Comparative Network Robustness Evaluation of Link Attacks

Clara Pizzuti[1], Annalisa Socievole[1], and Piet Van Mieghem[2]

[1] National Research Council of Italy (CNR), Institute for High Performance Computing and Networking (ICAR), Via P. Bucci, 8-9C, 87036 Rende (CS), Italy
{clara.pizzuti.annalisa.socievole}@icar.cnr.it

[2] Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, Delft, the Netherlands
P.F.A.VanMieghem@tudelft.nl

Abstract. Existing link attack strategies in networks differ in the importance or robustness metric, that quantifies the effect of a link removal upon the network's vulnerability. In this paper, we investigate the role of the *effective resistance matrix* in the removal of links on a graph and compare this removal strategy with other state-of-the-art attack strategies over synthetic networks. The results of the analysis show that the effective resistance and the link-betweenness strategies behave similarly and are more harmful than the degree based strategies when evaluating robustness with different performance measures.

Keywords: Complex networks, robustness, graph resistance.

1 Introduction

Several critical infrastructure, such as the transportation and telecommunication systems, the electric power grids, as well the Internet and the World-Wide-Web, are modeled with networks since this representation allows to specify how the components of a system are interconnected to the other components through links, and to understand many real-world phenomena. An important aspect to study is the capability of a system to withstand attacks. Network robustness [18] is interpreted as a measure of the network response to perturbations or challenges (such as failures or external attacks) imposed on the network. Currently, however, there does not exist an agreed framework that defines and quantifies network robustness for any network and any dynamic process or service on that network.

Since the seventies, Frank and Firsh [10] analyzed when a network can be considered to survive an attack. They introduced a number of criteria based on the connectivity of a graph. In particular, the "connectivity" of a graph should obey that (1) all the components can communicate with one another, (2) the shortest path between each pair of nodes is no longer than a specified length, (3) the size of the largest connected component is above a specified threshold. Several measures based on these concepts have been proposed since then. Albert et al. [2] studied the robustness of scale-free and random networks by evaluating the fragmentation of networks when an increasing fraction of nodes/links is removed. They computed the diameter D of a network, that is the number of links (or hops) in the longest shortest path in the graph, the fraction of nodes contained in the largest connected component, and the average size of the isolated clusters. Other measures of robustness are based on graph spectra. Fielder [9] introduced as metric of graph connectedness the *algebraic connectivity*, i.e. the second smallest eigenvalue of the Laplacian matrix of a graph. He showed that the larger the algebraic connectivity, the more difficult it is to cut the graph in components. Wu et al. [21] proposed the *natural connectivity*, which considers the number of closed walks of all possible lengths, where the length equals the sum of the link weights over the path in a graph. A closed walk is defined as an alternating sequence of nodes and links such that the first and the last node are the same [16]. Ellens et al. [7] proposed the *effective graph resistance* R_G of a graph G as a new measure of robustness based on concepts from the field of electric circuits. The effective graph resistance R_G also measures the closeness of two nodes i and j and the communication capability in a graph [11].

Intuitively, robustness is related to the redundancy of paths between nodes [21]. Abbas and Egerstedt [1] experimented that the existence of multiple paths between nodes means that these nodes are highly interconnected, thus they are resilient to node or link failures, because if one path is destroyed, the two nodes can continue to communicate through an alternative route. In addition, shorter paths are preferable over longer ones, since the former correspond to an augmented level of connectivity due to lower delay time in communication and shorter paths are less affected by failures. The effective graph resistance takes into account both these aspects, thus it can be considered as a reliable measure of robustness. A thorough study of the effective graph resistance R_G to evaluate the robustness of both synthetic and real-world networks has been presented by Wang et al. [20] and Cetinay et al. [3]. Different strategies to determine which link should be added to a graph, or which link should be protected in the graph, i.e. should not be removed, to improve the effective graph resistance are proposed.

To identify the important links, whose attack/removal would cause a severe network damage, in this paper, we investigate the *effective resistance matrix* Ω, whose mean over all its elements equals the effective graph resistance, as shown in equation (5) below. Through a real-world networking scenario, we show that the effective resistance matrix provides a ranking of the links to be removed corresponding to increasing values of R_G. Then, we compare this effective resistance based attack strategy with other classical link removal strategies and evaluate their consequences on the network robustness. Specifically, we compare the different attack strategies on synthetic networks by evaluating several robustness measures.

