Physica A 590 (2022) 126667

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

Vulnerability of link-weighted complex networks in central attacks and fallback strategy

Divya P.B. [a], Divya Sindhu Lekha [b,*], T.P. Johnson [c], Kannan Balakrishnan [d]

[a] Department of Mathematics, Cochin University of Science and Technology, India
[b] Indian Institute of Information Technology Kottayam, India
[c] Applied Sciences and Humanities Division, School of Engineering, Cochin University of Science and Technology, Cochin 22, India
[d] Department of Computer Applications, Cochin University of Science and Technology, India

ARTICLE INFO

Article history:
Received 7 January 2021
Received in revised form 24 August 2021
Available online 4 December 2021

Keywords:
Complex networks
Weighted networks
Centrality
Attacks, strategies
Average geodesic
Largest connected component

ABSTRACT

In this work, we study the vulnerability of link-weighted networks against different central-attack strategies. We simulate simultaneous and sequential attacks on networks based on three network centralities, viz. degree (DC), betweenness (BC) and closeness (CC) centralities. We observed two network properties, the disintegration of giant components and updates in the average geodesic distance, to assess the severity of attacks. If the severity of attacks is calculated based on the first property alone, BC and DC-based attacks are the most hazardous. But, if the severity is computed based on the latter property, the average geodesic distance, the CC-based attacks found to be equally relevant. We show that sequential attacks based on CC are effective in crippling link-weighted networks.

Also, suppose that the critical nodes (nodes with high BC and DC) in the network are protected. In such a circumstance, we show that the fallback strategy based on profile closeness is indeed a reasonable approach for attacking protected, link-weighted networks.

1. Introduction

A complex network is a dynamically changing network with non-trivial topological features. Such a network encompasses a large number of interacting components. But the pattern of those interactions are neither regular nor purely random [1–4].

Many a real-world phenomenon are complex systems and they can be modeled as complex networks. To name a few, consider the complex systems such as social systems, transportation systems, distribution systems/logistics, communication systems, epidemic spreading and market dynamics. Complex network-based modeling and studies have found to be very effective in understanding the dynamics of such systems. The past decade has seen a rigorous use of complex networks as an efficient vehicle to analyze many real phenomenon [4–14].

The robustness of a networked structure depends on its resilient components. While trying to attack a network, the attackers focus on identifying its vulnerable parts. For example, consider the complex networks such as computer networks or terrorist networks or networks modeling spread of epidemics. The strategy of the attacker here is to identify the vulnerable nodes/ edges/ other components, damage them and break the system.

* Corresponding author.
E-mail addresses: pbdivya@gmail.com (Divya P.B.), divyaslekha@iiitkottayam.ac.in (D.S. Lekha), tpjohnson@cusat.ac.in (T.P. Johnson), mullayilkannan@gmail.com (K. Balakrishnan).

https://doi.org/10.1016/j.physa.2021.126667
0378-4371/

This study focuses on network attacks in which the most critical nodes are identified and removed from the network. Such attacks are called *node-removal attacks*. The most critical nodes in a network are those which are crucial to the network structure. These nodes make easy targets for attaining complete network destruction. Network centralities are good metrics for assessing the importance of a network node. Different variants of centrality measures are devised and extensively used for this purpose [15–28]. However, the fundamental centrality concepts like degree centrality, betweenness centrality and closeness centrality effectively identify these highly critical nodes.

Among these critical nodes, attacking nodes with high BC and DC can lead to a faster disintegration of the network. Therefore, the beneficiaries of the network can be keen on protecting these nodes. Recently, Lekha and Balakrishnan, in [21], proposed a fallback strategy (a plan B) to attack a network in such a protected environment. They showed that this new strategy imparts an equal/near-to equal destruction to the network. However, they did not explore the vulnerability of weighted networks to such attacks. In our work, we also analyze the vulnerability of weighted networks in fallback strategy and compare them with their binary counterparts.

We need to assess the severity of different attacks on the networks. The most commonly used measure is the size of the residual giant that remains after each iteration. This part of the residual network adequately represents the connectivity information of the remaining network. But, as discussed in [21] this metric does not estimate the communication delays introduced into the system due to attacks. Attacks may destroy shorter communication paths, which will introduce communication delays between different parts of the network. Giant component size fails to represent these communication delays. Hence, following [21], we adopt severity measures based on average shortest path length and residual giant size in our study.

2. Preliminaries

In this study, we focus on undirected and weighted networks. N denotes network size (number of nodes/vertices) and M denote the number of link/edges in it.

Two nodes u and v are adjacent if there is an edge (u, v) joining u and v. Each edge (u, v) is associated with a weight, $w(u, v)$. A weight matrix representation $W = [w_{uv}]$ of the network is given by

$$w_{uv} = \begin{cases} w(u, v), & \text{if } u \text{ is adjacent to } v \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

The distance between two nodes u and v, denoted by d_{uv} is the sum of edge weights in a $u - v$ geodesic, provided the weight represents a spatial feature. In case the weight represents link strength, it is standard procedure to re-weight the links using inverse weights.

2.1. Centrality measures

Node centralities adequately measure the significance of a node in the network. There are many variants of centralities, depending on the criteria used for measuring node relevance.

2.1.1. Degree centrality

The degree centrality of a node v, for a given graph $G = (V, E)$ is defined as

$$DC_v = deg(v) \tag{2}$$

A related measure in weighted networks is the Strength Centrality SC (Node strength) which is calculated as total weights of edges incident on the node [29].

