strikes for $\alpha = 2.10$ and after five strikes for $\alpha = 2.30$ (see Fig. 2).

It is important to notice that there is a breaking point where *Miuz* is no longer the best attacking strategy (Fig. 3). This breaking point occurs with less strikes as the exponent of the scale-free network increases. Nevertheless, as shown in Fig. 3, this breaking point appears after the largest connected component is less than 1/3 of the original network.

4.1 Is the R-index a good metric for robustness?

From the above discussion it is valid to question whether the R-index is a good measure of robustness. Maybe it is important to revisit the definition of network robustness:

"A measure of the decrease of network functionality under a sinister attack"[10]

Therefore, the R-index can be considered as a good robustness metric even though it does not reflect how fast the network is disconnected (as it is shown in Fig. **??**).

We suggest that weighted versions of the R-index could be a good compromise. This is the case of the R_a-index proposed in Section 3 which takes into account the removal of only a percentage of the best ranked nodes (or until the network reaches its percolation threshold [10]) could be a more useful metric for robustness and/or resilience in worst-case scenarios.

4.2 Revisiting Miuz

Concerning the attacking strategies, it is important to notice that *Miuz* strategy was designed for disconnecting the network from the first strikes, aiming to get connected components with similar sizes. This is the main reason of its better performance than centrality metrics in a worst-attack scenario. For instance, in Fig. 1 we present examples where the *Miuz* strategy performs better attacks than the ones with other centrality metrics. In subfigure a) Degree-based attack will select node 2 (up) while *Miuz* selects node 20 (down). In b) Betweenness-based attack will select node 21 while *Miuz* selects node 18. In c) Harmonic-based attack will select node 25 (left) while *Miuz* selects node 14 (right).

Another interesting property of *Miuz* occurs when $\max_n(Miuz_n(\mathcal{N})) = 0$. In other words, when *Miuz* is 0 for any node. In that case, the full network will remain connected no matter which node is disconnected. Therefore, we suggest a resilience metric as the number (or percentage) of disconnected nodes until $\max(Miuz_n(\mathcal{N})) > 0$, a pre-defined threshold, or the percolation threshold [10].

5 Conclusions and Future Work

In this article we have presented *Miuz*, a robustness index for complex networks defined as the inverse of the size of the remaining largest connected component divided by the sum of the sizes of the remaining connected components.

We tested our index as a measure to quantify the impact of node removal in terms of the network robustness metric R-index. We compared *Miuz* with other attacks based on well-known centrality measures (betweenness centrality, degree and harmonic) for node removal selection. The attack strategy used was sequential targeted attack, where every index is recalculated after each removal, and the highest one is selected for the next extraction.

Preliminary results show that *Miuz* performs better compared to attacks with classical centrality measures in terms of decreasing the network robustness

Table 1: Robustness against sequential attacks based on different metrics. Table shows mean R-index and mean R_a-index for scale-free networks with exponent 2.1, 2.2 and 2.3. R_a-index corresponds to the equivalent to R-index, but only disconnecting a nodes. Attacks based on harmonic centrality are more harmful in the long term. However attacks based on *Miuz* turns out to be more dangerous than the others with only a few strikes.

metric	Miuz	Degree	Betweenness	Harmonic
scale-free network with exponent 2.1				
R_5-index	**0.6976**	0.6987	0.6994	0.6999
R_{10}-index	**0.6068**	0.6092	0.6108	0.6118
R_{20}-index	**0.4929**	0.499	0.5032	0.5059
R_{30}-index	**0.4051**	0.4135	0.4092	0.4166
R-index	0.016	0.0155	0.015	**0.0146**
scale-free network with exponent 2.2				
R_5-index	**0.6867**	0.6886	0.6897	0.6903
R_{10}-index	**0.599**	0.6039	0.6078	0.6092
R_{20}-index	**0.4721**	0.4859	0.4841	0.4911
R_{30}-index	0.3602	0.3812	**0.3504**	0.3619
R-index	0.0142	0.0137	0.0129	**0.0125**
scale-free network with exponent 2.3				
R_5-index	**0.6601**	0.677	0.6708	0.6734
R_{10}-index	**0.5321**	0.5585	0.5449	0.5541
R_{20}-index	0.3551	0.3926	**0.3405**	0.3567
R_{30}-index	0.2586	0.2862	**0.2363**	0.2487
R-index	0.0123	0.1063	0.0094	**0.0091**