This paper is organized as follows. Section 2 defines the effective resistance matrix and its properties. Section 3 illustrates the strategies of link attack/removal. Section 4 lists the robustness measures analyzed in the comparative analysis. Section 5 describes a case study of the effective resistance based attack on an

Internet backbone and the comparative analysis with other attack strategies on synthetic networks. Finally, Section 6 concludes the paper.

2 Preliminaries

Following the notation in [16], we consider an undirected graph G, where $\mathcal{N}$ is a set of N nodes and $\mathcal{L}$ is the set of L links. The adjacency matrix A of G is an $N \times N$ symmetric matrix with elements $a_{ij} = 1$, if there is a link between node i and j, otherwise $a_{ij} = 0$. Let $\Delta = diag(d_i)$ be the $N \times N$ diagonal degree matrix, where $d_i = \sum_{j=1}^{N} a_{ij}$, the Laplacian matrix Q of the graph G is defined as the $N \times N$ symmetric matrix $Q = \Delta - A$, with elements

$$q_{ij} = \begin{cases} d_i & \text{if } i = j \\ -1 & \text{if the link } (i,j) \in \mathcal{L} \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

The Laplacian Q is a real, semi-definite symmetric matrix, whose real eigenvalues $\mu_1 \geq \mu_2 \cdots \geq \mu_{N-1} \geq \mu_N = 0$. We denote by z_k the eigenvector of the Laplacian belonging to eigenvalue μ_k. The zero eigenvalue of any Laplacian is an important characteristic that follows from the fact that each row sum (or column sum) is zero, which implies that the eigenvector $z_N = u$, where u is the all-one vector. Like any symmetric matrix, the Laplacian possesses an eigendecomposition $Q = ZMZ^T$, where Z is the $N \times N$ orthogonal matrix with the eigenvectors $z_1, z_2, \ldots, z_N$ in the columns and $M = \text{diag}(\mu_1, \mu_2, \ldots, \mu_N)$.

If the graph G is connected, then Q has a unique smallest eigenvalue $\mu_N = 0$, while the remaining $N - 1$ are all positive. When the graph G contains m disconnected components, then the multiplicity of the zero eigenvalue is m, which means that $\mu_N = \mu_{N-1} = \cdots = \mu_{N-m-1} = 0$. Since any Laplacian Q possesses a zero eigenvalue, the rank of Q is at most $N - 1$ and $det\ Q = 0$, implying that the inverse matrix does not exist. However, the *Moore-Penrose pseudoinverse* of Q, denoted as $Q^\dagger$, exists, is unique, and can act similarly as the inverse matrix with interesting properties. In particular, for any connected graph, the eigen-decomposition of the pseudoinverse is $Q^\dagger = ZM^\dagger Z^T$, where $M^\dagger = \text{diag}\left(\frac{1}{\mu_1}, \frac{1}{\mu_2}, \ldots, 0\right)$. Even if Q is sparse, all elements in $Q^\dagger$ are non-zero [15]. More properties of the pseudoinverse $Q^\dagger$ are deduced in [17].

Given an undirected and connected graph G, we can associate an electric network to G by assigning with each link $(i,j) \in \mathcal{L}$ a positive link weights w_{ij} equal to the conductance, i.e. the inverse of the electrical resistance r_{ij} of a resistor, so that $w_{ij} = \frac{1}{r_{ij}}$. The associated electric network thus possesses a weighted adjacency matrix and a weighed Laplacian, from which the basic voltage-current relations between any pair of nodes can be deduced as explained in [17]. More precisely, the *effective resistance* ω_{ij} between any pair of nodes i and j in the associated electric network is defined as the voltage between i and j when a unit current is injected at node i, which leaves the electric network at node j. The $N \times N$ effective resistance matrix $\varOmega$ has as elements ω_{ij} the effective resistance between each node pair i and j.