Degree centrality is a direct measure which gives insight into the connectivity or 'popularity' of a node. However, it fails to represent the relevance of node's position in overall network topology.

2.1.2. Betweenness centrality

This variant of centrality measures the significance of a node in enabling network communication. The betweenness centrality of a node is computed as the fraction of shortest paths going through it. This metric was introduced by Linton Freeman [30] as a measure of quantifying the control of a person(node) in the communication between other people in a social network. Freeman defined the betweenness centrality of a node v, BC_v as:

$$BC_v = \sum_{s \neq v \neq t} \frac{\sigma_{st}(v)}{\sigma_{st}} \tag{3}$$

where σ_{st} is the total number of shortest paths from node s to node t and $\sigma_{st}(v)$ is the number of those paths that pass through v.

In weighted networks, the length of a path is the sum of the edge-weights in it.

Removing a node with large betweenness centrality from the network may lengthen many geodesics in it. Therefore, betweenness centrality gives a direct measure for a node's potential to control network-flow.

2.1.3. Closeness centrality

The closeness centrality of a node v, CC_v, is defined as

$$CC_v = \frac{1}{\sum_u d(u, v)} \tag{4}$$

where $d(u, v)$ is the shortest distance between u and v.

A node with maximum closeness centrality is the one which require minimum intermediaries to contact all other nodes in the network. Thus CC_v gives an indirect measure of the time required to spread information from v to the entire network.

Newman [31] generalized the concept of closeness to weighted networks. He used Dijkstra's algorithm to find the shortest path in weighted networks.

The closeness centrality is not applicable for disconnected graphs.

2.1.4. Profile closeness centrality

Profile closeness is used to identify the nodes that are close to a particular set of nodes defined as a profile [21]. Let π denote the profile containing a set of nodes then the profile closeness of node u is defined as

$$PC_u(\pi) = \frac{1}{D_u(\pi)} \tag{5}$$

where $D_u(\pi) = \sum_{v=1}^{|\pi|} d_{uv}$.

A profile closeness center is a node with maximum PC_u. We denote the set of all such nodes as PC.

2.2. Node-removal attacks in complex networks

Complex networks are resilient towards node-removal attacks, if the target nodes are chosen at random. However, if an attacker can identify the perilous nodes in a network, and remove/damage them, then the robustness of the network may be compromised. This fragility of network owes to the criticality of the chosen attack targets [19,32,33]. Severity of such an attack depends on the minimum fraction of nodes to be removed for collapsing the entire network. Quite a few node-removal strategies has been suggested in literature [15,19,32,33]. In our work, we focus on the selecting the target nodes based on their centrality measures. We call such a node-removal strategy, a *central attack*.

2.2.1. Random attacks vs central attacks

In random attacks, the targets are selected randomly; while in central attacks, the attacker has to identify the most central nodes and attack them. A much effortless approach is to identify the nodes which have large number of connections (high-degree nodes) and remove them. This will leave the network crippled. [15,33] Nevertheless, betweenness centrality and closeness centrality were also proven to be highly effective in causing an expeditious destruction to the network [19,20,23,34].

2.2.2. Simultaneous attacks vs sequential attacks

In any central attack strategy, we need to catalog the nodes based on their centrality values. We can then choose the targets in the descending order of their values. First targets are the most central nodes. If the network is not collapsing after the first attack, we can continue attacking the nodes of lesser centrality, until the network is completely destroyed. This fashion of attacking the nodes in a pre-calculated order of their centrality values, is known as a simultaneous (initial) attack [15,19].

On the other hand, after each attack, the network topology may change and the centrality values will be updated. In such a scenario, the pre-calculated values of centrality may no longer remain valid. Here, we can recalculate the centrality of remaining nodes and regrade the targets. Such a strategy is known as a sequential (recalculated) attack strategy [19].

2.3. Network attributes

The important network attributes that are useful to characterize the behavior of network are mentioned below.

- *Average degree* of a network

$$\Delta = \frac{1}{N} \sum_{i=1}^{N} \delta_i \tag{6}$$

- *Local clustering coefficient* of a node is the ratio of the number of edges between its neighbors to the number of maximum possible edges between them [35]. Let n_i denote the number of neighbors of i and μ_i denote the number of edges between them. Then

$$\gamma_i = \frac{2\mu_i}{n_i(n_i - 1)} \tag{7}$$

- *Global clustering coefficient* of a network is the average of all γ_i-s [35].

$$\gamma = \frac{1}{N}\sum_{i=1}^{N}\gamma_i \tag{8}$$

2.4. Vulnerability measures

The effectiveness of an attack can be measured in various ways. In this work, we focus on the following metrics to compute the severity of an attack.

