Modularity affects the robustness of scale-free model and real-world social networks under betweenness and degree-based node attack

Applied Network Science

RESEARCH

Open Access

Modularity affects the robustness of scale-free model and real-world social networks under betweenness and degree-based node attack

Quang Nguyen[1,2*], Tuan V. Vu[3], Hanh-Duyen Dinh[4], Davide Cassi[5,7], Francesco Scotognella[6], Roberto Alfieri[5,7] and Michele Bellingeri[5,6,7]

*Correspondence: nguyenquang29@duytan.edu.vn
[1] Institute of Fundamental and Applied Sciences, Duy Tan University, Ho Chi Minh City 700000, Vietnam
Full list of author information is available at the end of the article

Abstract

In this paper we investigate how the modularity of model and real-world social networks affect their robustness and the efficacy of node attack (removal) strategies based on node degree (ID) and node betweenness (IB). We build Barabasi–Albert model networks with different modularity by a new ad hoc algorithm that rewire links forming networks with community structure. We traced the network robustness using the largest connected component (*LCC*). We find that when model networks present absent or low modular structure ID strategy is more effective than IB to decrease the *LCC*. Conversely, in the case the model network present higher modularity, the IB strategy becomes the most effective to fragment the *LCC*. In addition, networks with higher modularity present a signature of a 1st order percolation transition and a decrease of the *LCC* with one or several abrupt changes when nodes are removed, for both strategies; differently, networks with non-modular structure or low modularity show a 2nd order percolation transition networks when nodes are removed. Last, we investigated how the modularity of the network structure evaluated by the modularity indicator (*Q*) affect the network robustness and the efficacy of the attack strategies in 12 real-world social networks. We found that the modularity *Q* is negatively correlated with the robustness of the real-world social networks for both the node attack strategies, especially for the IB strategy (p-value < 0.001). This result indicates how real-world networks with higher modularity (i.e. with higher community structure) may be more fragile to node attack. The results presented in this paper unveil the role of modularity and community structure for the robustness of networks and may be useful to select the best node attack strategies in network.

Keywords: Network robustness, Modular network, Node attack strategy, Centrality measures

Introduction

The study of real-world complex networks has attracted much attention in recent decades because a large number of complex systems in the real-world can be considered as complex networks, such as social (Borgatti et al. 2009; Bellingeri et al. 2020a, 2020b), technological (Albert et al. 1999; Faloutsos et al. 1999), biological (Jeong et al. 2000; Barra and Agliari 2010), ecological complex systems (Bellingeri and Bodini 2013; Bellingeri and Vincenzi 2013). Many real-world networks show a scale-free structure, making them resilient to random node failure (Cohen et al. 2000) but can disintegrate quickly when a small proportion of important nodes are removed (Albert et al. 1999). The network's robustness, which evaluates the capability of network to hold its functioning under such failures or attacks has drawn extensive attention in recent years (Albert and Barabási 2002; Cohen et al. 2000; Callaway et al. 2000; Iyer et al. 2013; Bellingeri et al. 2015; Bellingeri et al. 2014; Dall'Asta et al. 2006; Nguyen and Nguyen 2018; Wandelt et al. 2018; Bellingeri et al. 2019, 2020a, 2020b). Usually, Monte-Carlo simulation is used to evaluate the network robustness: for random failure, nodes/ links are removed with the same probability (random removal), while for intentional attack, nodes/links are removed according to different structural properties of the network and a robustness measure is then computed during the node/edge removal simulation (Albert et al. 2000; Cohen et al. 2000, 2001; Bellingeri et al. 2020a, 2020b; Lekha and Balakrishnan 2020). To identify the node/edge removal strategy that triggers the greatest amount of damage in the system is also highly important for revealing the links/nodes that act as key players in network functioning with many practical applications (Bellingeri et al. 2020a,2020b). For example, the understanding of how the node/edge removal affects real social systems may predict how the abandoning of individuals affects the information spread in the social network, thus individuating the "influential spreaders" in the network, such as most important scholars or influencers (Ahajjam and Badir 2018; Bellingeri et al. 2020a, 2020b). On the other hand, in social contact network on which a disease can spread, it is critical to understand how node removal through vaccination affects the spread of the disease to efficiently prevent an epidemic (Holme 2004; Wang et al. 2015; Bellingeri et al. 2020a, 2020b).

One of the most important measure of network robustness is the size of the largest connected component (*LCC*), i.e. the *LCC* is the highest number of connected nodes in the network (Albert et al. 2000). The *LCC* gives us a simple interpretation of the system robustness when subjected to node/edge removal accounting the largest functioning part of the network. For example, if the Internet is attacked, all nodes (servers) within the *LCC* can still transfer information mutually and indicating the largest networked structure still active. Another example, in a social contact network, the *LCC* represents the highest number of individuals that can be affected by a disease spreading (Bellingeri et al. 2019). For this reason, the most efficient node attack strategy is the one that is able to induce the fastest *LCC* decrease (Fig. 1). Numerical simulations have shown that attack strategies based on network's nodes centrality measures can effectively individuating the most important nodes to reduce the size of the *LCC* (Albert et al. 2000, Cohen et al. 2000, 2001; Callaway et al. 2000; Iyer et al. 2013; Bellingeri and Cassi 2018; Bellingeri et al. 2014; Nguyen and Nguyen 2018; Wandelt et al. 2018; Ghalmane et al. 2019a). In specific, overall findings showed that

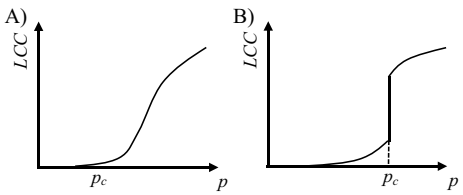


Fig. 1 Schematic behavior of the size of the *LCC* as a function of the proportion of remaining nodes p during a node removal process: **A** *LCC* shows a continuous 2nd order decreases without abrupt decrease and **B** *LCC* shows an abrupt decrease in correspondence of $p = p_c$. The node attack strategy in B is able to dismantle the network with a smaller proportion of removed nodes, i.e. is the most effective to decrease the *LCC*, thus individuating the most important nodes in network

nodes attack strategies based on betweenness centrality are highly efficient to dismantle the *LCC* (Iyer et al. 2013; Bellingeri et al. 2014; Sun et al. 2017; Nguyen and Nguyen 2018; Wandelt et al. 2018), especially for real-world networks. However, the difference in the effectiveness varied considerably among real-world networks (Iyer et al. 2013; Bellingeri et al. 2014; Wandelt et al. 2020).

The mechanism that gives rise to such an abrupt decrease is studied using percolation theory and is a signature of the first-order percolation phase transition (Achlioptas et al. 2009; Riordan and Warnke 2011; Cho et al. 2013). However, the question whether such an abrupt decrease occurs for a certain real-world network under attack remain unclear. This question is of great importance from two aspects: on one hand, if we want to break a network using node removal, we would find strategies that remove nodes that can cause such abrupt and fast decrease in *LCC*'s size. On the other hand, if we want to protect a network, we must design it in a way that such abrupt decrease should not happen. Since the network robustness must depend on its topology, several studies have investigated the relationship between topological metrics and the robustness of a network.

Iyer et al. (2013) studied robustness of model networks with power-law and exponential degree distribution, with various node clustering coefficient (or node transitivity) level. They found that increasing the clustering coefficient of the network nodes results in decreasing robustness to node attack with the most dramatic effect being displayed for node attack based on their degree and betweenness. The authors also suggested for increasing the robustness, it is necessary to design topological structures with low clustering coefficient as is consistent with the functional requirements of the network. Their simulation on real-world networks also show that the difference in the effectiveness among strategies varied across networks.

Nguyen and Trang Le (2019) studied the Facebook social networks and found those networks with higher modularity Q have lower robustness to node removal. The modularity indicator Q introduced by Newman and Girvan (2004) measures how well a network breaks into communities, (i.e. a community or module in a network is a well-connected group of nodes which have sparser connections with the nodes outside the group). Networks with high modularity Q have dense connections (more links) among the nodes within modules but sparse connections (few links) among nodes from different modules. Therefore, the modularity Q is higher in networks with marked community structure, which are called 'modular networks' (Newman and Girvan (2004)).

Using percolation theory, Dong et al. (2018) pointed out that in a modular network, a small fraction of nodes that connect nodes of different modules, called 'interconnected nodes', is critical to the robustness of the network. By analyzing the *LCC* size during node removal process by varying the fraction of interconnected nodes (r) in the network, they found that *LCC* scale with r by a power-law with universal criticality. This result suggests that modular networks with higher fraction of interconnected nodes (therefore of lower modularity Q, because the fraction of links among nodes in the same module is lower) will result in a lower *LCC* decrease during node removal and consequently higher network robustness.