in the worst-attack scenario. Compared to other centrality measures, strategies based on *Miuz* are more dangerous (decreasing the robustness) in the first strikes of the attacks. We suggest that *Miuz*, as well as other measures based on the size of the largest connected component, provides a good addition to other robustness metrics for complex networks.

As future work, we can study improving through new connections an already existing network to make it more robust to attacks, and we can study networks in which the topological space is correlated with the cost of nodes disconnections, nodes which are nearby have a lower cost to be disconnected compared with nodes which are far apart.

References

[1] N. I. Bersano-Méndez, S. E. Schaeffer, and J. Bustos-Jiménez, "Metrics and models for social networks," in *Computational Social Networks*, pp. 115–142, Springer, 2012.

[2] R. Albert, H. Jeong, and A. Barabasi, "Error and attack tolerance of complex networks," *Nature*, vol. 406, pp. 378–82, July 2000.

[3] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks," *Reviews of Modern Physics*, vol. 74, pp. 47–97, Jan. 2002, 0106096.

[4] D. J. Watts and S. H. Strogatz, "Collective dynamics of 'small-world' networks.," *Nature*, vol. 393, pp. 440–2, June 1998.

α	Miuz	Degree	Betweenness	Harmonic
2.10	0.01603	0.01549	0.01496	**0.01460**
2.15	0.01575	0.01525	0.01430	**0.01400**
2.20	0.01421	0.01372	0.01287	**0.01249**
2.25	0.01384	0.01299	0.01874	**0.01150**
2.30	0.01232	0.010631	0.00942	**0.009094**

Table 2: Mean values of R-index for different disconnection strategies. The harmonic centrality strategy gets the lowest R-index values (in bold) for all of the tested exponents. (The higher the R-index, the better in terms of robustness).

[5] J. Leskovec, K. J. Lang, A. Dasgupta, and M. W. Mahoney, "Statistical properties of community structure in large social and information networks," *Proceeding of the 17th international conference on World Wide Web - WWW '08*, p. 695, 2008.

[6] J. P. Sterbenz, E. K. Cetinkaya, M. Hameed, A. Jabbar, J. P. Rohrer, *et al.*, "Modelling and analysis of network resilience," in *Communication Systems and Networks (COMSNETS), 2011 Third International Conference on*, pp. 1–10, IEEE, 2011.

[7] E. K. Çetinkaya, D. Broyles, A. Dandekar, S. Srinivasan, and J. P. Sterbenz, "Modelling communication network challenges for future internet resilience, survivability, and disruption tolerance: A simulation-based approach," *Telecommunication Systems*, vol. 52, no. 2, pp. 751–766, 2013.

[8] J. Rak and K. Walkowiak, "Survivability of anycast and unicast flows under attacks on networks," in *Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2010 International Congress on*, pp. 497–503, IEEE, 2010.

[9] A. Sydney, C. Scoglio, M. Youssef, and P. Schumm, "Characterising the robustness of complex networks," *International Journal of Internet Technology and Secured Transactions*, vol. 2, no. 3-4, pp. 291–320, 2010.

[10] P. Holme, B. J. Kim, C. N. Yoon, and S. K. Han, "Attack vulnerability of complex networks," *Physical Review E*, vol. 65, no. 5, p. 056109, 2002.

[11] W. Molisz and J. Rak, "End-to-end service survivability under attacks on networks," *Journal of Telecommunications and Information Technology*, pp. 19–26, 2006.

