Computational Social Networks

RESEARCH Open Access

Network robustness improvement via long-range links

Vincenza Carchiolo[1], Marco Grassia[2], Alessandro Longheu[2], Michele Malgeri[2] and Giuseppe Mangioni[2*]

*Correspondence: giuseppe.mangioni@dieei.unict.it
[2] Department of Electrical, Electronics and Computer Engineering, University of Catania, V.le A. Doria, 6, Catania, Italy
Full list of author information is available at the end of the article

Abstract
Many systems are today modelled as complex networks, since this representation has been proven being an effective approach for understanding and controlling many real-world phenomena. A significant area of interest and research is that of networks robustness, which aims to explore to what extent a network keeps working when failures occur in its structure and how disruptions can be avoided. In this paper, we introduce the idea of exploiting long-range links to improve the robustness of Scale-Free (SF) networks. Several experiments are carried out by attacking the networks before and after the addition of links between the farthest nodes, and the results show that this approach effectively improves the SF network correct functionalities better than other commonly used strategies.

Keywords: Complex networks, Robustness, Network attacks, Long-distance links

Introduction

The ideas, principles and advantages gathered about complex networks during last decades affect disparate scenarios, since networks revealed as an effective approach to model, understand and control many real-world phenomena [1, 2]. Today, the ordinary course of our society more and more relies on the correct functioning and stability of its underlying networks, from power lines to air traffic and railways, as well as social, commercial, computer networks and many others.

One of the main reasons that could compromise the correct functioning of a network is the failing of one or more nodes, whose side effect is preventing other active nodes from connecting to the rest of network, leading to a partitioned or even destroyed system.

The vulnerability analysis holds a significant role in establishing to what extent a network still provides expected services notwithstanding failures in its structure, either natural or man-made. This property, known as *robustness*, is crucial in many cases and should be considered among the set of the properties of a network, such as the node types, its dynamics, the degree distribution an so on. Despite its importance, it is still missing a sharp definition; in the literature, it can be intended as the ability of a network "to deliver an anticipated level of performance" [3], or "to maintain its efficiency after failures" [4, 5].

Springer Open

Definition apart, a further and more relevant step is how to improve the network robustness; a first approach is protecting sensitive/critical nodes, but actually this solution is not effective when facing massive attacks, as for instance when malicious cooperate to subvert computer networks. More useful attempts are the insertion of new autonomous nodes, or the rewiring of specific (possibly extensive) portion of the network; such solutions though could require significant physical modifications and/or imply high costs (e.g. think to a railway system).

A more viable alternative is the addition of a small number of new connections between specific nodes to increase the overall network robustness. Several criteria can be adopted to achieve this goal, from random links addition [6], to low-betweenness/low-degree addition strategies [7], algebraic connectivity based addition [8] or even inter degree-degree strategy for multiplex networks [9].

The choice of which nodes should be considered is also affected by the type of the network involved; here, we focus in particular on Scale-Free (SF) networks, modelling many real-world scenarios. Although intuition could suggest to strengthen hub links, being hubs the nodes with high degree (that play a strategic role for in SF networks connectiveness), here we investigate on adding links between nodes with a secondary role respect to hubs, specifically between nodes belonging to the network *periphery*. The idea of improving such *long-range* connections aims at creating a sort of *backup* paths to leverage in case of hub failures due to attacks. The introduction of long-range links to enhance some properties of a network has been proposed in the past in a different context. For example, in [10–13], the authors exploit long-range links to improve the PageRank score of a target node.

The work presented in this paper investigates on this idea to improve the robustness of a network. Basically, we propose to add one or more links between the farthest nodes in the network; several experiments carried out with attacks before and after the addition of such links show that this approach is effective yet efficient in preserving network functionalities, hence enhancing its robustness.

The paper is organized as follows: in "Related works" section, an overview of related works is presented, while in "Robustness improvement strategy" section, our proposal is introduced in detail, followed by a set of experiments conducted on different networks, illustrated and discussed in "Robustness assessment" section. Our final remarks are summarized in "Conclusions" section.

Related works

The literature concerning robustness for complex networks steadily grows up over these last years due to their larger adoption in the modelling of complex systems. Papers covering this topic can be split into two large groups: theoretical studies on the meaning of robustness in the field of complex networks and a vibrant line of work concerning complex network robustness failures in the real-world case studies.

The literature devoted a big effort to define the meaning of *robustness* and to find metrics useful to evaluate it in several contexts. For example, it is generally quantified by measuring the impact of the removal of nodes (and their corresponding links) on specific network properties. The paper [14] evaluates robustness using the Largest Connected Component (LCC), while paper [15] engages percolation thresholds; other examples are the elasticity that captures throughput under node and link removal [16], the spectrum of a graph [17], or other more sophisticated approaches [18]. Paper [19] discusses the robustness of the link prediction in complex network [20] under several attack strategies to the network: random attack, centrality-based attacks, similarity-based attacks and simulated annealing-based attack. The paper [21] introduces the sub-graph robustness problem under random attacks, localized attacks and targeted attacks. The last attack strategy is quite frequent case in a real world mainly in popular social network platforms that are generally not completely mapped. The authors of [21] discuss metrics used to evaluate the robustness of complex networks via edge betweenness centrality, the number of links cut sets and node Wiener impact; they also propose a variable neighbourhood search heuristic to improve it by adding a few well-placed links. Finally, in [22], the authors deal with the robustness of community structure rather than that of complex networks.

Among the factors robustness depend on, the network structure is still one of the most relevant [23]. For instance, it is well established that Scale-Free networks are more robust than Erdős-Rényi to random failures, but it is particularly susceptible to intentional attacks that target their hubs, i.e. few nodes with very high degree that hold most of network connectedness [24]. The work [21] shows that the sub-network robustness depends on several factors including network topology, attack mode, sampling method and the amount of data missing, generalizing some well-known robustness principles of complex networks.