Shai et al. (2015) developed both analytical and simulation analyses for evaluating the robustness of random and scale-free model networks with modular structure (Shai et al. 2015). They simulate the attack of interconnected nodes, i.e. nodes that connect to neighbors that are in other modules, and analyze the critical node occupation probability p_c, i.e. the fraction of remaining nodes p when a large decrease in *LCC* occurs, as a function of the number of modules m and the ratio between probabilities for an intra- and inter-module link α.

They found that percolation phase transition falls into two regimes depending on the number of modules m for a fixed α:

- For $m < m^*$ the network presents very high modularity and collapses abruptly under node removal as a result of the modules becoming disconnected from each another, while their internal structure is almost unaffected.
- In contrast, for $m > m*$, the network presents low modularity and therefore, the node attack causes lower damage breaking continuously the entire system without sharp *LCC* decrease (i.e. 2nd order phase transition). Put another way, m^* represents the threshold above which the network modular structure vanishes and the network returns to behaving as a non-modular network.

The above studies indicate that network modular structure is a key role in determining its robustness. However, the study of this important structural property on the network's robustness as well as other dynamic processes is still limited, as pointed out by Cherifi et al (2019). In this work, we analyze empirically how the modularity of scale-free model and real-world social networks affects their robustness and the relative efficacy of different node attack strategies. We introduce a novel algorithm to build model networks tuning their modularity. Using the proposed algorithm, we simulate networks with different levels of modularity Q by changing the ratio of intra-modules links over inter-modules links (κ). We demonstrated this method on the scale-free Barabási–Albert (BA) (Barabási and Albert 1999) model network with different degree density. We found that the attack strategy based on node betweenness, which was found to be the most effective strategy to break the *LCC* of real-world networks (Wandelt et al. 2018; Nguyen et al. 2019), is the best strategy to disrupt the *LCC* only when κ is higher than a given value κ_c, i.e. when the network has high modularity Q. Below, when network has low modularity Q, or even no modular structure, the attack strategy based on node degree is more effective. In addition, the type of the network percolation phase transition when nodes are removed change from a continuous 2nd order (in which *LCC* has no abrupt decrease)

to an abrupt 1st order transition (with abrupt *LCC* decrease) when κ increases. We also examine the effect of network's density (i.e. the average number of links per node) and the number of modules on network robustness and found that those parameters affect the network robustness, but not the type of the network percolation phase transition (1st or 2nd order) which only depends on κ. Finally, we study those effects for a variety of real-world social networks and we found that the real-world social networks with higher modularity Q are less robust when subjected to both attack strategies, especially for betweenness-based strategy. In other words, the efficacy of the attack strategy based on nodes betweenness is higher for real-world social networks showing higher modularity Q.

Methods

A network can be represented as a graph $G=(V, E)$, where $V=\{1, 2, \ldots, N\}$ is the set of N nodes (vertices), and $E=\{e_{ij} \mid i, j \in V, i \neq j\}$ is the set of E links (edges). Networks can be undirected when the links have no specified direction, or directed, in the case links present directionality. Network are unweighted when only the presence-absence of the links is considered, or weighted, in the case some interaction value is associated to the link, i.e. the link weight. Undirected and unweighted networks can be abstracted by an NxN adjacency matrix A where element $a_{ij}=1$ when there is a link between node i and j and $a_{ij}=0$ otherwise. In this paper, only undirected and unweighted networks are considered.

Generation of model scale-free network

In order to generate a model scale-free networks, we select the well-known preferential attachment Barabási–Albert (BA) model (Barabási and Albert 1999) with size of $N=10{,}000$ nodes. The BA model starts from a small clique (a completely connected graph) of N_0 nodes. At each successive time step, a new node is added and connected to M_0 different existing nodes ($M_0 < N_0$) with the probability of connect an existing node is proportional to its degree (i.e. the number of links to the node). The network then has a power-law degree distribution $P(k)=k^{-\gamma}$ with degree exponent $\gamma=3$ (Barabási and Albert 1999). We chose the average node degree $\langle k \rangle$ between 2 and 32.

From the BA network we generated modular networks using a new ad hoc algorithm by re-wiring links as following:

- Each node is assigned randomly to a module $c_i=\{1, 2, \ldots, m\}$ where m is the total number of modules. The number of nodes in each module is approximately N/m.
- For each link connecting two nodes i and j of different modules $c_i \neq c_j$ (inter-modules links), we will rewire it with a probability w (and keep it without rewiring with probability $1 - w$) by the following procedure:
    - We randomly select one node between the two ending nodes of the link, says i, and find another node l within the same module of the node i ($c_l=c_i$). We then detach the inter-modules link between nodes i and j and create a new intra-module link between nodes i and l. The node l is selected with a probability propor-

tioned to its degree (node with higher degree in the module c_i has higher probability of being selected)

- If some nodes are isolated in the network after rewiring, they will be removed. However, we find that only a negligible proportion of nodes can be isolated after the rewiring.

We show in Appendix A that, as long as N is high enough, this rewiring procedure statistically preserve the BA model node degree distribution (scale-free and degree exponent $\gamma = 3$).

Thus, by changing the probability w we can change the ratio κ between the number of intra-module links L_{intra} (links that connects two nodes from the same module) and inter-modules links L_{inter} (links that connects two nodes of different modules), thus varying the community structure of the network. The relation between κ and w can be derived as following:

- The number of inter-modules links (L_{inter}) and intra-module links (L_{intra}) before the rewiring process are $L_{inter} = \frac{(m-1)}{m}\frac{N\langle k\rangle}{2}$ and $L_{intra} = \frac{1}{m}\frac{N\langle k\rangle}{2}$.
- After the rewiring process they become $L_{\text{inter}}=(1-w)\frac{(m-1)}{m}\frac{N\langle k\rangle}{2}$ and $L_{\text{intra}}=(\frac{1}{m}+w\frac{(m-1)}{m})\frac{N\langle k\rangle}{2}$
- The ratio κ between L_{intra} and L_{inter} becomes:

$$\kappa = \frac{L_{intra}}{L_{inter}} = \frac{\left(\frac{1}{m}+w\frac{(m-1)}{m}\right)\frac{N\langle k\rangle}{2}}{1-w\frac{(m-1)}{m}\frac{N\langle k\rangle}{2}}$$

$$= \frac{1+w(m-1)}{(1-w)(m-1)} = \frac{m}{(1-w)(m-1)} - 1$$

  which is a monotone function of w when $m > 1$.

- We derive α, the ratio between the probability for a given link to be intra-link (p_{intra}) over that for a given link to be inter-link (p_{inter}) as in (Shai et al 2015) by:

$$\alpha = \frac{p_{intra}}{p_{inter}} \sim (m-1)\frac{L_{intra}}{L_{inter}} = \frac{m}{(1-w)} - (m-1)$$

  which is also a monotone function of w when $m > 1$.

The monotone change of κ and α as function of w was confirmed with simulation results which are shown in Appendix B.

Thus increasing w, we increase the modularity of the network, i.e. increasing w we emphasize the network community structure. Figure 2 presents example of modular network with $m = 5$ and different value w, created from the initial network with $N = 10{,}000$ and the average degree of $\langle k\rangle = 8$. For each experiment, we simulate 100 model networks and average the results.

The node attack strategies

The network generated above will be exposed to two node attack (removal) simulation processes (or node attack strategies) where a p proportion of nodes with lowest

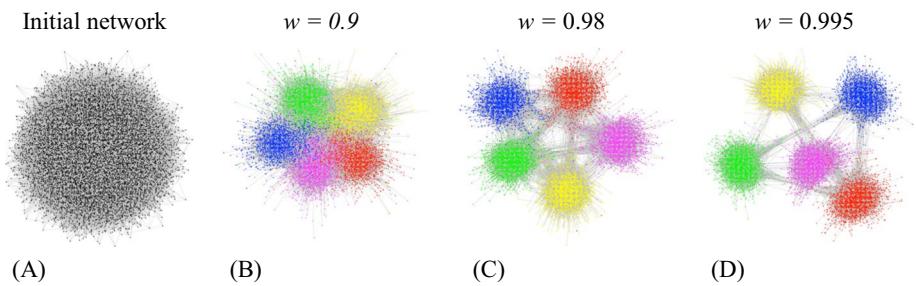


Fig. 2 Visualization of the model for generating scale-free BA modular networks. The modularity of the network increases from (**A**) to (**D**). **A** initial non-modular scale-free BA network of size $N = 10{,}000$ with average degree $\langle k \rangle = 8$. **B**–**D**: Illustration of the increasing modularity effect of w on the obtained modular network divided into $m = 5$ modules

centrality measures are kept and $q = 1\text{-}p$ proportion of highest centrality measure nodes are removed together with their links:

- The first attack strategy removes nodes according to their degree, i.e. the number of links to it, as centrality measure and it is called initial degree (ID) node attack strategy (Albert and Barabási 2002; Bellingeri et al. 2014; Wandelt et al. 2018).
- The second strategy uses a macro-scale network metric, the node betweenneess, which is the number of times that a node appears in the shortest paths among all nodes pairs in the network (Brandes 2001). This method is commonly used to break real-world networks and is called initial betweenneess (IB) node attack strategy (Bellingeri et al. 2014; Wandelt et al. 2018).