- *The fraction of nodes removed by k attacks*
  It is denoted as ρ_k and is defined as

$$\rho_k = \frac{R_k}{N} \tag{9}$$

  where R_k is the number of nodes removed by k attacks and N denote the total number of nodes The fraction of nodes to be removed to destruct the network completely is known as the *critical fraction*, $\rho_{critical}$. It is used to assess the vulnerability of the network towards attacks. [36–38]
- *Fraction of nodes in the giant component after k attacks:*
  It is defined as

$$\nu_k = \frac{G_k}{N} \tag{10}$$

  where G_k denotes size of the giant component in residual network after k attacks [26,36]
- *Diameter* of a network is the length of largest geodesic in it. Diameter is given by

$$\ell_{max} = \max_{i,j=1}^{N} d_{ij},\ i \neq j \tag{11}$$

  Diameter is a good measure of time delay in communication among nodes in a network [5,39,40]
- *Average shortest path length* of a network is given by [19]

$$\ell = \frac{1}{N(N-1)}\sum_{i=1}^{N}\sum_{j=1}^{N} d_{ij},\ i \neq j \tag{12}$$

  If ℓ is large, then the efficiency of information dissemination in the network is low. In social networks, $\ell \propto log(N)$ [41]. ℓ_k denotes the updated ℓ after kth attack.
- *Critical geodesic distance* $\ell_{critical}$ is the maximum value of average geodesic distance in the attacks. [21]

$$\ell_{critical} = \max_{k=1}^{T} \ell_k \tag{13}$$

- *Severity of an attack strategy*

$$\lambda = \frac{\ell_{critical} - \ell_{init}}{\ell_{init}} \tag{14}$$

  where ℓ_{init} is the ℓ of the original network and $\ell_{critical}$ is the ℓ at critical point. If $\lambda > 0$ then we call the attack k at which $\ell_k = \ell_{critical}$ as a critical attack [21].

3. Related literature

In this paper, we focus on *targeted node removal attacks in weighted networks*. A targeted attack can pose higher risks by compromising the network structure than a random attack [17,20,22,42]. The targets considered in our work are the network hubs based on centrality. As discussed earlier, centrality of a node determines its relevance in the entire network structure and behavior. Here, we use four centrality measures – Degree centrality, Betweenness centrality, Closeness centrality, Profile closeness centrality – in weighted as well as unweighted cases. We consider two types of attacks as well; simultaneous (initial) attacks and sequential (recalculated) attacks.

In 2000, Broder et al. [15] studied the impact of initial degree attack strategy(*ID* removal) on the resilience of web graphs. In the same year, Albert et al. [33] used recalculated degree attack(*RD* removal) to study the tolerance of scale-free networks. Later, Holme et al. [19] conducted a study on the vulnerability of real and synthetic networks based on recalculated betweenness centrality attack (*RD* removal) and compared it with the different attacking strategies like *ID*, *IB*, and *RD*. The sensitivity of the size of largest connected component is an important measure of vulnerability of network [7,43]. Nguyen et al. [23] suggested a modification on the classical recalculated betweenness centrality attacks by the condition that in every iteration it will consider the highest betweenness center in the largest connected component

(*LCC*) for removal. They analyzed the efficacy of these new criteria on various networks and found it is consistently efficient. Nie et al. [25] introduced a new metric combining degree centrality and betweenness centrality to select the targets of attack and observed that the efficiency of these strategies are higher than the traditional approaches. Comparison of attack strategies based on various centrality measures have been studied in [22,27,28,44,45].

Very recently, Lekha and Balakrishnan [21] introduced the *PC* attack (Profile closeness attack) in which the attack is performed on the nodes closer to the highly critical and (hence) protected nodes. The high profile nodes include degree centers and betweenness centers because they are the essential targets of node-removal attacks [27]. However, they investigated this attack strategy on unweighted networks. In our work, we extend this analysis to weighted networks. We experiment on both empirical and real-world networks with initial and recalculated attacks. Also, we compare the results in binary and weighted networks.

Most of the studies on network attacks in the last two decades were focused on binary models in which the link weights are either absent or ignored [46]. Bellingeri et al. [47,48] proved that neglecting the weighted structure of complex networks may produce misleading models to forecast the system's response to node failure. Hence the study on the robustness of weighted networks is very relevant. The impact of node removal attacks on weighted networks is studied in [49,50]. Nguis yen et al. [23] introduced a new nodes attack strategy removing nodes with the highest conditional weighted betweenness centrality (CondWBet).

Like the node removal attacks, link removal attacks also is a prominent area of research in complex networks. Studies on various strategies for link removal attacks can be found in [8,19,51].

Different metrics are used for the quantitative assessment of network vulnerability. The size of the giant residual component in the attacked network (*LCC*) [19,20,32], is the most prevalent measure. Another measure is average inverse geodesic length, ℓ^{-1}) [19], which was better named as network efficiency (*Eff*) [46,52]. While *LCC* is a simple indicator evaluating the binary-topological connectivity of network nodes, *Eff* uses the underlying link weights structure to account for the network information delivery rate in the network [24].

4. Methodology

We performed simulations of simultaneous and sequential attacks on synthetic and empirical networks. Twelve synthetic networks were constructed based on three network models, viz. random networks, small-world networks, and scale-free networks. Six real-world networks were also chosen for our study. We ran simulations of attacks on binary as well as weighted versions of these networks. Details of the network creation, network properties and simulations follow.

4.1. Construction of synthetic networks

We constructed random networks using the Erdös–Rényi model (E–R Model), small-world networks using the Watts–Strogatz model (W–S model) and scale-free networks using the Barabási–Albert model (B–A Model).

Since there are no default models that generate weighted network, we first generate binary networks with above mentioned models and then assigns a positive weight to each of its links based on some criteria. An analysis of various weighing approaches used in literature are discussed in [53].

In this paper we use two different strategies to assign weight for links in synthetic networks.

Method 1 Randomly assigning weights to the links.