In [3], the authors evaluate the relationship between network hierarchy and robustness using classical metrics to quantify robustness under several targeted failures, while in [25] the authors study the connection between robustness of community structure and the critical threshold of the resolution parameter, used to explore communities at different scales. In addition, the dynamics of the network must be considered [26] since the behaviour of robustness in dynamic systems is different than the one of static systems (some real systems for example can spontaneously recover from failures after a while, as in brain seizures). In [27], the changing of dependency among nodes over time is studied using an evolving network model consisting of failure and recovery mechanisms.

Paper [28] addresses the problem of combined attacks and [29] presents the problem of the cascading failures between interdependent networks, whereas [30] discusses the interplay between cascading failures and virus propagation.

Several applications are deeply discussed in the literature; we believe that one of the most interesting real-world application areas where robustness can impact significantly is social network, supply chain, power grid and public transport network. The paper [31] performs a comparative study based on distance distribution in social networks and shows an example applied to Amazon. The paper [32] presents Chilean Internet backbone as a case study to show the robustness, considering three and four extra links.

The authors of [33] present some interesting applications of complex network robustness to the supply chain problem and also discuss its risks, including the global supply chain one, planning for catastrophic events and increasing chain agility and risk mitigation. The authors model the system with a couple of interfering networks (an undirected and a direct network) and craft a time-varied functional equation to study the dynamic process of failed loads propagation in such interdependent network. The numerical simulations show that an abnormal crash of the network is recorded also with the removal of a small number of nodes. In [34], the authors study the robustness of manufacturing industry and validate it using an empirical dataset. Such industry is characterized by large-scale interdependent networks, a complex structure that connects companies according to commercial (buy or sell) transactions among them. The authors highlight macroscopic and microscopic characteristics of the network and shed light on vulnerabilities of the system.

In [35], the application of Network of Networks (NON) robustness for grid networks is discussed.

Another common area where complex network robustness is studied is the transport networks. Several case studies can be found in the literature; for instance, [36] analyses the vulnerability of the Shanghai urban rail, [37] proposes some ad hoc measuring of vulnerability of transportation network, [38] analyses the UK rail network in term of resilience and robustness, and [39] uses the case study of San Paulo transport network to discuss about the connection between structure and robustness.

With respect to all works cited in this section, in our work:

- the idea of exploiting long-range connections is not present in other papers; hence, to the best of our knowledge, this represents a main novelty;
- we do not introduce new robustness definitions, rather we assume as measure the LCC size [14] variation before and after attacks, mainly since it conveys information about the number and size of the connected network components;
- the type of network we focus on is the Scale-Free (SF), since this model better approximates real-world networks;
- the type of attack we consider for robustness assessment is those described in [40], i.e. targeted, degree-based attacks that particularly affect SF networks (as [23] pointed out);
- we do not address specific robustness issues as sub-graph [21], community structure [22], network hierarchy [3], or even dynamics [26]; these questions are currently out of our scope;
- the robustness question has a relevant impact on many real-world networks. For this reason, in addition to synthetic ones, we performed experiments on some real scenarios, as biological, social, technological and the Web (see "Robustness assessment" section).

Robustness improvement strategy

A commonly studied robustness enhancing technique is rewiring, i.e. the number and type of nodes are left untouched, while links among them can be modified according to some global strategy. Of course, the chosen strategy should avoid significant costs; therefore, one wants to achieve a more robust network while adding as few links as possible. The heuristic we propose in this paper is a wiring strategy based on adding long-distance links, i.e. connecting nodes belonging to the *periphery* of the network. The proposed strategy is applied to Scale-Free (SF) networks since they are the most common model for many real-world networks [2]. SF networks present a power–law degree distribution (i.e. a typical SF network shows few nodes with a very high-degree (*hubs*) and a large amount of nodes with very low degree) that is exploited by our strategy in order to improve the network robustness. Therefore, two different strategies against loss of connectivity can be evaluated:

1 increasing the number of links that connect the hubs (or their neighbours), i.e. acting on the so-called *short-distance* links;
2 conversely, increasing the number of links connecting node in the periphery (*long-distance* links).

The former strategy is based on the intuition that enhancing the connectivity among the hubs makes it harder to get a disconnected net. However, this strategy fails when hubs are directly attacked and, in addition, can be very expensive since hubs usually are very important nodes inside the network, hence creating new links for them could imply higher costs. On the other hand, the latter strategy, although counter-intuitive, is less expensive since it involves nodes playing a less relevant role in the network, and aims at creating new paths between them. Connecting long-distance nodes actually creates a set of *backup* paths whose impact is higher than adding "yet another" link between hubs; indeed, we believe that long-distance links act as *bridges* between the neighbourhood of two different hubs that can be effectively used in case of failures/attacks.

Figure 1 illustrates the proposed mechanism. As a toy example, the figure shows a portion of a Scale-Free network composed by six nodes, where two of them (nodes 3 and 4) are hubs. If we remove one of the two hubs (e.g. node 3), it is likely that the network splits in two separate components. Moreover, the distance (i.e. the shortest path) among hubs is always very short, since hubs are usually directly connected (or they are just at few steps far away). The strong connection among hubs mainly depends on two factors, (1) hubs are generally the core around which the network grown, and (2) they have many links; hence, they are connected with a high probability. In summary, it is highly unlikely that two hubs are very distant each other.

Applying the proposed strategy to the example, we made the network more robust by adding a new link (dashed line) between nodes 1 and 6. This increases the robustness since the resulting network remains connected even if hubs 3 and 4 are removed.