In the case of ties, i.e. nodes with equal ranking, we randomly sort the sequence. Since the node attack strategies are partially stochastic process, we average the outcomes over 100 simulations.

The network robustness measures

To measure the robustness of the network under nodes attack we traced the size of first largest connected component 1st *LCC* and the second 2nd *LCC* as a function of p. Further, for each attack simulation, we compute a single value defined as the network robustness (R) as done in Bellingeri et al. (2019). The value of R is the average of the normalized sized of the 1st *LCC* (normalized by the initial number of node N) along the removal process. R can range between two theoretical extremes, $R \simeq 0$ (absolute fragile network) and $R \simeq 1$ (absolute robust network). In addition, we identify the critical value of occupation probability p_c as the largest value of p where *LCC* has an abrupt decrease, as shown in Fig. 1B. In the case no abrupt decrease was found (Fig. 1A), we compute p_c using the "Molloy-Reed" criterion (Callaway et al. 2000; Cohen et al. 2000), which states that the network loses its overall connectivity when each node in the network has less than two links on average. It translates to the mathematic condition of $\langle k^2 \rangle / \langle k \rangle < 2$, where k is the node degree. Thus, the higher are R and the lower p_c the more robust is the network under node attack. As a consequence, when comparing the efficacy of the node attack strategies, the higher are R and lower p_c, the lower is the efficacy of the

strategy to disrupt the *LCC*. We then denote p_c^{ID} *and* p_c^{IB} the node occupation probability against ID and IB node attack strategies, respectively; as well as we denote R_{ID} *and* R_{IB} the network robustness against ID and IB node attack strategies, respectively.

Real-world social networks dataset

In addition to model networks, we analyze 12 real-world social networks, in which 8 are networks of Facebook's pages where nodes represent pages of different topics—TV Shows, Politician, Government, Public Figures, Athletes, Company, New sites and Artist—and links are mutual likes between them. The Facebook's pages data is collected from https://snap.stanford.edu, prepared by (Rozemberczki et al. 2019). Beside, we use two financial networks where nodes represent the US SP500 stocks and links are calculated from the correlation matrix using threshold method (see Nguyen et al. 2019); the co-authorship network of scientists working on network theory and experiment (NetScience) where nodes represent authors and link's weight represents the number of common papers (Newman 2003; Boccaletti et al. 2006); and the Email network of people in a large European Research Institution (Email) where nodes represent researchers and links indicate that at least one email was sent between two researchers (Leskovec and Faloutsos 2007; Hao Yin et al. 2017).

Table 1 summarizes the following statistics of the real-world social networks::

- *Node degree*: is the number of links to the node (Boccaletti et al. 2006). The degree of node i is given by:

$$k_i = \sum_{j \neq i \in N} a_{ij}$$

where a_{ij}=1 in the case there is a link connecting nodes i and j and is 0 otherwise; the term N means the sum is over all nodes in the network.

Table 1 Structural statistics of the real-world social networks: nodes (*N*), links (*L*), size of the *LCC*, size of the *LCC* as % with respect the total number of network nodes, average node degree $\langle k \rangle$, diameter (D), transitivity (C), the edge density and the modularity (*Q*)

Network	*N*	*L*	*LCC*	*LCC* (%)	$\langle k \rangle$	D	C	Density	Q
TV Shows	3892	17,262	3892	100	4.4	20.0	0.443	0.00228	0.830
Politician	5908	41,729	5908	100	7.1	14.0	0.429	0.00239	0.815
Government	7057	89,455	7057	100	12.7	10.0	0.433	0.00358	0.614
Public Figures	11,565	67,114	11,565	100	5.8	15.0	0.215	0.00100	0.645
Athletes	13,866	86,858	13,866	100	6.3	11.0	0.303	0.00090	0.637
Company	14,113	52,310	14,113	100	3.7	15.0	0.287	0.00053	0.656
New sites	27,917	206,259	27,917	100	16.2	15.0	0.138	0.00052	0.529
Artist	50,515	819,306	50,515	100	7.4	11.0	0.295	0.00064	0.457
SP500_1	315	8706	315	100	27.6	6.0	0.511	0.08802	0.253
SP500_2	371	10,636	369	99	28.7	6.0	0.718	0.07748	0.373
NetScience	1589	2742	379	24	1.7	17.0	0.878	0.00109	0.954
Email	1005	16,064	986	98	16.0	7.0	0.450	0.01592	0.341

To compute modularity Q, a clustering step was executed in priori using the popular fast-greedy modularity optimization algorithm (Clauset et al. 2004)

- *Modularity*: The modularity indicator Q calculates how modular is a given division of a network into subnetworks (modules or communities):

$$Q = \frac{1}{2L}\sum_{i,j}\left(a_{ij} - \frac{k_i k_j}{2L}\right)\delta(c_i, c_j)$$

where L is the number of links, a_{ij} is the element of the A adjacency matrix in row i and column j, k_i is the degree of i, k_j is the degree of j, c_i is the module (or community) of i, c_j that of j, the sum goes over all i and j pairs of nodes, and δ(x, y) is 1 if x = y and 0 otherwise (Clauset et al. 2004).

- *LCC*: the largest connected component (also called 'giant cluster') represents the maximum number of connected nodes in the network (Boccaletti et al. 2006; Bellingeri et al. 2020a, 2020b). Considering all the network clusters, i.e. the sub-networks of connected nodes, the *LCC* can be defined:

$$LCC = \max_j(S_j)$$

where S_j is the size (number of nodes) of the j-th cluster.

- *Diameter*: the diameter of the network (D) is the longest shortest path length of all pairs of nodes in the network, also called the longest geodesic (Newman 2013).
- *Transitivity*: the transitivity (C) is based on triplets of nodes. A triplet is three nodes that are connected by either two (open triplet) or three (closed triplet) undirected links. The transitivity is the number of closed triplets (or 3-node closed triangle) over the total number of triplets (both open and closed). In formula:

$$C = \frac{\lambda_{closed}}{\lambda_{total}}$$

where λ_{closed} is the number of closed triples and λ_{total} is the number of all possible triples in the network. Transitivity represents the overall probability for the network to have adjacent nodes interconnected, thus making more tightly connected modules (Newman et al. 2002)

- *Link Density*: the link density (Density) is number of links divided by the total number of possible links (Boccaletti et al. 2006).

Results

Robustness of non-modular scale-free BA network

In Fig. 3 we depict the outcome of a scale-free BA network of size $N = 10{,}000$ nodes and average degree $\langle k \rangle = 4$ without rewiring process subjected to ID and IB attack strategies. The average size of the 1st and 2nd *LCC* was shown as a function of the occupation probability p for each strategy. We found that the 1st *LCC* decreases continuously under both strategies and the network is completely broken down (i.e. the 1st *LCC* shrinks to *quasi* zero) at a critical occupation probability p_c (0.62 and 0.56 for ID and IB, respectively). At this transition, we also found that the 2nd *LCC* has its maximum value as shown in Fig. 3B. Such phase transitions are called 'continuous phase transitions' or 'second-order phase transitions' and denote robust network (Mnyukh 2013). Interestingly, while overall

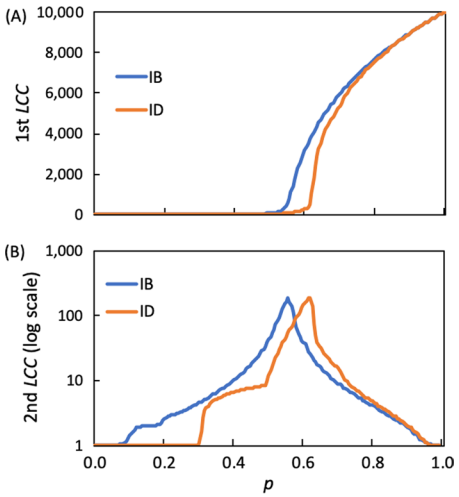


Fig. 3 Simulation result using ID and IB strategies for the non-modular network with $N = 10{,}000$ nodes and average degree $\langle k \rangle = 4$ with: **A** Size of the first largest connected component (1st *LCC*) and **B** the second largest connected component (2nd *LCC*) as a function of the occupation probability p. The result is averaged over 100 simulations

findings showed that nodes attack strategies based on betweenness centrality are highly efficient for most real-world networks (Bellingeri et al. 2014; Iyer et al, 2013; Nguyen and Nguyen 2018; Wandelt et al. 2018), our results shown different conclusion. For scale-free BA networks without modular structures, the degree-based strategy ID performs better than the betweenness-based strategy IB. On the contrary, for scale-free BA networks with significant modular structures (higher value of parameter w), betweenness-based strategy IB clearly performs better than the degree-based strategy ID. It is therefore arguable that the presence of modular structure in networks is an important factor enhancing the efficacy of betweenneess-based attack strategy for breaking the 1st *LCC*, as shown in the next sub-section.