Method 2 Clustering coefficient describes the tendency to form clusters. In our study, we consider the largest connected component as a parameter to measure the robustness of network. Hence, we adopt the weighing approach suggested by Zhu et al. [54] to use normalized clustering coefficient as a weighting scheme.

In this approach, for an edge (u,v) in $G = (V, E)$ the weight of (u, v),

$$w(u, v) = \frac{SCN_{(u,v)}}{(SN_u) \times (SN_v)} \tag{15}$$

where $SCN_{(u,v)}$ is the sum of the clustering coefficient of the common neighbors shared by u *and* v. SN_u, and SN_v denote the sum of the clustering coefficients of all the neighbors of u and v respectively.

In this calculation we found that many edges have turned up with zero weight which leads to confusion in the calculation of betweenness. So, a very small value was added to the w(u,v) to overcome this difficulty.

A summary of the network properties for unweighted and weighted networks generated (both methods) is shown in Appendix: Table 6, Tables 7 and 8.

4.2. Identification of empirical networks

We considered four empirical networks of different sizes whose characteristics are detailed below.

Game of Thrones co-appearances (GoT): Network of co appearances of characters in the Game of Thrones series, by George R. R. Martin, and in particular co appearances in the book "A Storm of Swords". Nodes are unique characters, and edges are weighted by the number of times the two characters' names appeared within 15 words of each other in the text [55].

Human brain functional coactivations (BR): A parameterizable consensus brain graph, derived from connectomes of 477 people, each computed from MRI datasets of the Human Connectome Project. Nodes are brain regions, and edges are weighted by the number of "tracks" that run between two nodes [56].

US airport network (US): Network of flights among the 500 busiest commercial airports in the United States, in 2002. Weights represent the number of seats available on the flights between a pair of airports [57]

Scientific collaborations in network science (SCN): A co-authorship network among scientists working on network science, from 2006. In this network, the scientists represents nodes and the times of co-authorships are taken as weight of the link [3]. This network is a one-mode projection from the bipartite graph of authors and their scientific publications [58].

Central Chilean power grid (CPW): The data set includes the connection structure of the real Central Chilean power grid. It includes the detailed attributes of each component of the power grid such as power plants, substations, towers, and taps that act as nodes and the transmission lines are the links. This network consist of 347 nodes(124 plants, 94 substations, 85 junctions (branch points), and 44 tap nodes) and 444 edges. The distance of transmission line is taken as the weight [59].

Messel Shale food web (MSFW): A network of feeling links among taxa based on the 48 million years old uppermost early Eocene Messel Shale. Here, edge weight denotes the certainty of the edge [60].

Appendix: Tables 9 and 10 summarizes the network properties — Number of nodes N, Size of largest connected component LCC, Average shortest path length ℓ, Diameter ℓ_{max}, Average degree Δ, and Average clustering coefficient γ - of unweighted and weighted empirical networks respectively.

The edge weights in five networks GoT, BR, US, SCN and MSFW, represent the link strength. As the link strength increases, the distance between the nodes connected by the link decreases. Hence, we consider the reciprocal edge weights as the distance for calculating the network properties and the weighted shortest path. An exception is the power grid network, CPW, where the edge weight represents the actual distance between nodes. Therefore, in the case of the CPW network, we used edge weight as the distance to calculate the weighted shortest path.

To avoid the anomaly, we normalized the distances by dividing them by the minimum distance so that the smallest normalized distance between any two nodes is one.

4.3. Performing initial attack

We perform random attacks by selecting the nodes randomly and removing them until the whole network break down. For central attacks, our strategy is to calculate degree/ betweenness/ closeness centrality based on which we rank the target nodes. For PC attacks, we consider the union of degree centers (DC) and betweenness centers (BC) as the profile and compute profile closeness for each node. Based on this value, we rank the target nodes.

$$\pi = BC \cup DC. \tag{16}$$

Once nodes are ranked, we perform initial attack (simultaneous attack) by removing them one-by-one from the network until the structure disintegrates completely. The response of each network to these attacks are plotted for comparison.

4.4. Performing recalculated attack

After each attack (node removal), the network undergoes structural changes. So the centrality values also change. In recalculated attacks (sequential attacks), we recalculate the centralities and re-rank the nodes after each attack. That is, the targets are revised after each iteration. Even though this strategy is more cost-consuming than simultaneous attack, it is more efficient and realistic. After performing the attacks, the severity of attack in each network is plotted and compared.

Table 1
Severity of simultaneous and sequential attacks on unweighted synthetic networks.