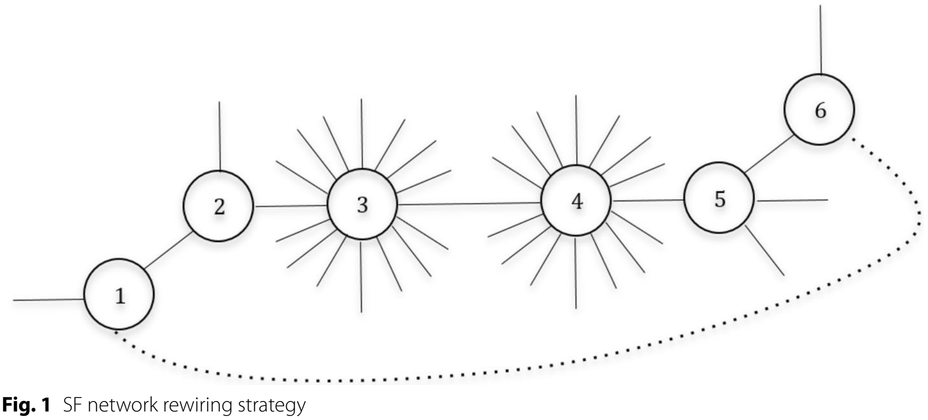


Fig. 1 SF network rewiring strategy

Robustness assessment

In order to evaluate the proposed strategy, we simulate an attack on several networks before and after the addition of new links between unconnected nodes and use as robustness measure the size of the Largest Connected Component (LCC), i.e. the largest sub-network in which any nodes pair is connected by some path. We compare various rewiring strategies in addition to our proposal. In the following, we detail the test networks, the attack process and other rewiring approaches considered.

Experiments outline

Test networks

Experiments dataset consists of five synthetic and four real-world networks. Specifically, we test on five Scale-Free (SF) networks with $1k$ nodes and average degree 2, generated using a refined version of the model presented in [41] and implemented in Pajek [42], while the four real-world networks come from NetworkRepository [43], featured with $1k \sim 3k$ nodes and average degree $\langle k \rangle \ll N$, where N is the number of nodes, i.e. they are sparse. The real-world networks belong to four different categories (biological, social, technological and web), and for each of them, we extract the LCC before performing the simulations. All networks are undirected or considered as such. See Table 1 for more details about the pre-processed networks.

Attacks

During each experiment, we perform two types of degree-based attack on the vertices which differ on when nodes degree is computed. As seen in [40], during the initial degree attack (ID) we compute the degree of each node at the beginning and we remove the nodes in descending degree order, while during the recalculated degree attack (RD) we compute the degree before any removal step and remove only the node with the highest degree.

Other strategies

Here, we briefly introduce other robustness enhancement strategies that are based on the creation of new links and that are used in the next section as baselines.

Table 1 Full list of the test networks. The column $|N|$ is the number of nodes, column $|E|$ is the number of edges, column $\langle k \rangle$ is the average degree, column $\overline{C}$ is the average clustering coefficient (as defined in [44]), and column l_G is the average path length

Network	Category	$\|N\|$	$\|E\|$	$\langle k \rangle$	$\overline{C}$	l_G
Scale-Free {1–5}	Synthetic	1000	~ 2000	~ 2	~ 0.01	~ 4.65
Bio-yeast-protein-inter	Biological	1458	1993	1.36	0.07	6.81
soc-hamsterster	Social	2000	16097	8.04	0.54	3.58
Tech-routers	Technological	2113	6633	3.13	0.24	4.60
Web-edu	Web	3031	6475	2.13	0.56	4.27

- Random based (R) [45]: one of the most extensively used strategies just adds new links between randomly chosen unconnected pair of nodes. Of course, the time complexity of this strategy is very low ($O(1)$);
- Degree based [45]: another class of strategies that employs preferential attachment between nodes depending on their degree. Low-degree (LK) strategy connects nodes with the lowest degree in the network, while the high-degree (HK) strategy connects nodes with the highest degree. The time complexity of this strategy depends on the sorting algorithm used to sort nodes in degree order, so we assume it is $O(N\log N)$, where N is the number of nodes in the network;
- Betweenness based: in a similar fashion as the degree strategy, we try connecting nodes with the lowest (LB) or the highest betweenness (HB). The betweenness of a node is a centrality measure defined as the ratio of the shortest paths between every pair of nodes that pass through that node [46]. The time complexity is polynomial because of the betweenness computation and of the sorting of the nodes according to their value, so it is $O(NM + N\log N)$, where M is the number of links in the network.

It should be noted that in the above strategies neither self-loops nor multiple links are allowed, since the attacks are performed on the nodes and those links would be removed all at once with one of the incident nodes.

Finally, we leave out the complexity of testing if the link already exists and the multiple picks if the chosen pair of nodes is already connected.

Results

In this section, we present the results of the robustness enhancement simulations obtained by applying our proposed strategy. Each experiment is repeated ten times and averaged in order to remove any bias. In addition, we average again the results on the five Scale-Free networks to remove any realization-related bias.

Figure 2 reports the dismantling curves of the network obtained adding from 0 to 50 new links according to the proposed long-distance wiring strategy. Note that the LCC is computed during an ID attack (as defined in the previous section). As shown in the figure, there is a clear gain in robustness, that becomes more substantial as the number of added links increases. Specifically, by introducing long-distance links, we obtain a peak increment of about 16% of LCC size by introducing 2.5% of new links. To help quantify the robustness enhancement, we also report the LCC size gains in the figure inset, and also peak values of each curve in Table 2. These results confirm our intuition that a small fraction of new links placed in the right place can provide a significant improvement in the network resilience.

As shown in Fig. 3 and Table 2, the above results also hold in the case of the more aggressive RD attack strategy. This is a further confirmation that long-distance links are able to increase the robustness of the original network independently of the degree-based node removal type of attacks used. Unless otherwise specified, in the rest of the paper, all results are obtained by considering the RD attack algorithm.

The next question we try to address concerns the comparison of performance of our wiring strategy (LD) with respect to the other robustness enhancement techniques

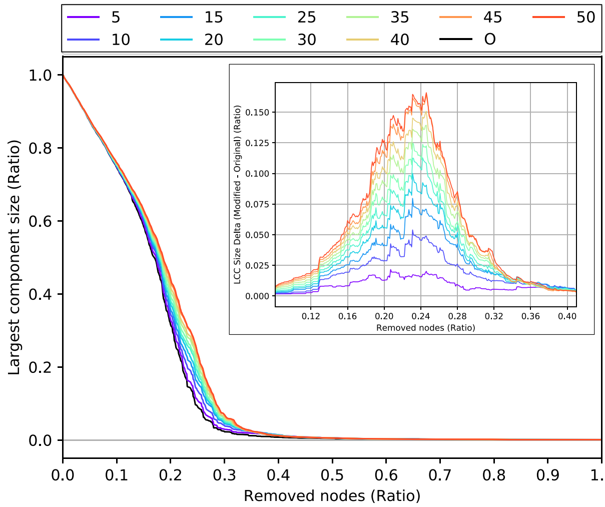


Fig. 2 SF networks robustness enhancement by using long-distance strategy under ID attack. The inset shows the gain (or delta) in the size of the LCC with respect to the original network