The effective resistance ω_{ij} is upper bounded by the shortest path distance in a graph [16]: graphs with low diameter have also low effective graph resistance R_G. Moreover, the commute time C_{ij} between two nodes i and j, i.e. the expected number of steps in a random walk starting from the node i to visit the node j and then return to i, is $C_{ij} = 2\widetilde{L}\omega_{ij}$ or, in matrix notation $C = 2\widetilde{L}\varOmega$, where $\widetilde{L} = \frac{1}{2}u^T\widetilde{A}u$ is the sum of all the link weights in the weighted[3] adjacency matrix $\widetilde{A}$, or simply the number L of links in an unweighted graph [4]. It has also been shown [6, 13] that the square root $\sqrt{\omega}_{ij}$ of the effective resistance is an Euclidean metric. More precisely, the effective resistance matrix $\varOmega$ is a distance matrix, in which a triple of elements is non-negative, $\omega_{ii} = 0$, and obeys the triangle inequality, $\omega_{ij} \leq \omega_{ik} + \omega_{kj}$.

From the voltage-current relation derived in [17], the effective resistance matrix $\varOmega$ can be derived [13],[16, p. 205-207] as

$$\varOmega = \zeta u^T + u\zeta^T - 2Q^\dagger \tag{2}$$

where the vector

$$\zeta = \left(Q^\dagger_{11}, Q^\dagger_{22}, \ldots, Q^\dagger_{NN}\right) \tag{3}$$

contains the diagonal elements of the pseudo-inverse matrix $Q^\dagger$ of the weighted Laplacian $\widetilde{Q}$. In particular, the effective resistance between node a and b equals

$$\omega_{ab} = (e_a - e_b)^T Q^\dagger (e_a - e_b) = Q^\dagger_{aa} + Q^\dagger_{bb} - 2Q^\dagger_{ab} \tag{4}$$

where e_k is the basic vector with the m-th component equal to $(e_k)_m = \delta_{mk}$ and δ_{mk} is the Kronecker-delta: $\delta_{mk} = 1$ if $m = k$, otherwise $\delta_{mk} = 0$. The weighted effective graph resistance $\widetilde{R}_G$ is defined as the sum of the effective resistances between all possible pairs of nodes in the graph G,

$$\widetilde{R}_G = \sum_{i=1}^{N} \sum_{j=i+1}^{N} \omega_{ij} = \frac{1}{2}u^T\varOmega u \tag{5}$$

When introducing (2) in (5) and using the spectral decomposition $Q^\dagger = ZM^\dagger Z^T$, the effective graph resistance also equals [16, p. 207]

$$R_G = N \sum_{k=1}^{N-1} \frac{1}{\mu_k} \tag{6}$$

Finally, we mention interesting recent insight, deduced from the pseudoinverse of the Laplacian. Each undirected graph G, possibly weighted, can be represented by a simplex on N nodes[4] in the $N-1$-dimensional Euclidean space

[3] Weighted graph matrices are denoted by a tilde.

[4] In the topology domain, we speak about a graph consisting of nodes and links, while in the geometric space, a node corresponds to a point or node and the links in the simplex connect nodes.

[5]. We can associate a simplex to the Laplacian Q and an inverse simplex to its pseudoinverse $Q^{\dagger}$. The squared distance between two nodes i and j in the inverse simplex is equal to the effective resistance ω_{ij}.

3 Motivation of our link attack strategy

Earlier in [17] and [3], *nodes* have been removed in a graph according to their rank in the ζ vector in (3). This strategy of removing the lowest diagonal element in the pseudoinverse of the Laplacian was found, in over 100 real-world networks, to be the second best, very near though, to the removal of nodes according to highest node-betweenness. Here, we focus on removing *links* in the graph by the following strategy.

Let ω_{ik} be the minimum element of the matrix Ω. If the element a_{ik} of the adjacency matrix A is not zero, i.e. there is a link between node i and node k, then it means that the link (i, k) has the minimum resistance. This implies that a high flow of communication (in telecom networks) or current (in power grids) or traffic (in road networks), etc. can traverse that link.

While there exist several robustness definitions, here, *we consider a network as "robust" if it has a high transport capability* and hence, a low effective graph resistance R_G. The removal of the link with minimum effective resistance is expected to have a serious impact, because a considerable network flow will try to propagate over a link with low effective resistance. The removal of the link with minimum effective resistance may increase the effective graph resistance R_G most and hence, degrade the network robustness most. Let $A \circ \Omega$ be the *Hadamard* product between the adjacency matrix A of the graph and the corresponding effective resistance matrix Ω, with $(A \circ \Omega)_{ij} = a_{ij}\omega_{ij}$. The ordering of the links of A with respect to increasing elements of $A \circ \Omega$ gives the sequence of links to be removed in our link attack/removal strategy.