Synthetic networks	λ				
	BC	DC	CC	PC	Random
Erdos–Renyi (N = 1000)	0.002	0.097	0.005	0.571	0.002
	0.003	0.070	0.003	0.007	0.002
Erdos–Renyi (N = 500)	0.004	0.072	0.014	1.014	0.004
	0.004	0.041	0.006	0.025	0.004
Erdos–Renyi (N = 100)	0.020	0.088	0.088	1.639	0.020
	0.020	0.045	0.045	0.735	0.020
Erdos–Renyi (N = 50)	0.041	0.164	0.164	4.167	0.041
	0.042	0.116	0.112	2.174	0.041
Barabasi–Albert (N = 1000)	0.002	0.101	0.007	0.414	0.002
	0.002	0.031	0.003	0.016	0.002
Barabasi–Albert (N = 500)	0.004	0.141	0.014	0.541	0.004
	0.005	0.057	0.006	0.017	0.004
Barabasi–Albert (N = 100)	0.028	0.549	0.0425	0.193	0.023
	0.056	0.366	0.047	0.0516	0.024
Barabasi–Albert (N = 50)	0.090	0.485	0.068	0.202	0.077
	0.172	0.472	0.184	0.141	0.061
Newman–Watts–Strogatz (N = 1000)	0.005	0.032	0.004	1.034	0.002
	0.006	0.032	0.006	0.021	0.002
Newman–Watts–Strogatz (N = 500)	0.010	0.042	0.009	0.980	0.004
	0.012	0.042	0.012	0.032	0.005
Newman–Watts–Strogatz (N = 100)	0.038	0.094	0.04	1.449	0.021
	0.046	0.109	0.051	0.228	0.022
Newman–Watts–Strogatz (N = 50)	0.075	0.155	0.107	3.846	0.050
	0.097	0.182	0.098	1.923	0.047

Table 2
Severity of simultaneous and sequential attacks on weighted synthetic networks in which weight is assigned based on clustering coefficients.

Weighted synthetic networks	λ				
	BC	DC	CC	PC	Random
Erdos–Renyi (N = 1000)	0.002	0.002	0.002	0.144	0.002
	0.002	0.002	0.002	0.004	0.002
Erdos–Renyi (N = 500)	0.004	0.004	0.005	0.324	0.004
	0.004	0.004	0.004	0.013	0.004
Erdos–Renyi (N = 100)	0.027	0.027	0.041	0.510	0.022
	0.035	0.038	0.034	0.101	0.219
Erdos–Renyi (N = 50)	0.063	0.073	0.070	0.289	0.059
	0.117	0.108	0.086	0.120	0.055
Barabasi–Albert (N = 1000)	0.002	0.002	0.002	0.074	0.002
	0.002	0.002	0.002	0.004	0.002
Barabasi–Albert (N = 500)	0.004	0.004	0.004	0.091	0.004
	0.005	0.004	0.005	0.011	0.004
Barabasi–Albert (N = 100)	0.032	0.022	0.026	0.032	0.025
	0.052	0.026	0.048	0.072	0.025
Barabasi–Albert (N = 50)	0.082	0.072	0.080	0.205	0.083
	0.229	0.472	0.161	0.199	0.077
Newman–Watts–Strogatz (N = 1000)	0.004	0.004	0.004	0.255	0.002
	0.006	0.010	0.005	0.010	0.002
Newman–Watts–Strogatz (N = 500)	0.008	0.007	0.007	0.247	0.004
	0.012	0.014	0.009	0.024	0.004
Newman–Watts–Strogatz (N = 100)	0.032	0.028	0.031	0.238	0.021
	0.055	0.042	0.037	0.041	0.025
Newman–Watts–Strogatz (N = 50)	0.051	0.054	0.056	0.205	0.045
	0.079	0.074	0.0717	0.090	0.044

4.5. Severity checking

As discussed in Section 1, we tracked the updates on *LCC*, diameter ℓ_{max} and average shortest path length ℓ for every attack. We computed severity (λ) of attacks based on the changes in ℓ (Refer Eq. (14)). Tables 1–3 gives the comparison of λ values of central attacks on unweighted, random-weighted and clustering-based weighted networks respectively. First row for each network shows the values for simultaneous attacks and second row shows them for sequential attacks. Tables 4 and 5 gives the λ values of central attacks on weighted and unweighted empirical networks respectively.

Table 3
Severity of simultaneous and sequential attacks on randomly weighted synthetic networks.

Weighted synthetic networks	λ				
	BC	DC	CC	PC	Random
Erdos–Renyi (N = 1000)	0.0022	0.0020	0.0020	0.0024	0.0020
	0.002	0.002	0.002	0.007	0.002
Erdos–Renyi (N = 500)	0.0043	0.0041	0.0040	0.0052	0.0040
	0.004	0.004	0.004	0.013	0.004
Erdos–Renyi (N = 100)	0.0273	0.0295	0.0234	0.0279	0.0227
	0.035	0.034	0.031	0.045	0.023
Erdos–Renyi (N = 50)	0.076	0.075	0.058	0.054	0.054
	0.119	0.092	0.099	0.085	0.059
Barabasi–Albert (N = 1000)	0.0021	0.0020	0.0020	0.0022	0.0020
	0.0021	0.0020	0.0021	0.0095	0.0020
Barabasi–Albert (N = 500)	0.0043	0.0040	0.0040	0.0044	0.0041
	0.0046	0.0042	0.0044	0.0157	0.0040
Barabasi–Albert (N = 100)	0.0279	0.0248	0.0233	0.0232	0.0241
	0.0453	0.0305	0.0413	0.0571	0.0234
Barabasi–Albert (N = 50)	0.0916	0.0906	0.0608	0.0509	0.0765
	0.2959	0.1388	0.1724	0.2146	0.0746
Newman–Watts–Strogatz (N = 1000)	0.0037	0.0046	0.0025	0.0026	0.0022
	0.0061	0.0052	0.0058	0.0057	0.0022
Newman–Watts–Strogatz (N = 500)	0.0072	0.0094	0.0050	0.0048	0.0045
	0.0120	0.0106	0.0110	0.0096	0.0043
Newman–Watts–Strogatz (N = 100)	0.0337	0.0393	0.0258	0.0234	0.0223
	0.0519	0.0476	0.0452	0.0367	0.0210
Newman–Watts–Strogatz (N = 50)	0.0536	0.0671	0.0529	0.0469	0.0464
	0.0892	0.0794	0.0794	0.0499	0.0501

Table 4
Severity of simultaneous and sequential attacks on unweighted empirical networks.