Robustness of modular scale-free BA network

We first present the robustness of the network of different modularity by varying the rewiring ratio w, then we discuss the robustness of the network with different node average degree $\langle k \rangle$ and number of modules m.

Robustness as a function of the modularity

We simulate scale-free BA network of size $N = 10{,}000$ nodes with $m = 5$ modules and average degree $\langle k \rangle = 4$, then applying the rewiring method with increasing w. At first when w is small (and the network presents low modularity), we found that the network is resilient and the p_c remains approximately equivalent as with the original non-modular network for both ID and IB attack strategies (Fig. 4). Also, the degree-based strategy ID still performs better than the betweenness-based strategy IB. At this level of modularity, the network still owns a high number of inter-modules links. In consequence, when the attack strategies remove nodes the 1st *LCC* continuously become smaller but still

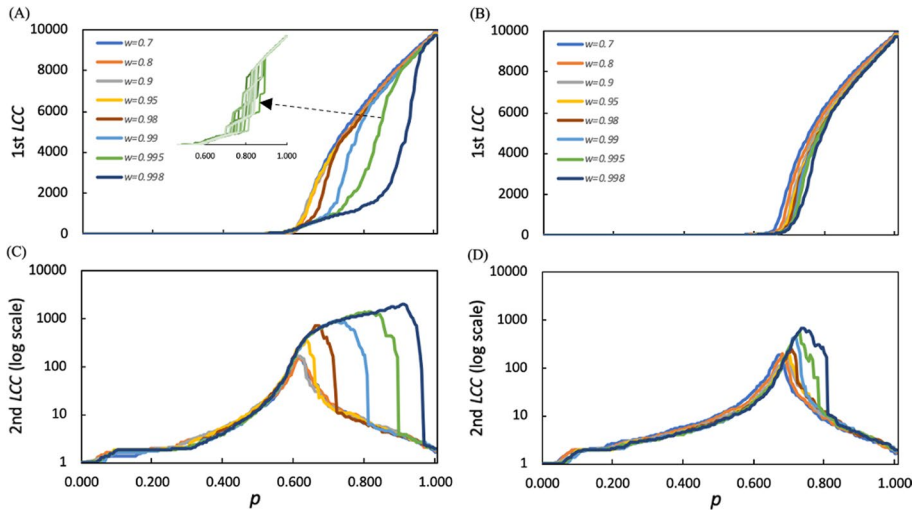


Fig. 4 Averaged simulation result for modular networks generated from BA network with $N = 10{,}000$, $m = 5$ and $\langle k \rangle = 4$ with different value of rewiring probability w: Size of the first largest connected component (1st *LCC*) and the second largest connected component (2nd *LCC*) as a function of the occupation probability p when attacked by IB (**A** and **C**, respectively) and ID (**B** and **D**, respectively). In (**A**), an insert showing 20 single simulations of the network with rewiring probability of $w = 0.995$ illustrates the abrupt decreases

hold the connection among modules, denoting higher network robustness against node attack.

Only when w is higher than 0.95 the network become fragile and the 1st *LCC* abruptly decreases at some value of p, as seen in Fig. 4A,B when the network is attacked by the IB and ID strategies, respectively. The abrupt decrease of the 1st *LCC* is clearly observed if we plot individual simulations as can been seen in the insert graph of Fig. 4A. We observed that the abrupt decrease can occur several times during a simulation and it correspond to the moment in which the node removal triggers the disconnection of a module, thus producing a faster *LCC* decrease.

This value of $w = 0.95$ corresponds to the ratio between the number of intra-module links and inter-modules links $\kappa_c = 23.8$ (for $m = 5$). At this point the connection between modules in network is sparse enough and the removal of critical nodes may break down the global connectivity. We call p_c the largest value of p with an abrupt decrease of the 1st *LCC*, as proposed by (Shai et al. 2015), and show its relationship with w in Fig. 5A. This abrupt decrease happens when a local structure is separated from the 1st *LCC* (denoting lower network robustness). As a result, the size of the 2nd *LCC* abruptly increase at p_c and gradually decrease afterward (see Fig. 4C,D).

Now we analyze the modular network robustness using the metric R. As can be seen from Fig. 4, all networks become more fragile when w increases for both IB and ID strategies. This is illustrated in Fig. 5A where R was found to be a monotonic decreasing function of w for both IB and ID strategies. We also found that the R_{IB} is higher than the R_{ID} when w is small (< 0.98); on the contrary when w is clearly higher than 0.98, R_{IB} become lower than R_{ID} showing that the network becomes more vulnerable to the IB strategy than the ID strategy.

For illustration of the relative effectiveness, we plot the performance of the IB and ID strategies at three values of w within the three regimes discussed above, $w = 0.8$, 0.99

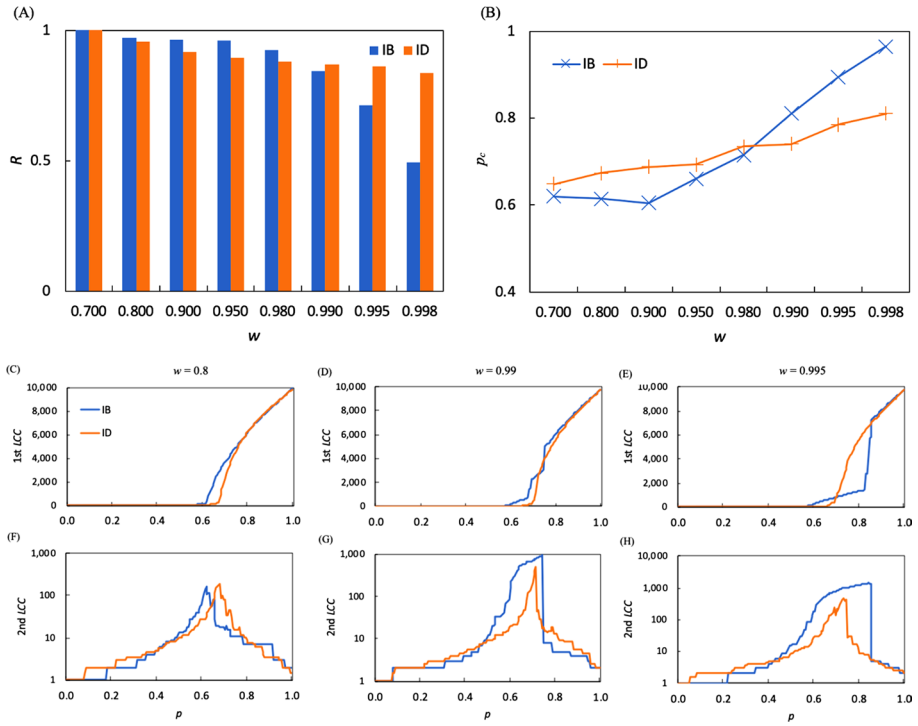


Fig. 5 Simulation result for modular networks generated from BA network with $N = 10{,}000$, $m = 5$ and $\langle k \rangle = 4$: **A** The critical occupation probability p_c and **B** the single value network robustness (R) as a function of the re-wiring ratio w. The trend is clear, when $w > 0.98$, p_c^{IB} becomes higher than p_c^{ID} and R_{IB} becomes smaller than R_{ID}, showing that the network becomes more vulnerable to the betweenness-based strategy than the degree-based strategy. **C**–**H** Size of the 1st *LCC* and the 2nd *LCC* as a function of the occupation probability p with three different value of w: 0.8 (**C**,**F**), 0.99 (**D**,**G**) and 0.995 (**E**,**H**). All results are averaged over 100 simulations

and 0.995 in Fig. 5C,D,E,F,G,H. Clearly, the ID strategy performs better than IB strategy when $w = 0.8$, approximately equally when $w = 0.99$, and it is less effective when $w = 0.995$.

Robustness as a function of network density

Next we examine the effect of the link density (i.e. the average number of links per node) by simulating scale-free BA network of size $N = 10{,}000$ nodes, number of modules $m = 5$ with varying average node degree $\langle k \rangle$ from 2 to 16, attacked for both the attack strategies IB and ID. We found that p_c decreases as the link density increase (Figs. 6 and 7B,D)—the networks become more robust when nodes have more links. However, the transitions type only depends on the rewiring ratio w and is relatively stable with respect to the average degree $\langle k \rangle$ change (Fig. 6). In other words, the ratio of the probability of inter-modules links over the probability of intra-module links α (which is a function of w) is the critical factor to determine the type of the phase transition.