An interesting open question is the relation between *node* and *link* removal strategies. In particular, removing nodes in the line[5] graph $l(G)$ of the graph G corresponds to removing links in the graph G. Hence, a node removing strategy amounts to a link removal strategy in the line graph. However, for our strategy, the relation between the Laplacian of the line graph and the graph itself is not obvious, which does not allow us to immediately map the performance of a node removal strategy to the performance of a link removal strategy.

Our objective is to evaluate and compare different measures of robustness of a network when "important" links are iteratively removed. Since several definitions of link/node importance for network robustness have been defined so far (for a spectral approach, see [19]), we compare our attack strategy of removing low effective resistance links with other link attack strategies defined below. There are many methods measuring the importance of a link in terms of harmful

[5] The line graph $l(G)$ of the graph $G(N, L)$ has as set of nodes the links of G and two nodes in the line graph $l(G)$ are adjacent if and only if they have, as links in G, exactly one node of G in common [16].

effects on the network when the link is removed. Here, we consider the following strategies (at each step a link is removed according to these strategies):

- S1 (Semi-random): the link (i,j) to remove has i with maximum degree, while its neighbor j is randomly chosen;
- S2 (Degree-product): nodes i and j of the removed link have the maximum product of the degrees;
- S3 (Effective resistance): the link (i,j) to remove has the minimum effective resistance on the Ω matrix initially computed.
- S4 (Link-betweenness): the link (i,j) to remove has the maximum link-betweenness.

4 Robustness Measures in Complex networks

To evaluate how robust a network is after a particular sequence of link are removed, we adopt different performance measures:

- *Link robustness index* (R_l), proposed by Zeng and Liu [22], is defined as:

$$R_l = \frac{1}{L}\sum_{P=1}^{L} S(P) \tag{7}$$

  where L is the total number of links and $S(P)$ is the fraction of nodes of the giant component in the network after removing P links. The more robust a network is, the higher R_l is.
- *Network diameter* (D): the largest hopcount (i.e. the number of links in the path) among all the shortest paths in the graph G. As observed in [2], the smaller the diameter D, the higher the communication capability between two nodes.
- *Algebraic connectivity* (AC): the second smallest eigenvalue of the Laplacian matrix of a graph. The larger the algebraic connectivity, the more difficult to cut the graph in components [9].
- *Natural connectivity* (NC): quantifies the redundancy of alternative routes in the network by evaluating the weighted number of closed walks of all lengths.

$$NC = \ln\left(\frac{1}{N}\sum_{i=1}^{N} \exp\lambda_i\right) \tag{8}$$

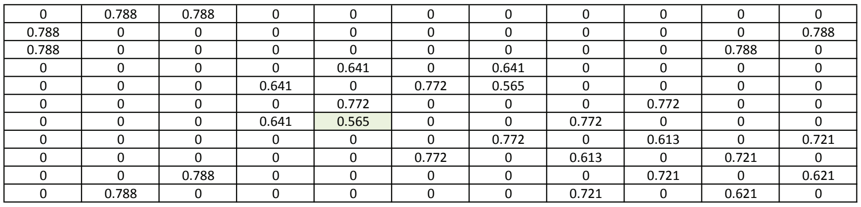
  It can be regarded as an "average exponential eigenvalue" of the adjacency matrix A. The higher the NC value, the more robust the network, since the connection between nodes is possible even if the network is damaged [21].
- *Effective graph resistance* (R_G), defined in (5) and reviewed in Section 2, is a graph metric that reflects the overall transport capability a graph: the lower R_G, the better the graph conducts traffic. The "spectral" form of R_G is presented in equation (6).
- *Randić Index (R_I)* is $R_I = \sum_{(u,v)\in\mathcal{L}} \frac{1}{d_u d_v}$, where d_u is the degree of node u. The lower R_I, the more robust the network [14].