Table 2 SF networks peak increase in LCC size using long-distance and low-degree strategies under ID and RD attack

Attack type	ID				RD			
Strategy	LD		LK		LD		LK	
Added links	Delta	Nodes	Delta	Nodes	Delta	Nodes	Delta	Nodes
5	0.022	22	0.006	6	0.027	27	0.006	6
10	0.054	54	0.009	9	0.054	54	0.011	11
15	0.080	80	0.013	13	0.076	76	0.015	15
20	0.100	100	0.019	19	0.090	90	0.020	20
25	0.113	113	0.025	25	0.112	112	0.025	25
30	0.125	125	0.029	29	0.125	125	0.029	29
35	0.139	139	0.033	33	0.135	135	0.033	33
40	0.151	151	0.036	36	0.144	144	0.039	39
45	0.164	164	0.040	40	0.157	157	0.044	44
50	0.166	166	0.043	43	0.168	168	0.049	49

cited in the previous section. The first set of experiments (Fig. 4) reports the increments of robustness of a SF networks obtained by adding 10 links using LD, LB, HB, LK, HK and R strategies. Specifically, the inset shows the gain in LCC size with respect to the original network for different strategies. The results highlight that LD strategy outperforms all the others. Of course, the gain is larger when we add 50 new links (see Fig. 5). In this case, LD gets a peak gain that is twice with respect to the second best strategy. Therefore, we conclude that LD seems a good wiring strategy even in comparison with other approaches. The peak values of LCC size gain for each strategy are found in Table 3.

In order to quantify the magnitude of the increase in performance of LD strategy with respect to others, in Fig. 6 we plot a comparison between LB and LD by varying

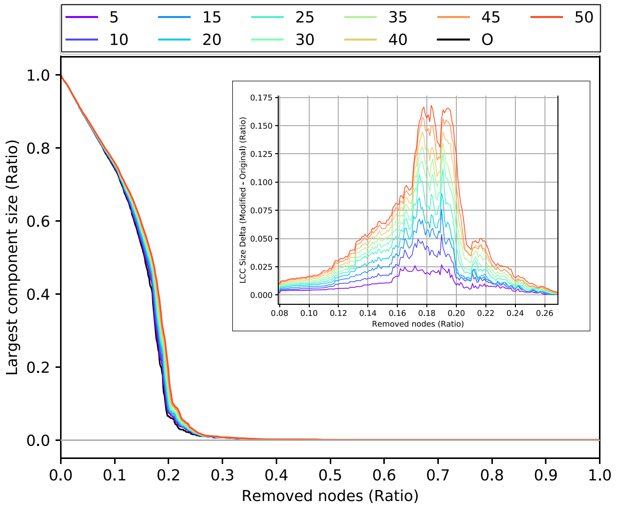


Fig. 3 SF networks robustness enhancement by using long-distance strategy under RD attack. The inset shows the gain (or delta) in the size of the LCC with respect to the original network

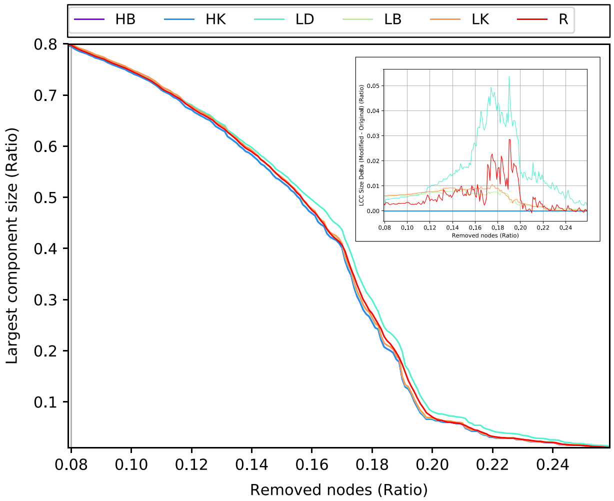


Fig. 4 SF networks robustness enhancement by using different strategies under RD attack. All plots are obtained by adding 10 new links. The inset shows the gain (or delta) in the size of the LCC with respect to the original network

the number of links added. Similar figures could be shown for the other strategies, but we omit them for the sake of concision and space as the results would be similar in the best case. As shown in the figure, LD performs initially worse than LB with a low number of new links, but this trend changes just after removing about 13% of nodes. After such a threshold, LD usually creates networks that are more robust than those obtained by using an LB-based wiring strategy. In fact, LD exhibits a peak performance of about 15% greater than LB when a fraction of 20% of nodes is removed.

Before moving to real-world networks, we investigate why the low-degree strategy performs better when few nodes are removed in the network. Please note that similar considerations can be made for the low-betweenness case. To get an insight, we plot the

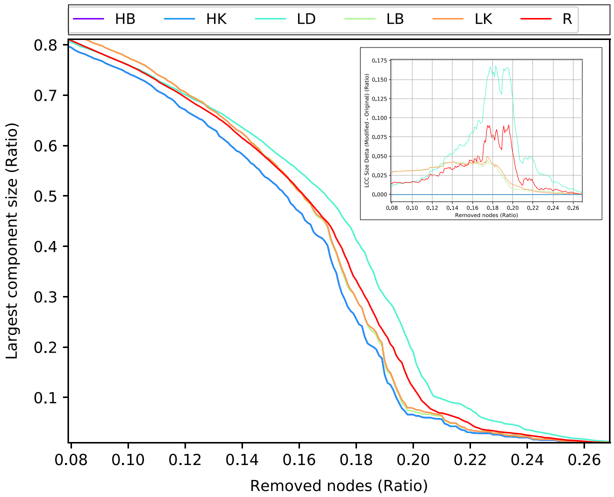


Fig. 5 SF networks robustness enhancement by using different strategies under RD attack. All plots are obtained by adding 50 new links. The inset shows the gain (or delta) in the size of the LCC with respect to the original network