Robustness as a function of number of modules

Here, we generated scale-free BA network of size $N = 10{,}000$ nodes and average degree $\langle k \rangle = 4$ with number of modules m varying from 2 to 20. We run node attack

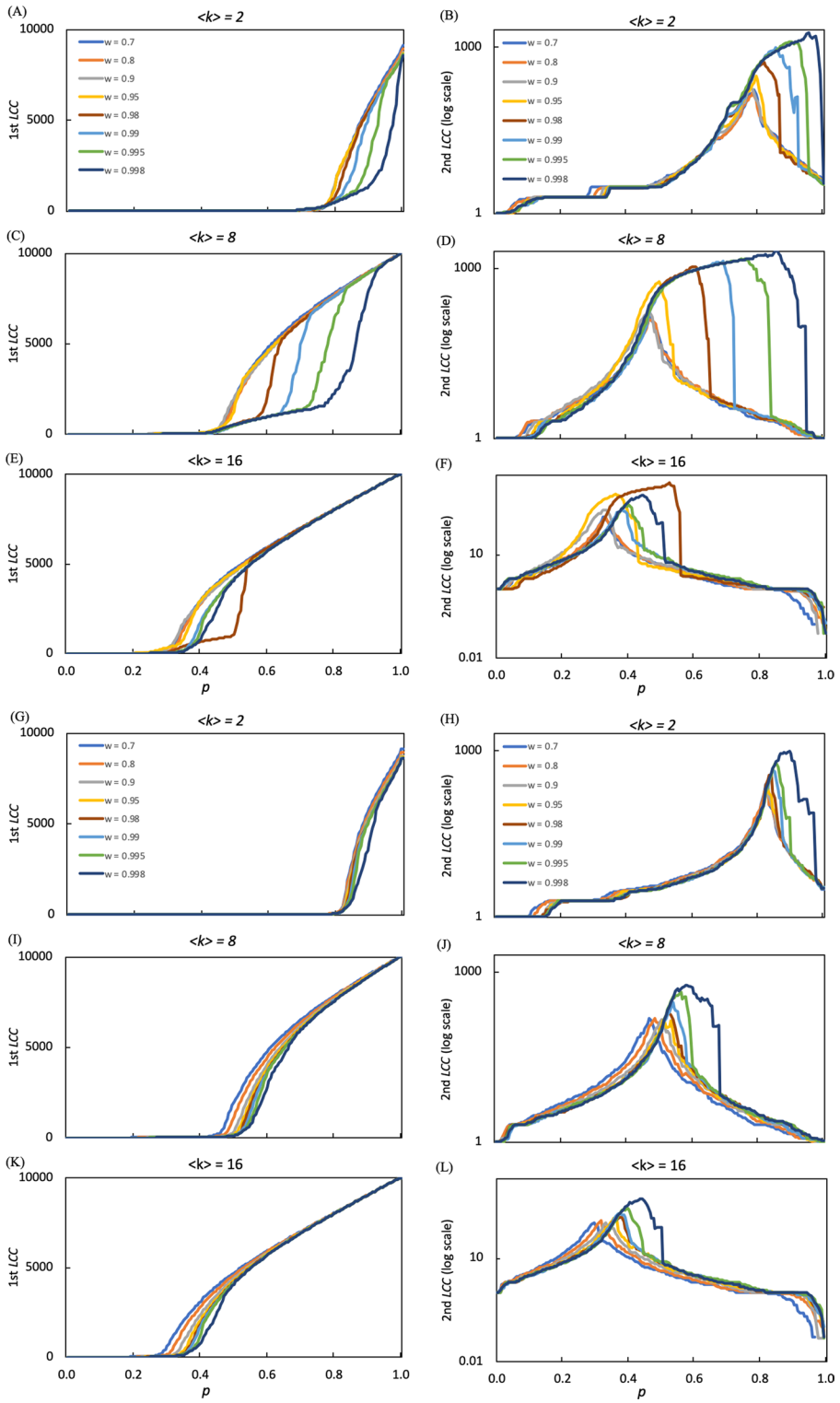


Fig. 6 Simulation result by IB and ID attack strategies for the modular networks generated from BA network with $N = 10{,}000$, $m = 5$ with different value of rewiring probability w and for different node average degree $\langle k \rangle$. Size of the 1st *LCC* (**A**, **C**, **E**) and the 2nd *LCC* (**B**, **D**, **F**) as a function of the occupation probability p when attacked by IB for various average node degree $\langle k \rangle$. Size of the 1st *LCC* (**G**, **I**, **K**) and the 2nd *LCC* (**H**, **J**, **L**) as a function of the occupation probability p when attacked by ID for various average node degree $\langle k \rangle$. All results are averaged over 100 simulations

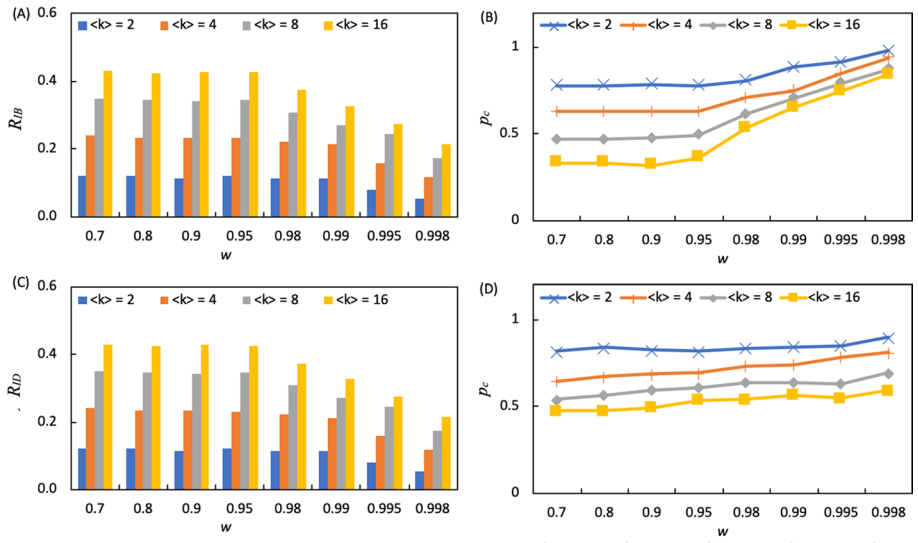


Fig. 7 Robustness measures of simulation result for the modular networks generated from BA network with $N = 10{,}000$, $m = 5$ with different value of rewiring probability w and for different node average degree $\langle k \rangle$: **A**, **C** the single value network robustness (R) and **B**, **D** the critical occupation probability p_c as a function of the re-wiring ratio w for different node average degree $\langle k \rangle$ for IB and ID strategies, respectively. All results are averaged over 100 simulations

simulation by both attack strategies IB and ID. We found that for IB strategy the p_c sharply decreases when $w < 0.98$ regardless of the number of modules in the network (Fig. 8B). The decrease is somehow smoother for ID strategy. For this reason, the transition type is relatively insensitive to the number of modules m, as we observed for the network density. Moreover, we found that the critical occupation probability p_c slightly increases with m, suggesting that the model networks become slightly more fragile when they have more modules (Fig. 8).

Robustness and structural properties in real-world networks

In Fig. 9 we present the average size of the 1st and 2nd *LCC* as a function of the occupation probability p for both IB and ID strategies for the 12 real-world networks. We found that the IB strategy is more effective than ID strategy in 7 out of 12 of the real-world networks. Those networks are supposed to have higher level of modular structure. Of the 5 remaining networks, the ID strategy is more effective than the IB strategy for the Public Figures, Athletes and Company networks, while both strategies are of the same efficacy for News sites and Artist networks.

In order to shed light on the relationship between modularity Q, node degree, and the efficacy of the attack strategies, we fit the linear models of the robustness R_{IB} against the modularity Q and the average node degree $\langle k \rangle$. In Fig. 10A we show the linear model of the R_{IB} with respect to the modularity Q for our modular model network generated with different w from a BA network of $N = 10{,}000$, $\langle k \rangle = 4$ and $m = 5$. We find a significant trend as R_{IB} decreases when Q increases (p-value = 0.01) with an abrupt decrease when Q is high (about 0.8). Very interesting, in our real-world social networks dataset, we find a similar R_{IB} decrease with modularity Q (Fig. 10E,