5 Performance Evaluation

In this section, we present the results of our comparative analysis. We start analyzing a small Internet Backbone and discuss the role of the effective resistance matrix in identifying the important links to remove. Then, we perform several experiments on larger synthetically generated networks to compare the link removal strategy based on the effective resistance to the other strategies.

5.1 Case study: effective resistance on an Internet Backbone

Let us consider the network graph in Fig. 2 (the first on the left) selected from the Internet Backbones available in the repository Internet Topology Zoo (http://www.topology-zoo.org/). This graph has an effective graph resistance value of $R_G = 75.418$.



0	0.788	0.788	0	0	0	0	0	0	0	0
0.788	0	0	0	0	0	0	0	0	0	0.788
0.788	0	0	0	0	0	0	0	0	0.788	0
0	0	0	0	0.641	0	0.641	0	0	0	0
0	0	0	0.641	0	0.772	0.565	0	0	0	0
0	0	0	0	0.772	0	0	0	0.772	0	0
0	0	0	0.641	0.565	0	0	0.772	0	0	0
0	0	0	0	0	0	0.772	0	0.613	0	0.721
0	0	0	0	0	0.772	0	0.613	0	0.721	0
0	0	0.788	0	0	0	0	0	0.721	0	0.621
0	0.788	0	0	0	0	0	0.721	0	0.621	0

Fig. 1. The Hadamard product $A \circ \Omega$ between the effective resistance matrix Ω and the adjacency matrix A for the Internet Backbone. The link with the lowest value of effective resistance w_{ij} is the link (5,7) highlighted in green.

Fig. 1 illustrates that link (5,7) is the most important link with minimum $\omega_{ij} = 0.565$, whose removal deteriorates the network robustness most.

In Table 1(a) we show a ranking of the links of the Internet Backbone in increasing effective resistance ω_{ij}. We also report the resulting R_G for each link after its removal. We observe that the incremental removal of links from the graph impacts the effective graph resistance. In particular, *we observe that the ranking of the links given by the Ω matrix corresponds to an optimal order of removal of the links.* Specifically, by first removing from the graph the link (5,7) we obtain an effective graph resistance of 80.733. By subsequently removing from the graph the link (8,9) the robustness of the graph further decrease achieving 90.256 until the removal of a link disconnects the graph, in which case $R_G = \infty$ (e.g. link (8,11)). In Fig. 2, we graphically show the subsequent link removals from the Internet Backbone graph for this strategy.

We now check what happens if we iteratively recompute the Ω matrix after each link removal and delete again the link with the lowest value w_{ij}. We observe that at each step of link removal, the Ω matrix corresponding to the modified graph changes providing a difference sequence of link removals. In Table 1(b), we

Table 1. (a) Ranking of links based on the effective resistance and the resulting effective graph resistance after the removal of the link and (b) when recomputing Ω matrix after each link removal.

Node i	Node j	w_{ij}	R_G^{-}
5	7	0.567	80.733
8	9	0.613	90.256
10	11	0.621	110
4	5	0.641	220
4	7	0.641	7.125e+17
8	11	0.721	∞
9	10	0.721	∞
5	6	0.772	∞
6	9	0.772	∞
7	8	0.772	∞
1	2	0.788	∞
1	3	0.788	∞
2	11	0.788	∞
3	10	0.788	∞

(a)

Node i	Node j	w_{ij}	R_G^{-}
5	7	0.567	80.733
10	11	0.623	88.536
8	9	0.731	110
1	2	0.909	220
1	3	1	∞
2	11	1	∞
3	10	1	∞
4	5	1	∞
4	7	1	∞
5	6	1	∞
6	9	1	∞
7	8	1	∞
8	11	1	∞
9	10	1	∞

(b)

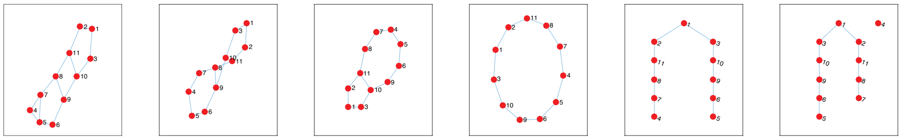


Fig. 2. Strategy S3 of subsequent removals on the Internet Backbone (the first on the left) until the first network disconnection. From left to right: (5,7),(8,9),(10,11),(4,5),(4,7).

show the ranking of the links resulting from this alternative strategy. We observe that the two strategies, even having different link removals sequences, are similar for the first three steps. However, the ordering obtained by recomputing the effective resistance disconnects the network earlier and splits the network in two pieces of almost the same size, while in the former case only node 4 is isolated from the rest of the network.