Unweighted empirical networks	λ				
	BC	DC	CC	PC	Random
GoT Network (N = 107)	0.057	0.109	0.066	0.748	0.021
	0.090	0.107	0.083	0.314	0.022
BR NetWork (N = 480)	0.029	0.094	0.034	0.446	0.005
	0.092	0.096	0.080	0.293	0.005
US Network (N = 500)	0.026	0.039	0.021	1.016	0.005
	0.044	0.042	0.036	0.516	0.005
SCN Network (N = 1461)	0.265	0.489	0.115	1.047	0.038
	0.525	0.436	0.477	0.547	0.040
CPW Network (N = 347)	0.045	0.049	0.022	0.323	0.014
	0.133	0.266	0.104	0.198	0.012
MSFW Network (N = 700)	0.004	0.004	0.006	1.273	0.003
	0.006	0.019	0.006	0.066	0.003

Table 5
Severity of simultaneous and sequential attacks on weighted empirical networks.

Weighted empirical networks	λ				
	BC	DC	CC	PC	Random
GoT Network (N = 107)	0.07	0.064	0.038	0.026	0.020
	0.086	0.069	0.073	0.034	0.022
BR NetWork (N = 480)	0.022	0.042	0.023	0.025	0.006
	0.079	0.044	0.071	0.044	0.006
US Network (N = 500)	0.033	0.009	0.016	0.012	0.005
	0.038	0.013	0.022	0.011	0.005
SCN Network (N = 1461)	0.243	0.084	0.093	0.102	0.029
	0.433	0.171	0.332	0.236	0.037
CPW Network (N = 347)	0.038	0.022	0.013	0.008	0.018
	0.113	0.046	0.048	0.038	0.013
MSFW Network (N = 700)	0.004	0.004	0.004	0.188	0.003
	0.005	0.009	0.005	0.019	0.003

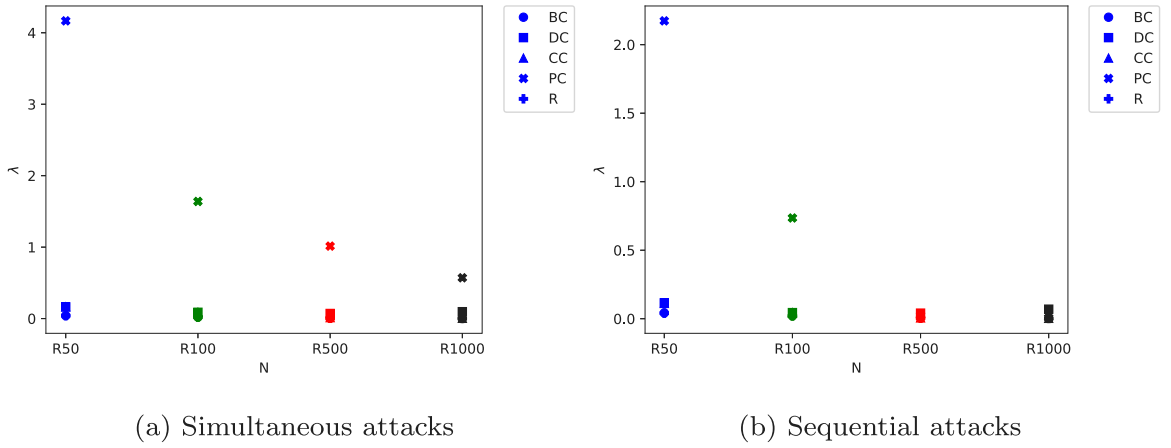


Fig. 1. Comparison of severity (λ) of different attack strategies in binary random networks of sizes 50, 100, 500 and 1000.

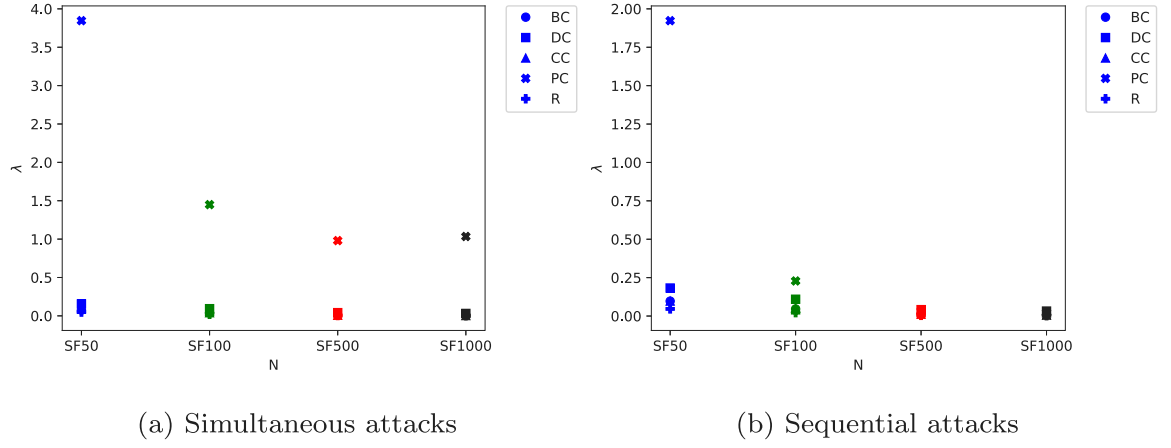


Fig. 2. Comparison of severity (λ) of different attack strategies in binary scale free networks of sizes 50, 100, 500 and 1000.