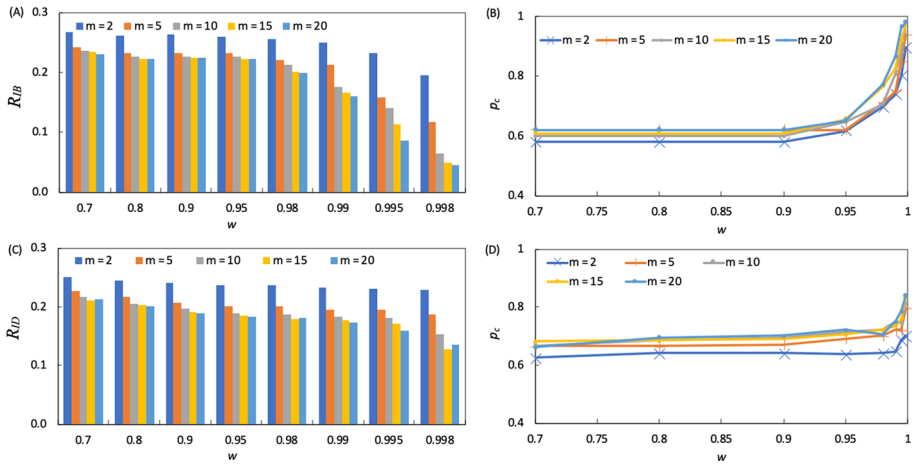


Fig. 8 Robustness measures of simulation result for the modular networks generated from BA network with $N = 10{,}000$, $\langle k \rangle = 4$ with different value of rewiring probability w and for different number of modules m in the network: **A**, **C** the single value network robustness (R) and **B**, **D** the critical occupation probability p_c as a function of the re-wiring ratio w for different node average degree $\langle k \rangle$ for IB and ID strategies, respectively. All results are averaged over 100 simulations

p-value < 0.001) corroborating the negative relationship between R_{IB} and the modularity Q of the networks. To note, we do not observe the abrupt robustness decrease in the real-world social networks (Fig. 10E). This absence of an abrupt robustness R_{IB} decrease can be due to the fact that real-world networks may vary in other structural properties (for example, links density, transitivity, assortativity, number of modules, etc..), and this structural variability may affect the network response to IB node attack. For this reason, the variability in real-world social networks structure, with many structural factors affecting the network robustness, may prevent the abrupt R_{IB} decrease as a function of the modularity Q that we observe in model networks. In fact, it should be noted that the network's robustness can be changed without changing the modularity Q. For example, Yang et al. (2015) and Mozafari and Khansari (2019) were able to improve the network's robustness with links rewiring while preserving the modularity Q.

Further, we find a clear R_{IB} and R_{ID} increase by increasing the average node degree in our model networks (p-value < 0.001, Fig. 10B,D). This is in agreement with past analyses showing how the network robustness to node removal increases with the linkage density, i.e. the higher the number of links per node, the slower is the network fragmentation under node removal (Albert and Barabási 2002; Iyer et al. 2013).

Differently, we do not find a significant relationship between R_{IB} and R_{ID} and $\langle k \rangle$ in our real-world social networks dataset (p-value > 0.1, Fig. 10F,H). Even in this case, the variability in real-world networks structure, with many structural factors affecting their robustness, may hide the emergence of a clear relationship between the linkage density measured by the average node degree $\langle k \rangle$ and the robustness of the network against node attack.

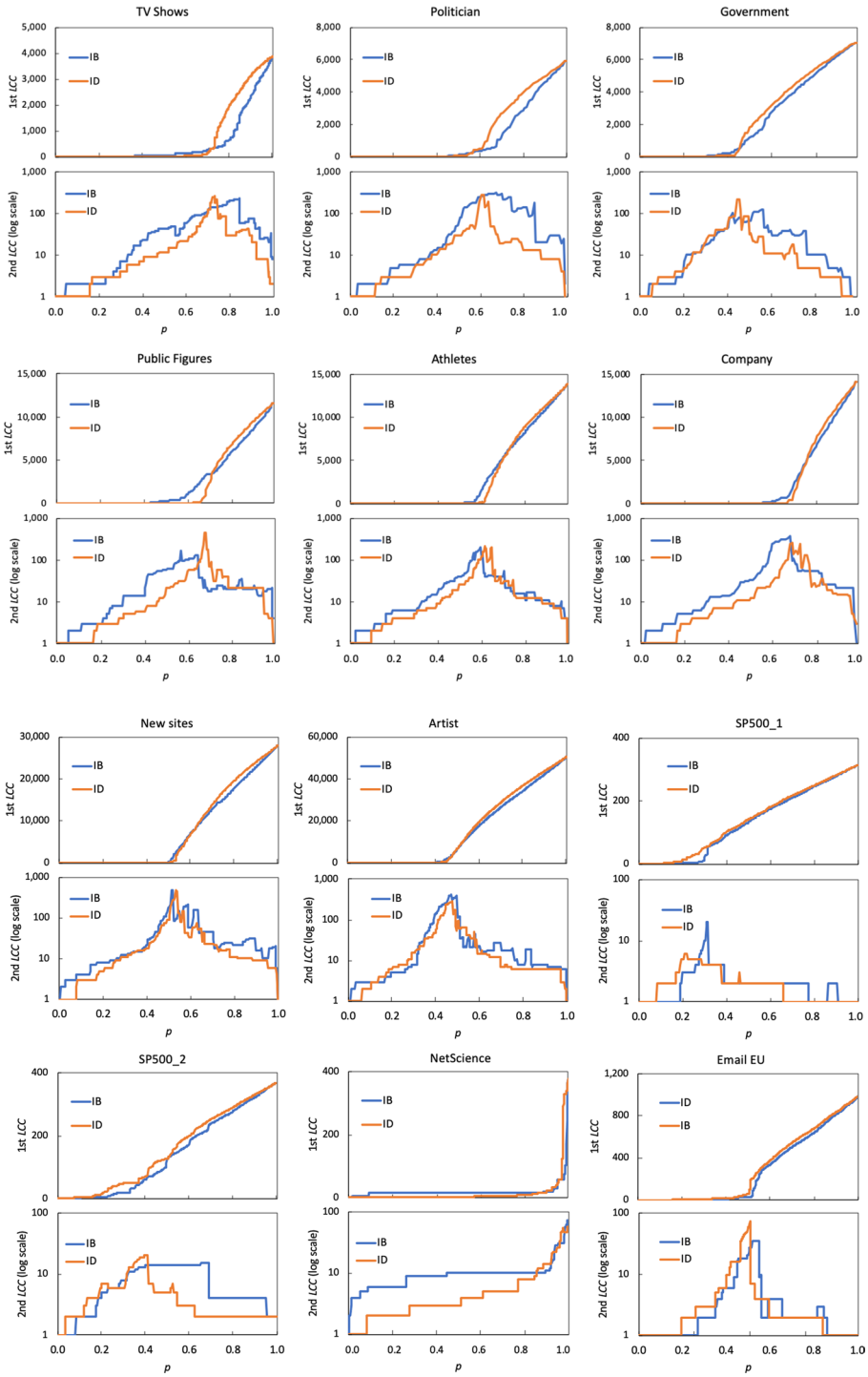


Fig. 9 The size of the 1st and 2nd *LCC* as a function of occupation probability p of 12 real-world networks when attacked by IB and ID strategies

Discussion and Conclusion

In this work we study the robustness of scale-free model and real-world social networks with different modularity. The scale-free model networks are generated from BA model

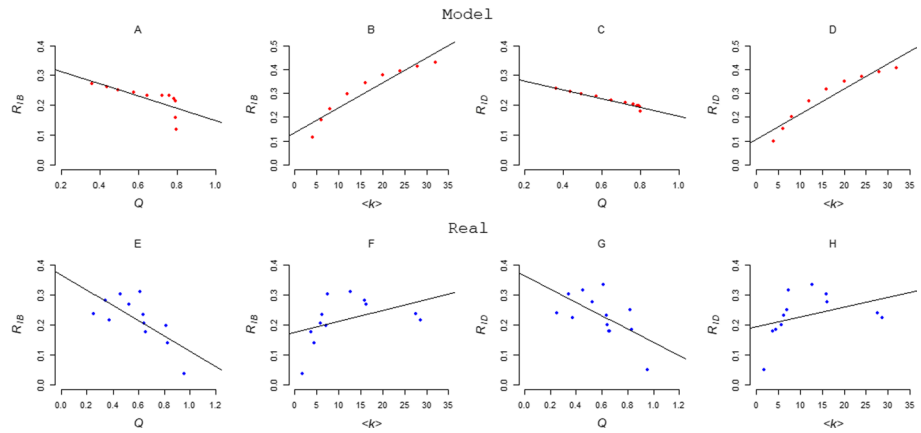


Fig. 10 Linear models of the robustness R as a function of the modularity indicator Q ($R = \alpha \cdot Q + \beta$) and the average node degree $\langle k \rangle$ ($R = \alpha \cdot \langle k \rangle + \beta$). Top row: model networks (red points); Bottom row: real-world social networks (blue points). **A**, **C** Model networks are generated with $N = 10{,}000$, $\langle k \rangle = 4$, $m = 5$ and with increasing modularity by varying the parameter w. **B**, **D** Model networks are generated with $N = 10{,}000$, $m = 5$, $w = 0.9$ and varying $\langle k \rangle$ in the interval (4, 32). Statistical outcomes of the linear model parameters (slope α and intercept β): **A** R_{IB} versus Q: $\alpha = -0.2$, $\beta = 0.35$, p-value $= 0.01$; **B** R_{IB} versus $\langle k \rangle$: $\alpha = 0.01$, $\beta = 0.14$, p-value < 0.001; **C** R_{ID} versus Q: $\alpha = -0.15$, $\beta = 0.31$, p-value < 0.001; **D** R_{ID} versus $\langle k \rangle$: $\alpha = 0.01$, $\beta = 0.1$, p-value < 0.001; **E** R_{IB} versus Q: $\alpha = -0.26$, $\beta = 0.37$, p-value $= 0.001$; **F** R_{IB} versus $\langle k \rangle$: $\alpha = 0.004$, $\beta = 0.18$, p-value $= 0.16$; **G** R_{ID} versus Q: $\alpha = -0.22$, $\beta = 0.36$, p-value $= 0.035$; **H** R_{ID} versus $\langle k \rangle$: $\alpha = 0.003$, $\beta = 0.2$, p-value $= 0.2$

with a novel method for tuning their modular structure. Using Monte-Carlo simulation we simulate two node attack strategies, IB and ID based on node's betweenness and degree, respectively. With both attack strategies, we found two types of percolation transitions take place. The 1st type of transition with abrupt decrease happens when the model network has high modularity, representing by $\kappa > \kappa_c$ with $\kappa_c \sim 23.8$ (or equivalently by $w \sim 0.98$) for both IB and ID attack strategies. Also at and above this critical point, the model network is more fragile under betweenness-based strategy attack: $R_{IB} < R_{ID}$, as found in many real-world complex networks. When $\kappa < \kappa_c$ or when the model network has no modular structure, the network experiences a continuous 2nd order phase transition under both node-attack strategies. Interestingly, under this regime, the network is more robust against the betweenness-based attack strategy IB than the degree-based attack strategy ID, contrary to most of the results on real-world networks.