5.2 Comparative analysis of different link removal strategies

We continue the analysis on the effective resistance by comparing the harm caused by this strategy to other malicious attack strategies on links. The aim is to understand which is the most destructive attack to links and which ”important link” definition of a particular strategy makes the network less robust to subsequent link removals in decreasing order of ”importance”. To this end, we studied the random synthetic networks proposed by Erdős and Rényi [8]. These networks are generated from an initial set of $N = 128$ unconnected nodes subsequently connected between them at a random time with a fixed probability p_c. A threshold for the connectivity of these networks is $p_c \approx \ln(N)/N$ for large N. Thus, if $p > p_c$, an Erdős-Rényi graph is almost surely connected. In our simulations, to be sure to obtain a connected graph, we set $p_c = 2\ln(N)/N$.

Fig. 3 reports the comparison between the effective resistance based link removal strategy (S3) and other attack strategies over the Erdős-Rényi networks, according to the different robustness measures, as a function of the fraction of links p removed. Analyzing the average size of the largest connected component (LCC), the most destructive strategy is the link-betweenness (S4), which defines an important link as the link through which many paths traverse. Interestingly, S3 behaves similarly to S4. For both strategies, the network remains connected until the 46% of removed links, after that, the size of the LCC gradually decreases. The strategies based on node degree, S1 (semi-random) and S2 (degree-product) maintain the network connected until the 80% of link removal but, after that, the size of the LCC rapidly decreases causing a severe damaging to the network. In fact, the obtained R_l values are 0.817, 0.813, 0.837 and 0.818 for S1, S2, S3, S4, respectively, while, for $p \leq 80\%$ the R_l values are 0.995, 0.998, 0.958, 0.949, confirming the damage of the strategies as obtained by the LCC size.

Evaluating the variation of the network diameter as robustness index, strategy S4 tends to maintain the highest diameter of the LCC until the 65% of link removal. When the p value is between 0.65 and 0.84, S1 and S2 result in a diameter of the LCC very high, meaning that the information flow among nodes is difficult, especially around 0.8 when the network starts collapsing, as shown by the size of the LCC. For p values around the 90% of removed links, S3 is even more harmful than S4.

Regarding the algebraic connectivity, S3 and S4, having overall low connectivity values, are the most destructive strategies. Notice that this figure uses a logarithm scale for a better view.

Concerning the natural connectivity, we can observe that this measure is higher for S4 compared to the other strategies. Thus the other strategies, including the graph resistance-based S3, make the network less robust according to this robustness index. Hence, even if the link removal according to S4 produces the smallest LCC, compared to those of the other strategies, S4 still maintains many alternative routes. This means that the connection between nodes remains possible in spite of network damage. Only after the 80% of link removal we observe that the natural connectivity for S4 has values lower than for S3. Overall, S1 and S2 have a lower and similar natural connectivity.

Looking at the effective graph resistance measured on the LCC, we find that the edge-betweenness and the effective resistance based strategies behave again similarly. In fact, they have the highest values of R_G until the 65% of removed links, resulting in the most harmful attack strategies. Only at the critical threshold around the 80% of link removal, the node degree based strategies are more harmful, showing a peak in the R_G. As already observed, at this threshold value the network starts collapsing, thus it is unable to spread the traffic within the network.

For the Randić Index, the node degree based strategies are the most harmful having the highest R_I values. This is expected, since they remove the links where one or both nodes have high degree, and hence, the R_I index increases.