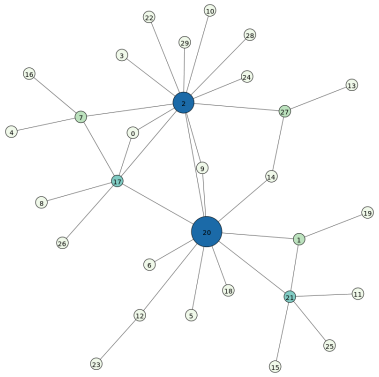
[12] P. Smith, D. Hutchison, J. P. Sterbenz, M. Scholler, A. Fessi, M. Karaliopoulos, C. Lac, and B. Plattner, "Network resilience: a systematic approach," *Communications Magazine, IEEE*, vol. 49, no. 7, pp. 88–97, 2011.

[13] S. Iyer, T. Killingback, B. Sundaram, and Z. Wang, "Attack robustness and centrality of complex networks," *PloS one*, vol. 8, no. 4, p. e59613, 2013.

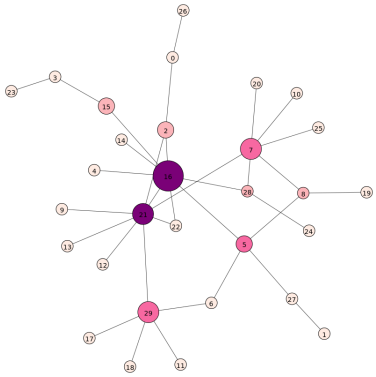
[14] P. Mahadevan, D. Krioukov, M. Fomenkov, X. Dimitropoulos, A. Vahdat, *et al.*, "The internet as-level topology: three data sources and one definitive metric," *ACM SIGCOMM Computer Communication Review*, vol. 36, no. 1, pp. 17–26, 2006.

[15] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin, and H. J. Herrmann, "Mitigation of malicious attacks on networks," *Proceedings of the National Academy of Sciences*, vol. 108, no. 10, pp. 3838–3841, 2011.

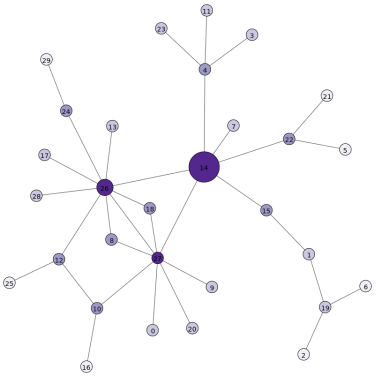
[16] P. Boldi and S. Vigna, "Axioms for Centrality," *Internet Mathematics*, vol. 10, pp. 222–262, Sept. 2014.



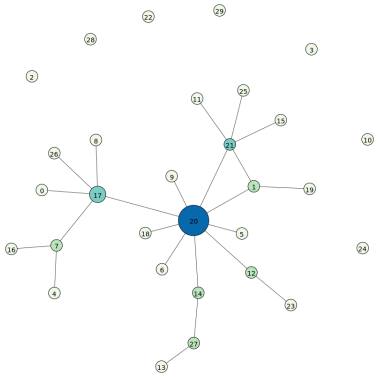
(a) Original network A, color coded by degree centrality



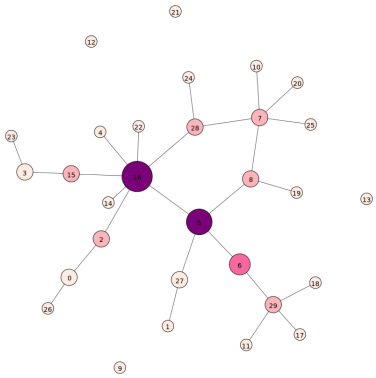
(b) Original network B, color coded by betweenness centrality



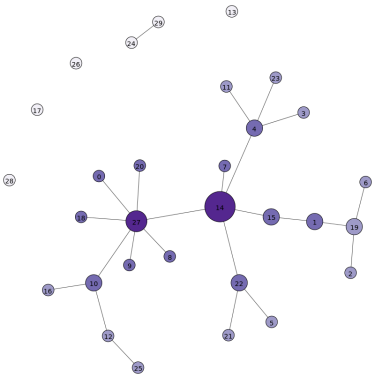
(c) Original network C, color coded by harmonic centrality