In addition, our work showed that the ratio κ is the main factor for the relative efficacy between two strategies as well as the type of percolation transition: small κ corresponds to 2nd order continuous phase transition while high κ corresponds to an abrupt percolation transition. Further, we investigate how the modularity affects the robustness of the system against node removal in 12 real-world social networks and find a similar R_{IB} decrease with modularity Q (p-value < 0.001) that we observe in model networks varying the modularity. This result indicates how networks with higher modularity (i.e. with higher community structure) may be more fragile to betweenness-based node attack. At the same, this result shows how the betweenness based node attack (IB) is highly effective when attacking a network with a marked community structure (higher modularity Q). Differently, in the case the network

shows very low modularity (or no modularity), the degree-based node attack ID may perform better than IB.

The implication of this work is multiple. Firstly, it helps to understand the role of modularity and community structure for the robustness of networks, and to select the most effective node removal in networks, depending on their modular structure. If a network has high modularity, and one would like to break it, it would be better to adopt the betweenness-based strategy (IB), otherwise one should use the degree-based strategy (ID). Although we have tested two main attack strategies, the IB and ID strategies, the same procedure can be extended to other node attack strategies, especially the one that takes into account the network's community structure (Magelinski et al. 2021). Inversely, if one found that the betweenness-based strategy is more efficacy than the degree-based strategy, one can infer that this network is highly modular, and vice-versa.

Secondly, model networks of different structures can be tested using the rewiring method we propose in this paper, such as the Erdos–Renyi (ER) random network (Erdos and Renyi 1960; Bollobas 2001), the Watts-Strogatz (WS) small-world network model (Watts and Strogatz 1998), or scale-free networks with different power exponents. These analyses may be useful to find different relationship between the model network community structure and its robustness.

Finally, our novel algorithm which built model networks with tunable modularity, provides a method to study role of community structure for other dynamic processes on networks, such as epidemic spreading process (Salathe and Jones 2010), and the immunization strategy (Gupta et al. 2016, Chakraborty et al. 2016, Kumar et al. 2018, Ghalmane et al. 2019b).

Appendix

A. Prove that the rewired network statistically preserves the original node degree distribution

Given a node with degree k, the proportion of inter-modules links and intra-module links of this node before the rewiring process are approximated by $\frac{(m-1)}{m}k$ and $\frac{1}{m}k$, respectively, where m is the number of modules. A proportion w of its inter-modules links will be rewired, thus the expected number of links that this node loses is:

$$w\frac{(m-1)}{m}k$$

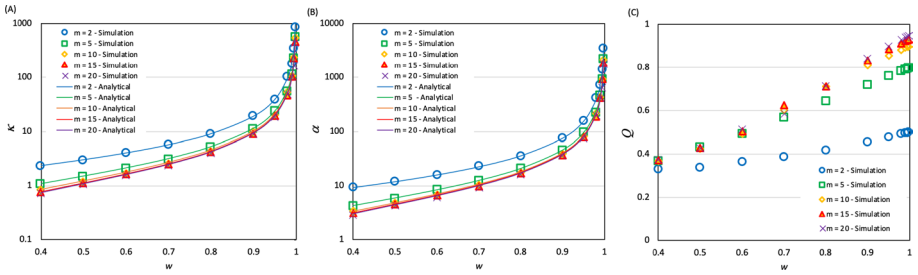
Similarly, this node can also be selected when links from nodes of the same modules are rewired. We compute the expected number of rewired links that this node can acquire as following:

- The total of rewired links in the network is $w\frac{(m-1)}{m}N < k >$
- The total of rewired links that will be connected to nodes within the module of the node is: $w\frac{(m-1)}{m}N < k > /m$

- The probability that the node is selected is proportioned to the ratio of its degree to the total degree of all nodes in the module (according to our method) and is: $k/(N < k > /m)$
- The expected number of rewired links that this node can be selected is therefore equal to: $w\frac{(m-1)}{m}N < k > /m \times k/(N < k > /m) = w\frac{(m-1)}{m}k$

which is exactly equal to the expected number of links that this node loses. In consequence, the expected number of links of each node after rewiring process is equal to their initial degree, and the network's degree distribution remain unchanged.

B. Graph of κ, α and Q as function of rewiring probability w and number of modules m



(A, B) Comparison of analytical and simulation results for modular scale-free BA network for κ (A) as a function of w and m and α (B) as a function of w and m. Both measures show the goodness of mathematical derivation in the Method section. In (C) we present the simulation results for modular scale-free BA network for the modularity measure Q as a function of w and m.

Abbreviations

ID: The node degree-based attack strategy; *IB*: The node betweenneess-based attack; *LCC*: The largest connected component; *Q*: The network modularity; *BA*: The Barabási–Albert model; L_{intra}: The number of intra-module links; L_{inter}: The number of inter-modules links; p_{intr}: The probability for a given link to be intra-link; p_{inter}: The probability for a given link to be inter-link; 1st *LCC*: The first largest connected component (is also the LCC); 2nd *LCC*: The second largest connected component; *D*: The diameter of the network; *C*: The network transitivity (clustering coefficient); R_{ID}: The network robustness under *ID* attack; R_{IB}: The network robustness under IB attack; p: The network node occupation probability; p_c: The critical value of occupation probability *p* where the transition occurs.

Acknowledgements

Many thanks to Dr. Vu-Lan Nguyen for useful comments on the paper.

Authors' contributions

QN and MB conceived the analyses, QN, T.V. Vu, H.-D. Dinh performed the simulation. QN, FS. RA, MB and DC wrote the paper. All authors read and approved the final manuscript.

Funding

This work is supported by the Vietnam National University Ho Chi Minh City (VNU-HCM), Ho Chi Minh city, Vietnam (under grant number B2018-42-01) and by the Vietnam's Ministry of Science and Technology (MOST) under the Vietnam-Italy scientific and technological cooperation program for the period of 2021–2023. This research is funded by a grant from the Italian Ministry of Foreign Affairs and International Cooperation.

Availability of data and materials

8 networks of Facebook's pages (TV Shows, Politician, Government, Public Figures, Athletes, Company, New sites and Artist) and the Email_EU networks are collected from https://snap.stanford.edu, prepared by Rozemberczki et al. (2019) and Leskovec and Faloutsos (2007). Two financial networks, SP500_1 and SP500_2 are prepared as described in Nguyen et al. (2019) from historical daily close price of the SP500 index download from the website finance.yahoo.com. The final network datasets can be provided upon reasonal request. The NetScience network dataset is download from Newman's website http://www-personal.umich.edu/~mejn/netdata/.

Declarations

Competing interests
The authors declare no competing interests.

Author details
[1]Institute of Fundamental and Applied Sciences, Duy Tan University, Ho Chi Minh City 700000, Vietnam. [2]Faculty of Natural Sciences, Duy Tan University, Da Nang City 550000, Vietnam. [3]Institute for Computational Science, Ton Duc Thang University, Ho Chi Minh City, Vietnam. [4]John Von Neumann Institute, Vietnam National University Ho Chi Minh City, Ho Chi Minh City, Vietnam. [5]Dip. Scienze Matematiche, Fisiche e Informatiche, Università di Parma, Parco Area delle Scienze, 7/A, 43124 Parma, Italy. [6]Dipartimento di Fisica, Politecnico di Milano, Piazza Leonardo da Vinci 32, 20133 Milan, Italy. [7]INFN, Gruppo Collegato di Parma, 43124 Parma, Italy.