4.6. Results

This section investigates the effect of different attacks on the link-weighted networks and their binary equivalents.

4.6.1. Results in unweighted synthetic networks

Fig. 1 shows the severity of central attacks in different E–R networks. Figs. 1(a) and 1(b) show that *PC* attacks have higher λ values.

Fig. 2 shows attack severity in scale-free networks. Figs. 2(a) and 2(b) show that the λ severity is very high for *PC* attacks. Also, simultaneous attacks are more severe than sequential attacks.

Fig. 3 shows the severity of different central attacks in small world networks. Simultaneous *PC* attacks are shown to have high λ, and comparable to *DC* attacks (See Fig. 3(a)).

4.6.2. Results in random-weighted synthetic networks

Fig. 4 shows the severity of central attacks in different weighted E–R networks. Figs. 4(a) and 4(b) show that *PC* attacks have higher λ values. BC& DC attack also prominent in sequential attacks. *PC* attacks are severe in sequential case.

Fig. 5 shows attack severity in weighted scale-free networks. Figs. 5(a) shows that the λ severity is very high for *DC* attacks in simultaneous case. In the case of sequential attacks also, *BC* attack was found to be hazardous.

Fig. 6 shows attack severity in weighted small world networks. In simultaneous λ severity is almost same for all attacks in networks of higher size . Also *BC* attacks also has prominence in some networks. See Fig. 6(a). And, severity of sequential *PC* attacks is only slightly higher than its *BC*/ *DC* counterparts.

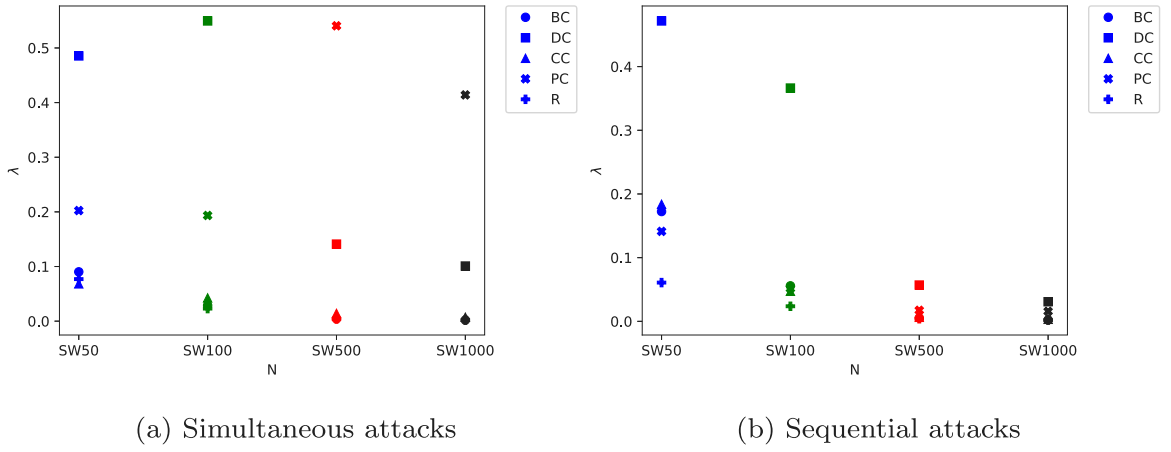


Fig. 3. Comparison of severity (λ) of different attack strategies in binary small world networks of sizes 50, 100, 500 and 1000.

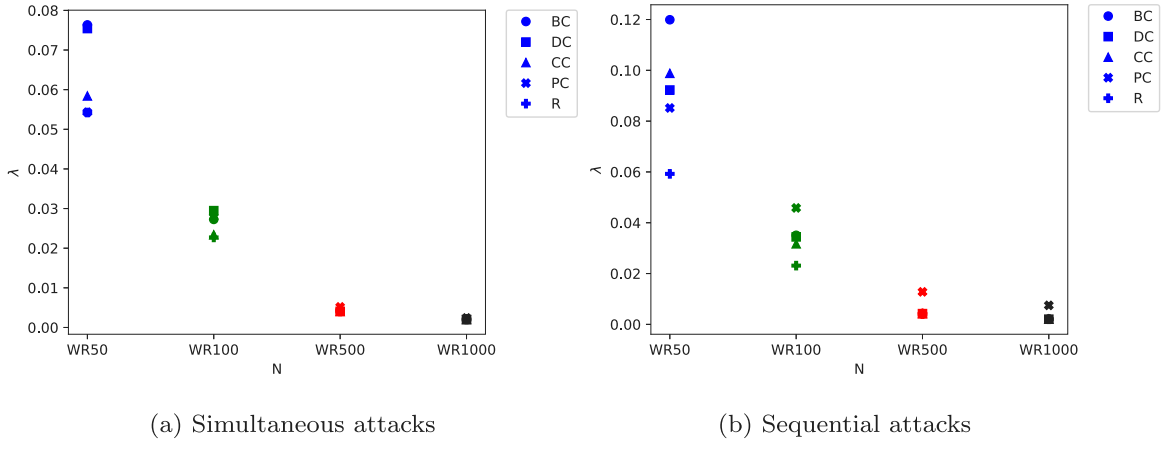


Fig. 4. Comparison of severity (λ) of different attack strategies in random-weighted E–R networks of sizes 50, 100, 500 and 1000.