Table 3 SF networks peak increase in LCC size by using different strategies under RD attack with 10 and 50 new links

Added links	10		50	
Strategy	Delta	Nodes	Delta	Nodes
HB	0.000	0	0.000	0
HK	0.000	0	0.000	0
LD	0.054	54	0.168	168
LB	0.008	8	0.045	45
LK	0.011	11	0.049	49
R	0.029	29	0.091	91

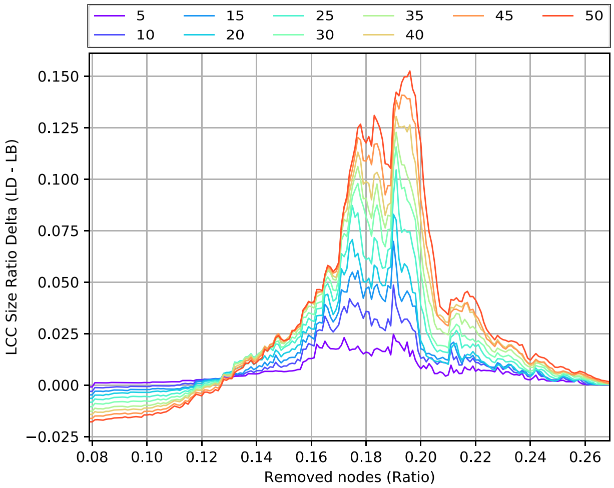


Fig. 6 SF networks robustness enhancement: comparison between LD and LB strategies under RD attack. Each plot represents the (normalized) difference between the LCC size of the network rewired by using LD strategy and that obtained using an LB-based robustness enhancement method

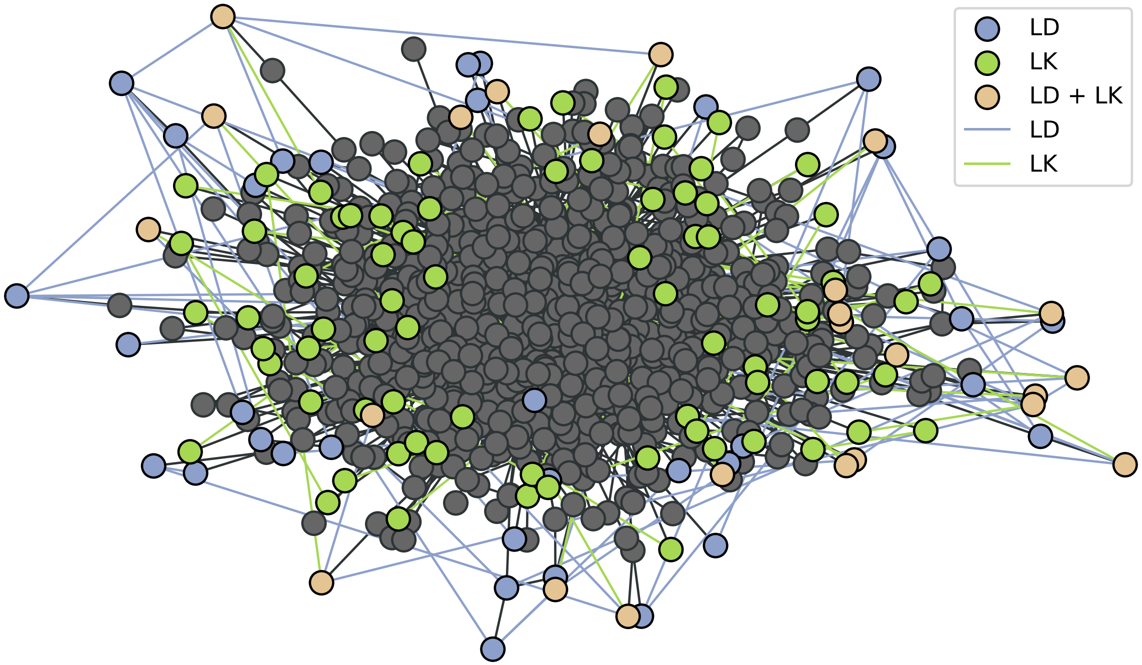
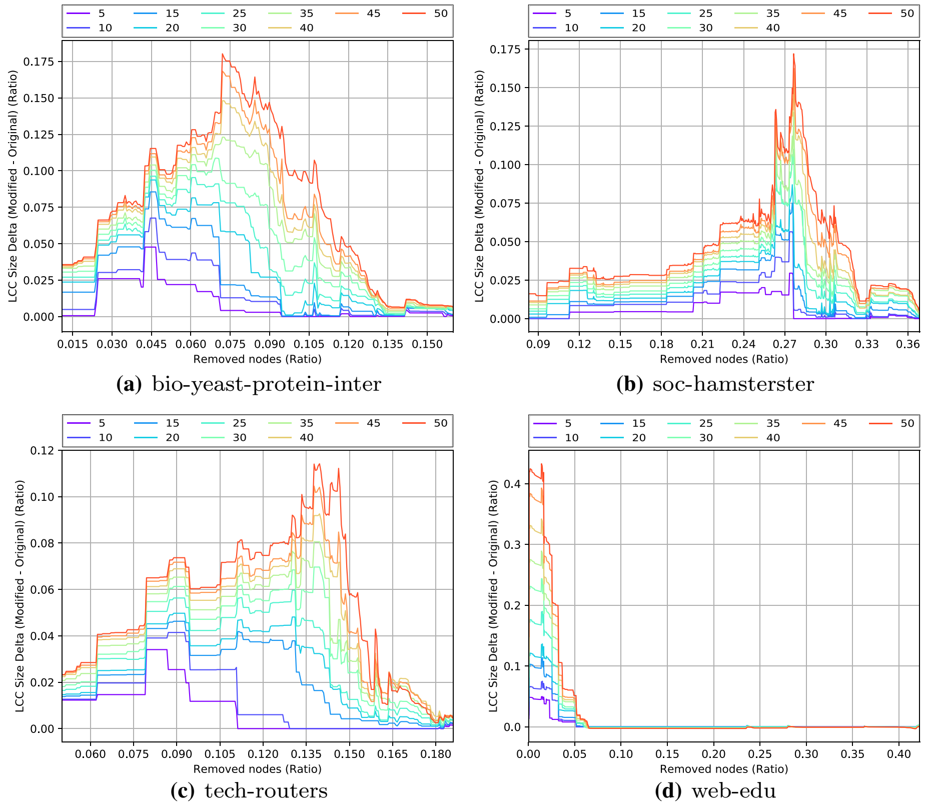