Received: 19 May 2021 Accepted: 12 October 2021
Published online: 02 November 2021

References

Achlioptas D, D'souza RM, Spencer J (2009) Explosive percolation in random networks. Science 323(5920):1453–1455
Ahajjam S, Badir H (2018) Identification of influential spreaders in complex networks using HybridRank algorithm. Sci Rep 8:1–10. https://doi.org/10.1038/s41598-018-30310-2
Albert R, Barabási AL (2002) Statistical mechanics of complex networks. Rev Modern Phys 74:47
Albert R, Jeong H, Barabasi A-L (1999) Diameter of the world-wide web. Nature 401:130
Albert R, Jeong H, Barabasi A-L (2000) Error and attack tolerance of complex networks. Nature 406:378
Barabási A-L, Albert R (1999) Emergence of scaling in random networks. Science 286:509–512
Barra A, Agliari E (2010) Stochastic dynamics for idiotypic immune networks. Physica A 389:5903–5911
Bellingeri M, Bodini A (2013) Threshold extinction in food webs. Thyroid Res 6(2):143–152
Bellingeri M, Cassi D (2018) Robustness of weighted networks. Physica A 489:47–55
Bellingeri M, Vincenzi S (2013) Robustness of empirical food webs with varying consumer's sensitivities to loss of resource. J Theor Biol 333:18–26
Bellingeri M, Cassi D, Vincenzi S (2014) Efficiency of attack strategies on complex model and real-world networks. Physica A 414:174–180
Bellingeri M, Agliari E, Cassi D (2015) Optimization strategies with resource scarcity: from immunization of networks to the traveling salesman problem. Mod Phys Lett B 29:1550180
Bellingeri M, Bevacqua D, Scotognella F, Cassi D (2019) The heterogeneity in link weights may decrease the robustness of real-world complex weighted networks. Sci Rep 9:10692
Bellingeri M, Bevacqua D, Scotognella F, Alfieri R, Nguyen Q, Montepietra D, Cassi D (2020a) Link and node removal in real social networks: a review. Front Phys 8:228. https://doi.org/10.3389/fphy.2020.00228
Bellingeri M, Bevacqua D, Scotognella F, Alfieri R, Cassi D (2020b) A comparative analysis of link removal strategies in real complex weighted networks. Sci Rep 10(1):1–15
Boccaletti S, Latora V, Moreno Y, Chavez M, Hwang D (2006) Complex networks, structure and dynamics. Phys Rep 424:175–308
Bollobas B (2001) Random graphs, 2nd edn. Cambridge University Press, Cambridge
Borgatti SP et al (2009) Network analysis in the social sciences. Science 323:892
Brandes U (2001) A faster algorithm for betweenness centrality. J Math Sociol 25:163–177
Callaway DS, Newmann MEJ, Strogatz SH, Watts DJ (2000) Network robustness and fragility: percolation on random graphs. Phys Rev Lett 85:5468
Chakraborty D, Singh A, Cherifi H (2016) Immunization strategies based on the overlapping nodes in networks with community structure. In: Nguyen H, Snasel V (eds) Computational social networks. CSoNet 2016. Lecture Notes in Computer Science, vol 9795. Springer, Cham. https://doi.org/10.1007/978-3-319-42345-6_6
Cherifi H, Palla G, Szymanski BK, Lu X (2019) On community structure in complex networks: challenges and opportunities. Appl Netw Sci 4(1):1–35
Cho YS, Hwang S, Herrmann HJ, Kahng B (2013) Avoiding a spanning cluster in percolation models. Science 339(6124):1185–1187
Clauset A, Newman MEJ, Moore C (2004) Finding community structure in very large networks. http://www.arxiv.org/abs/cond-mat/0408187
Cohen R, Erez K, ben Avraham D, Havlin S (2000) Resilience of the internet to random breakdowns. Phys Rev Lett 85:4626
Cohen R, Erez K, ben Avraham D, Havlin S (2001) Breakdown of the internet under intentional attack. Phys Rev Lett 86:3682
Dall'Asta L, Barrat A, Barthélemy M, Vespignani A (2006) Vulnerability of weighted networks. J Stat Mech Theor Exper P04006
Dong G, Fan J, Shekhtman LM, Shai S, Du R, Tian L, Chen X, Stanley HE, Havlin S (2018) Resilience of networks with community structure behaves as if under an external field. PNAS 115(27):6911–6915
Erdos P, Renyi A (1960) On the evolution of random graphs. Publ Math Inst Hung Acad Sci 5:17
Faloutsos M, Faloutsos P, Faloutsos C (1999) On power-law relationships of the internet topology. Comput Commun Rev 29:251
Ghalmane Z, El Hassouni M, Cherifi C, Cherifi H (2019a) Centrality in modular networks. EPJ Data Sci 8(1):1–27
Ghalmane Z, El Hassouni M, Cherifi H (2019b) Immunization of networks with non-overlapping community structure. Soc Netw Anal Min 9(1):45

Gupta N, Singh A, Cherifi H (2016) Centrality measures for networks with community structure. Phys a: Stat Mech Appl 452:46–59
Hao Yin JL, Benson AR, Gleich DF (2017) Local higher-order graph clustering. In: Proceedings of the 23rd ACM SIGKDD international conference on knowledge discovery and data mining, ACM
Holme P (2004) Efficient local strategies for vaccination and network attack. Europhys Lett 68:908–914. https://doi.org/10.1209/epl/i2004-10286-2
Iyer S, Killingback T, Sundaram B, Wang Z (2013) Attack robustness and centrality of complex networks. PLoS ONE 8(4):e59613. https://doi.org/10.1371/journal.pone.0059613
Jeong H, Tombor B, Albert R, Oltvai ZN, Barabasi A-L (2000) The large-scale organization of metabolic networks. Nature 407:651
Kumar M, Singh A, Cherifi H (2018) An efficient immunization strategy using overlapping nodes and its neighborhoods. In: Companion proceedings of the web conference 2018 (WWW '18). International World Wide Web Conferences. https://doi.org/10.1145/3184558.3191566
Lekha DS, Balakrishnan K (2020) Central attacks in complex networks: a revisit with new fallback strategy. Physica A 549:124347
Leskovec JKJ, Faloutsos C (2007) Graph evolution: densification and shrinking diameters. ACM Trans Knowl Discov Data (ACM TKDD), ACM 1(1):2-es
Magelinski T, Bartulovic M, Carley KM (2021) Measuring node contribution to community structure with modularity vitality. IEEE Trans Netw Sci Eng 8(1):707–723
Mnyukh Y (2013) Second-order phase transitions, L. Landau and his successors. Am J Condens Matter Phys 3(2):25–30. https://doi.org/10.5923/j.ajcmp.20130302.02
Mozafari M, Khansari M (2019) Improving the robustness of scale-free networks by maintaining community structure. J Complex Netw 7(6):838–864
Newman MEJ (2003) The structure and function of complex networks. SIAM Rev 45:167–256
Newman M (2013) Networks: an introduction. Oxford University Press, Oxford
Newman MEJ, Girvan M (2004) Finding and evaluating community structure in networks. Phys Rev E 69:026113
Newman ME, Watts DJ, Strogatz SH (2002) Random graph models of social networks. Proc Natl Acad Sci 99(1):2566–2572
Nguyen K, Nguyen Q (2018) Resilience of stock cross-correlation network to random breakdown and intentional attack. In: Studies in computational intelligence, pp 553–61
Nguyen Q, Pham HD, Cassi D, Bellingeri M (2019) Conditional attack strategy for real-world complex networks. Physica A 530:121561
Nguyen Q, Trang Le T (2019) Structure and robustness of Facebook's pages networks. In: Proceeding of the 2019 the 10th conference on network modeling and analysis (Marami 2019), Dijon, France
Riordan O, Warnke L (2011) Explosive percolation is continuous. Science 333(6040):322–324
Rozemberczki B, Davies R, Sarkar R, Sutton C (2018) GEMSEC: graph embedding with self clustering
Salathe M, Jones JH (2010) Dynamics and control of diseases in networks with community structure. PLoS Comput Biol 6(4):e1000736. https://doi.org/10.1371/journal.pcbi.1000736
Shai S et al (2015) Critical tipping point distinguishing two types of transitions in modular network structures. Phys Rev E 92:062805
Sun X, Gollnick V, Wandelt S (2017) Robustness analysis metrics for worldwide airport network: a comprehensive. Chin J Aeronaut 30(2):500–512
Wandelt S, Sun X, Feng D, Zanin M, Havlin S (2018) A comparative analysis of approaches to network-dismantling. Sci Rep 8:13513
Wandelt S, Shi X, Sun X, Zanin M (2020) Community detection boosts network dismantling on real-world networks. IEEE Access 8:111954–111965
Wang Z, Zhao DW, Wang L, Sun GQ, Jin Z (2015) Immunity of multiplex networks via acquaintance vaccination. EPL 112:48002. https://doi.org/10.1209/0295-5075/112/48002
Watts DJ, Strogatz SH (1998) Collective dynamics of "small-world" networks. Nature 393:6684
Yang Y, Li Z, Chen Y, Zhang X, Wang S (2015) Improving the robustness of complex networks with preserving community structure. PLoS ONE 10:1–14

Publisher's Note