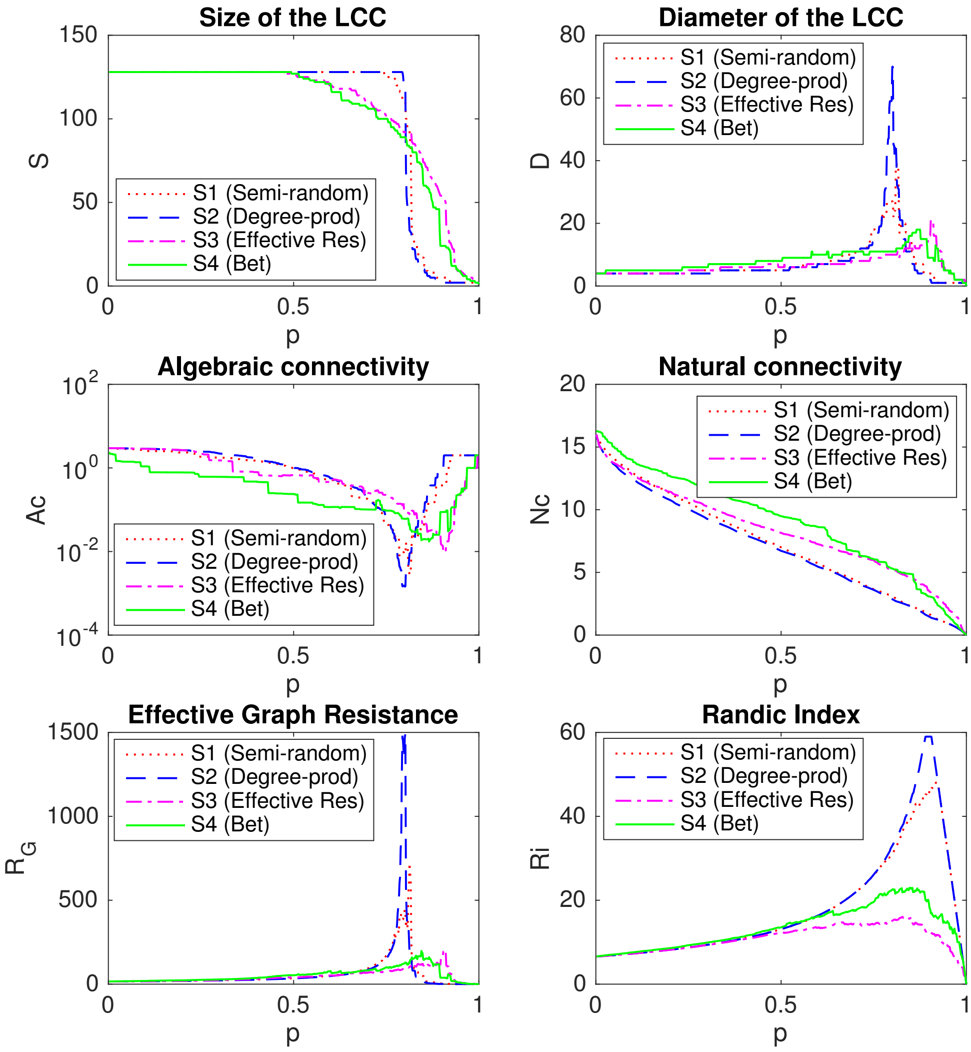


Fig. 3. Results for the Erdős-Rényi networks.

6 Conclusion

In this paper, we have focused on link attacks on networks by investigating which link removal strategy has the worst consequences on network robustness. Motivated by previous studies on the effective resistance matrix and attacks to nodes [17] [3], here we have specifically investigated the role of this matrix in identifying the links causing severe damages to the network. This matrix, in fact, provides a ranking of the links based on their transport capability and hence, a specific order of link removal. Comparing this strategy of link attacks with other removal strategies over a pool of Erdős-Rényi networks in terms of different robustness measures, we found that the strategy based on the effective resistance, namely S3, is similar to the edge-betweenness based (S4). S3 and S4 are the most destructive, according to the measure evaluating size of the largest connected component, the network diameter, the algebraic connectivity, and the effective graph resistance. The two strategies S1 and S2, based on node degree, almost always obtain the same results and are those making the networks less robust when considering the natural connectivity and the Randić index.

The effective resistance strategy, as well as the other strategies, remove links by ordering them at the beginning on the initial network. An alternative approach, as outlined in [12], consists in determining the link to remove by recomputing degrees, edge-betweenness and effective resistance at every removal step. This approach, however, needs a much higher time-demanding computation. Future work will investigate the strategies with recalculation and extend the study on other network models, such as Watts-Strogatz and Bárabasi-Albert, to understand the differences with respect to Erdős-Rényi networks. Moreover, an interesting research to pursue is to understand the relation between the Laplacian of the line graph and the graph itself, in order to compare the performance of node removal strategies to that of link removal strategies.