Fig. 7 Plot of one of the SF networks enhanced by LD and LK using the Fruchterman–Reingold layout



(a) bio-yeast-protein-inter

(b) soc-hamsterster

(c) tech-routers

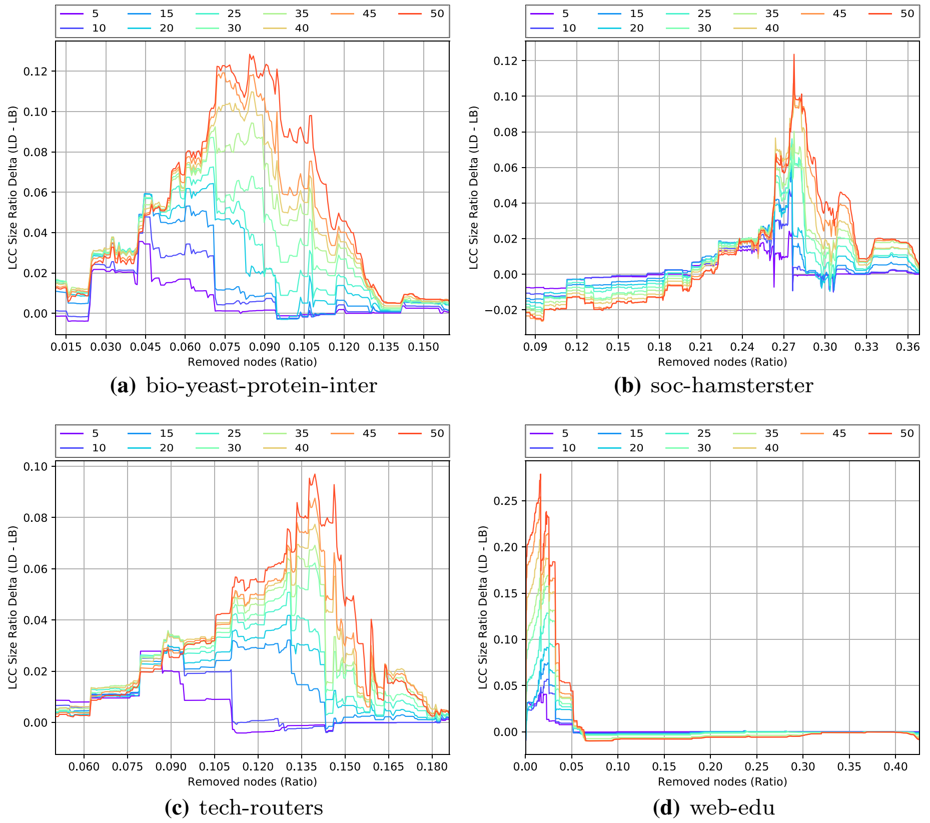
(d) web-edu

Fig. 8 Real-world networks robustness enhancement by using long-distance strategy under RD attack

synthetic networks using a force-directed layout, specifically the Fruchterman–Reingold and visually inspect which nodes are connected by the two strategies. One of the networks is shown in Fig. 7. We colour links that are added by the LD and LK strategies (and also the nodes they connect) and use a third colour if there is an overlap between the two. Our intuition is that LK strategy tends to connect nodes that are closer to the rich-group of the network, thereby creating alternative paths that keep it connected as hubs are removed, while LD strategy focuses on the periphery creating new paths that are left untouched when the rich-group is destroyed (i.e. when many nodes are removed along with the links introduced by LK strategy).

After investigating the LD strategy behaviour on synthetic SF networks, we test it on real-world networks. Specifically, we test on a biological network (*bio-yeast-protein-inter*), on a social network (*soc-hamsterster*), on a technological network (*tech-routers*) and on a Web network (*web-edu*). Refer to Table 1 for details about them.

Figure 8 shows the LCC size gain (w.r.t. the original instance) for each of those networks. Again, we add from 5 to 50 new links by using the LD strategy and perform a RD-based node removal attack. The strategy shows variable performance depending on the considered network, but the gain is always greater than zero, meaning that the LD strategy can be successfully used to enhance networks modelling real-world systems. Peak values of these plots can be found in column “LD” of Table 4.



(a) bio-yeast-protein-inter **(b)** soc-hamsterster

(c) tech-routers **(d)** web-edu

Fig. 9 Real-world networks robustness enhancement: comparison between LD and LB strategies under RD attack. Each plot represents the (normalized) difference between the LCC size of the network rewired by using LD strategy and that obtained using an LB-based robustness enhancement method

Finally, in Fig. 9, we show a comparison between LD and LB strategies on the above-mentioned real-world networks. Even in this case, LD is a more promising wiring strategy than the latter. In fact, it provides larger gains in robustness (computed as the difference between the gains), with a peak value of almost 28% on the *web-edu* network. All peak values of can be found in column "LD–LB" of Table 4.

Conclusions

This paper presents a new strategy to address the problem of network robustness enhancement.

The proposed strategy tries to increase the *interconnection* among nodes by introducing new links that connect long-distance ones. This operation is quite counter-intuitive since the most common way to enhance network connectivity is by reinforcing the most important junctions (as hubs in SF networks).

To validate the proposal, we simulated attacks on several networks—both synthetic and real-world—before and after the addition of long-distance links and compared different rewiring strategies using the Largest Connected Component size as a robustness measure. The results show that our proposed strategy outperforms other popular ones.