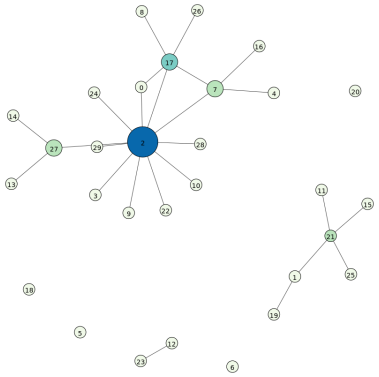
(d) Network A, after removal of node with highest degree centrality



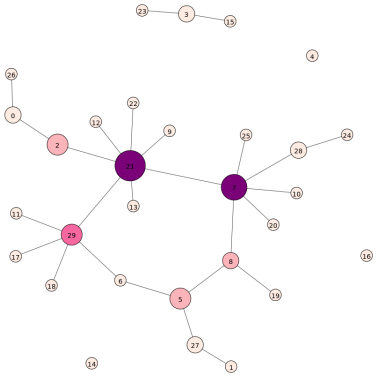
(e) Network B, after removal of node with highest betweenness centrality



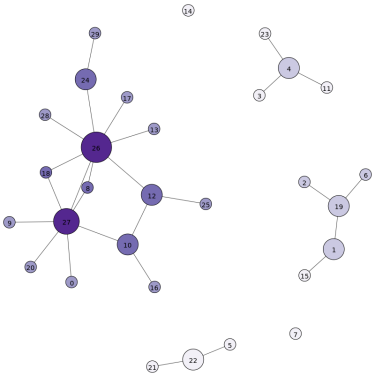
(f) Network C, after removal of node with highest harmonic centrality