References

1. Waseem. Abbas and Magnus Egerstedt. Robust graph topologies for networked systems. In *3rd IFAC Workshop on Distributed Estimation and Control in Networked Systems*, pages 85–90, 2012.
2. Réka Albert, Hawoong Jeong, and Albert-László Barabási. Error and attack tolerance of complex networks. *Nature*, 406:378–381, 2000.
3. H Cetinay, K. Devriendt, and P. Van Mieghem. Nodal vulnerability to targeted attacks in power grids. *Applied Network Science*, 3:34, 2018.
4. A. K. Chandra, P. Raghavan, W. L. Ruzzo, and R. Smolensky. The electrical resistance of a graph captures its commute and cover times. In *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*, STOC '89, pages 574–586, New York, NY, USA, 1989. ACM.
5. K. Devriendt and P. Van Mieghem. The Simplex Geometry of Graphs. *Journal of Complex Networks*, 7(4):469–490, August 2019.
6. P. G. Doyle and J. L. Snell. *Random Walks and Electric Networks.* The Mathematical Association of America, USA, 1984.

7. W. Ellens, F.M. Spieksm, P. Van Mieghem, A. Jamakovic, and R.E. Kooij. Effective graph resistance. *Linear Algebra and its Applications*, 435(10):2491–2506, 2011.
8. Paul Erd6s and Alfred Renyi. On the evolution of random graphs. *Publ. Math. Inst. Hungar. Acad. Sci*, 5:17–61, 1960.
9. Miroslav Fiedler. Algebraic connectivity of graphs. *Czechoslovak Mathematical Journal*, 23(2):298–305, 1973.
10. H. Frank and Frish I. Analysis and design of survivable networks. *IEEE Transactions on Communication Technology*, 8(5):501–519, 1970.
11. Arpita Ghosh, Stephen Boyd, and Amin Saberi. Minimizing effective resistance of a graph. *SIAM Rev.*, 50(1):37–66, February 2008.
12. Petter Holme, Beom Jun Kim, and Seung Kee Yoon, Chang Noand Han. Attack vulnerability of complex networks. *Physical Review E*, 65(5):056109, 2002.
13. D. J. Klein and M. Randić. Resistance distance. *Journal of Mathematical Chemistry*, 12:81–95, 1993.
14. X. Li and Y. T. Shi. A survey on the randić index. *JCommun.Math. Comput. Chem.*, 59(1):127–156, 2008.
15. G. Ranjan, ZL. Zhang, and D. Boley. Incremental computation of pseudo-inverse of laplacian. In *Combinatorial Optimization and Applications. COCOA*, pages 730–749, Switzerland, 2014. Springer International Publishing.
16. P. Van Mieghem. *Graph Spectra for Complex Networks.* Cambridge University Press, Cambridge, U.K., 2011.
17. P. Van Mieghem, K. Devriendt, and H. Cetinay. Pseudo-inverse of the Laplacian and best spreader node in a network. *Physical Review E*, 96(3):032311, September 2017.
18. P. Van Mieghem, C. Doerr, H. Wang, J. Martin Hernandez, D. Hutchison, M. Karaliopoulos, and R. E. Kooij. A framework for computing topological network robustness. Delft University of Technology, Report20101218 (www.nas.ewi.tudelft.nl/people/Piet/TUDelftReports), 2010.
19. Piet Van Mieghem. Graph eigenvectors, fundamental weights and centrality metrics for nodes in networks. *arXiv preprint arXiv:1401.4580*, 2014.
20. Xiangrong Wang, Evangelos Pournaras, Robert E Kooij, and Piet Van Mieghem. Improving robustness of complex networks via the effective graph resistance. *The European Physical Journal B*, 87(9):221, 2014.
21. Jun Wu, Mauricio Barahona, Yue-Jin Tan, and Hong-Zhong Deng. Spectral measure of structural robustness in complex networks. *Trans. Sys. Man Cyber. Part A*, 41(6):1244–1252, November 2011.
22. A. Zeng and W. Liu. Enhancing network robustness for malicious attacks. *Physical Reviews E*, 85(6):066130, 2012.