Table 4 RW networks peak increase in LCC size by using long-distance strategy (LD column) and the peak difference with the low-betweenness-based one in column (LD–LB), computed as the difference of deltas

Network	Strategy	LD		LD–LB	
	Added Links	Delta	Nodes	Delta	Nodes
Bio-yeast-protein-inter	10	0.068	99	0.048	69
	20	0.094	137	0.064	93
	30	0.109	158	0.087	126
	40	0.148	215	0.110	160
	50	0.180	262	0.128	186
Soc-hamsterster	10	0.056	112	0.048	96
	20	0.087	174	0.063	126
	30	0.110	220	0.071	142
	40	0.154	308	0.108	216
	50	0.172	344	0.124	248
Tech-routers-rf	10	0.041	86	0.030	63
	20	0.050	105	0.042	88
	30	0.070	147	0.062	131
	40	0.093	196	0.077	162
	50	0.114	240	0.097	204
Web-edu	10	0.075	227	0.057	172
	20	0.136	412	0.091	275
	30	0.244	739	0.157	475
	40	0.342	1036	0.219	663
	50	0.433	1312	0.279	845

Further investigations are needed to study the theoretical reasons that make the long-distance links a better choice than others apparently more intuitive. Other questions also deserve future attention, as other robustness measure criteria than LCC size, the resilience of our proposal with respect to specific SF network attacks, as well as its feasibility to other structures (as Erdős-Rényi and Watts-Strogatz).

Abbreviations
LCC: Largest Connected Component; SF: Scale-free; ID: Initial degree; RD: Degree attack; R: Random based; LK: Low degree; HK: High degree; LB: Lowest betweenness; HB: Highest betweenness; LD: Long distance.

Acknowledgements
Not applicable.

Authors' contributions
All authors contributed equally to this work. All authors read and approved the final manuscript.

Funding
This work has been partially supported by "Università di Catania - Piano della Ricerca 2016-2018 - Linea di Intervento 2".

Availability of data and materials
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Author details
[1] Department of Mathematics and Computer Sciences, University of Catania, V.le A. Doria, 6, Catania, Italy. [2] Department of Electrical, Electronics and Computer Engineering, University of Catania, V.le A. Doria, 6, Catania, Italy.

Received: 7 May 2019 Accepted: 5 November 2019
Published online: 19 November 2019

References

1. Latora V, Nicosia V, Russo G. Complex networks: principles, methods and applications. Cambridge: Cambridge University Press; 2017. https://doi.org/10.1017/9781316216002.
2. Newman M. Networks. 2nd ed. Oxford: Oxford University Press; 2018.
3. Bilal K, Manzano M, Erbad A, Calle E, Khan SU. Robustness quantification of hierarchical complex networks under targeted failures. Comput Electr Eng. 2018;72:112–24. https://doi.org/10.1016/j.compeleceng.2018.09.008.
4. Dekker AH, Colbert BD. Network robustness and graph topology. In: Proceedings of the 27th Australasian conference on computer science, vol 26. ACSC '04. Australian Computer Society, Inc., Darlinghurst, Australia; 2004. p. 359–68. http://dl.acm.org/citation.cfm?id=979922.979965.
5. Iyer S, Killingback T, Sundaram B, Wang Z. Attack robustness and centrality of complex networks. PLoS ONE. 2013;8(4):1–17. https://doi.org/10.1371/journal.pone.0059613.
6. Cao X-B, Hong C, Du W-B, Zhang J. Improving the network robustness against cascading failures by adding links. Chaos Solitons Fractals. 2013;57:35–40. https://doi.org/10.1016/j.chaos.2013.08.007.
7. Jiang Z, Liang M, Guo D. Enhancing network performance by edge addition. Int J Modern Phys C. 2011;22(11):1211–26. https://doi.org/10.1142/S0129183111016841.
8. Sydney A, Scoglio C, Gruenbacher D. Optimizing algebraic connectivity by edge rewiring. Appl Math Comput. 2013;219(10):5465–79. https://doi.org/10.1016/j.amc.2012.11.002.
9. Ji X, Wang B, Liu D, Chen G, Tang F, Wei D, Tu L. Improving interdependent networks robustness by adding connectivity links. Phys A Stat Mech Appl. 2016;444:9–19. https://doi.org/10.1016/j.physa.2015.10.010.
10. Carchiolo V, Grassia M, Longheu A, Malgeri M, Mangioni G. Climbing ranking position via long-distance backlinks. In: International conference on internet and distributed computing systems. New York: Springer; 2018. p. 100–8.
11. Carchiolo V, Grassia M, Longheu A, Malgeri M, Mangioni G. Long distance in-links for ranking enhancement. In: International symposium on intelligent and distributed computing. New York: Springer; 2018. p. 3–10.
12. Carchiolo V, Grassia M, Longheu A, Malgeri M, Mangioni G. Strategies comparison in link building problem. In: Kotenko I, Badica C, Desnitsky V, El Baz D, Ivanovic M, editors. Intelligent distributed computing XIII. Cham: Springer; 2020. p. 197–202.
13. Carchiolo V, Grassia M, Longheu A, Malgeri M, Mangioni G. Exploiting long distance connections to strengthen network robustness. In: Xiang Y, Sun J, Fortino G, Guerrieri A, Jung JJ, editors. Internet and distributed computing systems. Cham: Springer; 2018. p. 270–277.
14. Herrmann HJ, Schneider CM, Moreira AA, Andrade JSA Jr, Havlin S. Onion-like network topology enhances robustness against malicious attacks. J Stat Mech Theory Exp. 2011;2011(01):01027.
15. Gao J, Buldyrev SV, Stanley HE, Havlin S. Networks formed from interdependent networks. Nat Phys. 2011;. https://doi.org/10.1038/nphys2180.
16. Sydney A, Scoglio C, Youssef M, Schumm P. Characterizing the robustness of complex networks. ArXiv e-prints; 2008. arXiv:0811.3272.
17. Jamakovic A, Uhlig S. Influence of the network structure on robustness. In: 2007 15th IEEE international conference on networks; 2007. p. 278–83. https://doi.org/10.1109/ICON.2007.4444099.
18. Zhou A, Maletić S, Zhao Y. Robustness and percolation of holes in complex networks. Phys A Stat Mech Appl. 2018;502:459–68. https://doi.org/10.1016/j.physa.2018.02.149.
19. Wang K, Li L, Pu C. Robustness of link prediction under network attacks. arXiv e-prints; 2018. p. 1811–04528. arXiv:1811.04528.
20. Martínez V, Berzal F, Cubero J-C. A survey of link prediction in complex networks. ACM Comput Surv. 2016;49(4):69–16933. https://doi.org/10.1145/3012704.
21. Shang Y. Subgraph robustness of complex networks under attacks. IEEE Trans Syst Man Cybern Syst. 2018;. https://doi.org/10.1109/TSMC.2017.2733545.
22. Li H-J, Wang H, Chen L. Measuring robustness of community structure in complex networks. EPL (Europhys Lett). 2014;108(6):68009. https://doi.org/10.1209/0295-5075/108/68009.
23. Schneider CM, Moreira AA, Andrade JS Jr, Havlin S, Herrmann HJ. Mitigation of malicious attacks on networks. Proc Natl Acad Sci. 2011;108:3838–41. https://doi.org/10.1073/pnas.1009440108. arXiv:1103.1741.
24. Albert R, Jeong H, Barabasi A-L. Error and attack tolerance of complex networks. Nature. 2000;406:378.
25. Wu J, Tan S-Y, Liu Z, Tan Y-J, Lu X. Enhancing structural robustness of scale-free networks by information disturbance. Sci Rep. 2017;7:127–43.
26. Li D, Fu B, Wang Y, Lu G, Berezin Y, Stanley HE, Havlin S. Percolation transition in dynamical traffic network with evolving critical bottlenecks. Proc Natl Acad Sci. 2015;112(3):669–72. https://doi.org/10.1073/pnas.1419185112.
27. Bai Y-N, Huang N, Wang L, Wu Z-X. Robustness and vulnerability of networks with dynamical dependency groups. Sci Rep. 2016;. https://doi.org/10.1038/srep37749.
28. Liu Y, Zhao C, Yi D, Eugene Stanley H. Robustness of partially interdependent networks under combined attack. Chaos Interdiscip J Nonlinear Sci. 2019;29(2):021101. https://doi.org/10.1063/1.5085850.
29. Baxter GJ, Dorogovtsev SN, Goltsev AV, Mendes JFF. Avalanche collapse of interdependent networks. Phys Rev Lett. 2012;109:248701. https://doi.org/10.1103/PhysRevLett.109.248701.
30. Zhao D, Wang Z, Xiao G, Gao B, Wang L. The robustness of interdependent networks under the interplay between cascading failures and virus propagation. EPL (Europhys Lett). 2016;115(5):58004. https://doi.org/10.1209/0295-5075/115/58004.