(g) Network A, after removal of node with highest *Miuz*

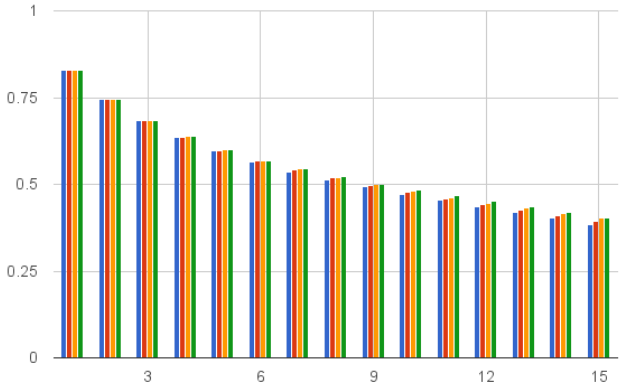


(h) Network B, after removal of node with highest *Miuz*

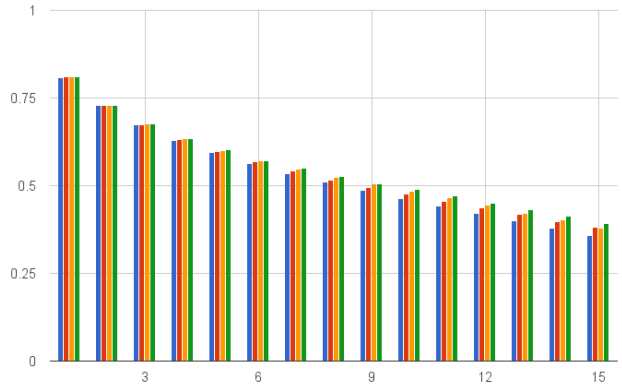


(i) Network C, after removal of node with highest *Miuz*

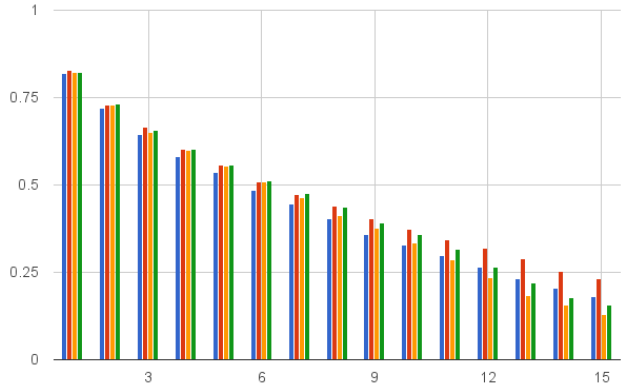
Figure 1: Effects of attacking strategies. The size shows the Miuz-ness and the color darkness reflects the centrality metric. Metrics were recalculated after node removal.



(a) $\alpha = 2.10$

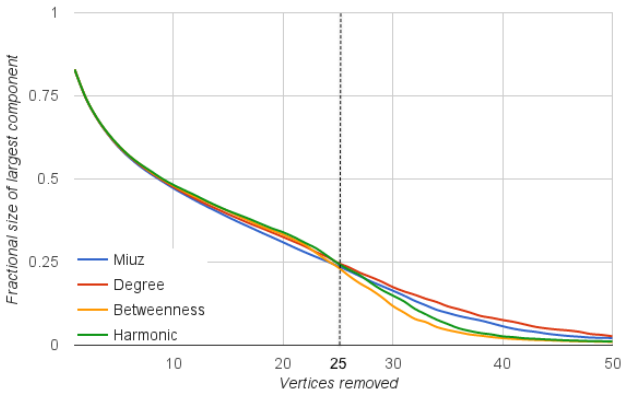


(b) $\alpha = 2.20$

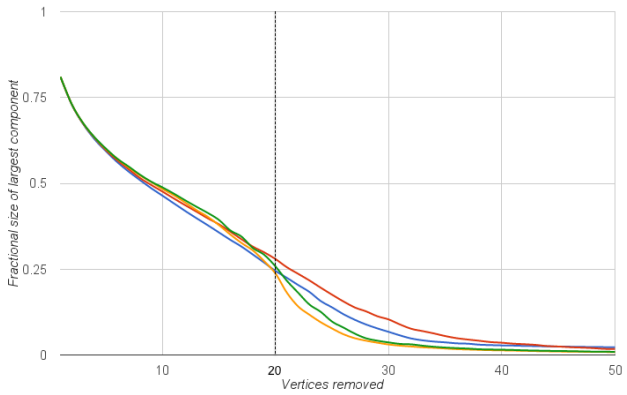


(c) $\alpha = 2.30$

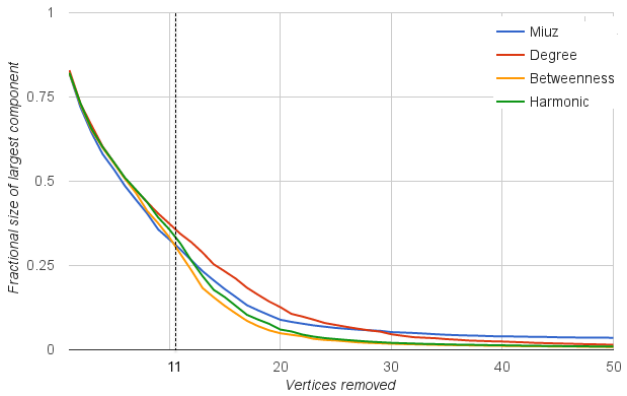
Figure 2: Effects of sequentially disconnecting nodes on power-law networks, plotting the fractional size of largest component after disconnecting x nodes and using as a selection strategy: Miuz (blue), Degree (red), Betweenness (orange), and Harmonic (green).



(a) $\alpha = 2.1$



(b) $\alpha = 2.2$



(c) $\alpha = 2.3$

Figure 3: Size of the largest fractional connected component and number disconnected nodes. Dashed line shows the breaking point when Miuz is no longer the best attacking strategy for $\alpha = 2.1 - 2.3$.