31. Boldi P, Rosa M, Vigna S. Robustness of social networks: comparative results based on distance distributions. In: Datta A, Shulman S, Zheng B, Lin S-D, Sun A, Lim E-P, editors. Social informatics. Berlin: Springer; 2011. p. 8–21.
32. Morales FG, Paiva MHM, Bustos-Jimenez JA. Measuring and improving network robustness: a Chilean case study. IEEE Commun Lett. 2019;23(1):44–7. https://doi.org/10.1109/LCOMM.2018.2879641.
33. Tang L, Jing K, He J, Stanley HE. Complex interdependent supply chain networks: cascading failure and robustness. Phys A Stat Mech Appl. 2016;443:58–69. https://doi.org/10.1016/j.physa.2015.09.082.
34. Brintrup A, Ledwoch A, Barros J. Topological robustness of the global automotive industry. Logist Res. 2016;9:1–1117.
35. Tu H, Xia Y, Iu HH, Chen X. Optimal robustness in power grids from a network science perspective. IEEE Trans Circuits Syst II Express Briefs. 2019;66(1):126–30. https://doi.org/10.1109/TCSII.2018.2832850.
36. Sun DJ, Zhao Y, Lu Q-C. Vulnerability analysis of urban rail transit networks: a case study of Shanghai, China. Sustainability. 2015;7(6):1–18.
37. Gao L, Liu X, Liu Y, Wang P, Deng M, Zhu Q, Li H. Measuring road network topology vulnerability by ricci curvature. CoRR; 2018. arXiv:abs/1811.05743.
38. Pagani A, Mosquera G, Alturki A, Johnson S, Jarvis S, Wilson A, Varga WG. Liz: resilience or robustness: identifying topological vulnerabilities in rail networks. R Soc Open Sci. 2019;. https://doi.org/10.1098/rsos.181301.
39. Ferreira Sousa S, Rodrigues Neto C, Fagundes Ferreira F. Structure and robustness of Sao Paulo public transport network. arXiv e-prints; 2018. p. 1808–08117. arXiv:1808.08117.
40. Holme P, Kim BJ, Yoon CN, Han SK. Attack vulnerability of complex networks. Phys Rev E Stat Nonlinear Soft Matter Phys. 2002;65(5):056109.
41. Pennock DM, Flake G, Lawrence S, Glover EJ, Giles CL. Winners don't take all: characterizing the competition for links on the web. Proc Natl Acad Sci USA. 2002;99:5207–11. https://doi.org/10.1073/pnas.032085699.
42. Batagelj V, Mrvar A. Pajek program for analysis and visualization of large networks reference manual list of commands with short explanation version be; 1999. http://mrvar.fdv.uni-lj.si/pajek/pajekman.pdf.
43. Rossi RA, Ahmed NK. The network data repository with interactive graph analytics and visualization. In: Proceedings of the twenty-ninth AAAI conference on artificial intelligence; 2015. http://networkrepository.com.
44. Watts DJ, Strogatz SH. Collective dynamics of small world networks. Nature. 1998;393:440–2. https://doi.org/10.1038/30918.
45. Beygelzimer A, Grinstein G, Linsker R, Rish I. Improving network robustness by edge modification. Phys A Stat Mech Appl. 2005;357:593–612. https://doi.org/10.1016/j.physa.2005.03.040.
46. Freeman LC. A set of measures of centrality based on betweenness. Sociometry. 1977;40(1):35–41.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.