4.6.3. Results in clustering-weighted synthetic networks

Fig. 7 shows the severity of central attacks in different weighted E–R networks. Figs. 7(a) and 7(b) show that *PC* attacks have higher λ values. BC& DC attack also prominent in sequential attacks. *PC* attacks are severe in simultaneous case.

Fig. 8 shows attack severity in weighted scale-free networks. Figs. 8(a) shows that the λ severity is very high for *PC* attacks in simultaneous case. In the case of sequential attacks also, *PC* attack was found to be hazardous. However, *BC* and *DC* attacks were also having comparable effect in some networks.

Fig. 9 shows attack severity in weighted small world networks. λ severity of simultaneous *PC* attacks is very high in these networks. See Fig. 9(a). And, severity of sequential *PC* attacks is only slightly higher than its *BC*/ *DC* counterparts. This result is similar to what we have observed in weighted scale-free networks.

4.6.4. Results in real networks

Fig. 10 shows the severity of different central attacks in real world networks. We can see that the severity of both simultaneous and sequential *PC* attacks is very high.

Unlike in synthetic networks, *CC* attacks show considerable effect on weighted real-world networks. See Fig. 11. *BC* attack is most hazardous among the sequential/ recalculated attacks. See Fig. 11(b).

5. Analysis and discussion

We simulated simultaneous and sequential attacks on networks based on three network centralities, viz. degree (DC), betweenness (BC) and closeness (CC) centralities, and a different centrality approach known as profile closeness (PC). We

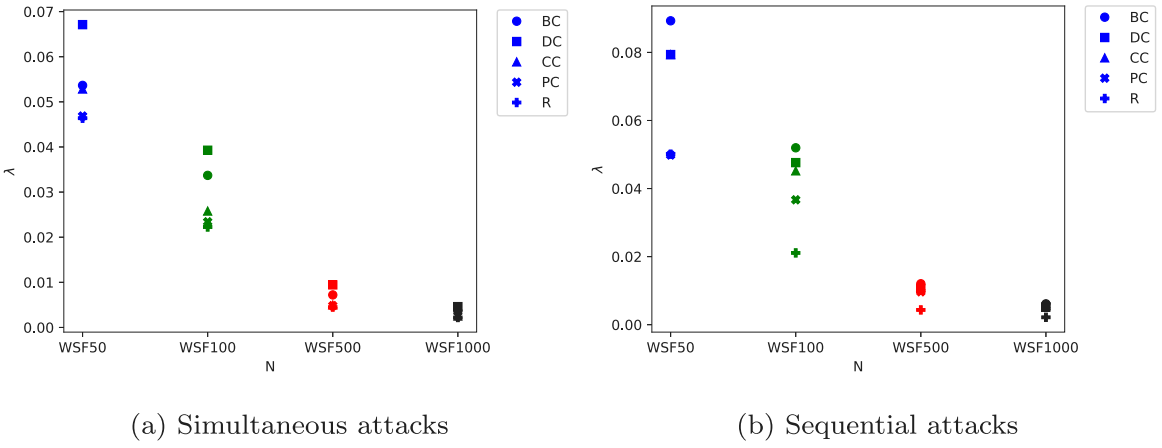


Fig. 5. Comparison of severity (λ) of different attack strategies in random-weighted scale free networks of sizes 50, 100, 500 and 1000.

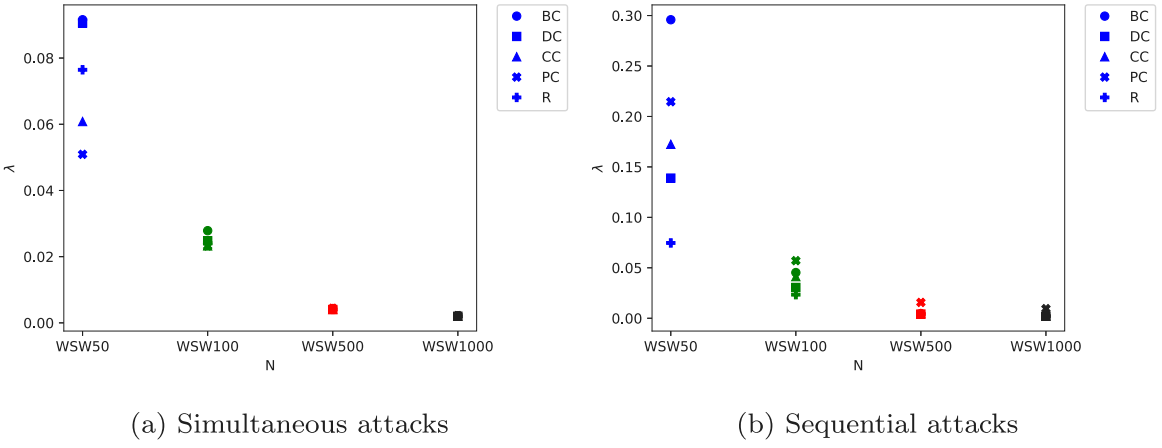
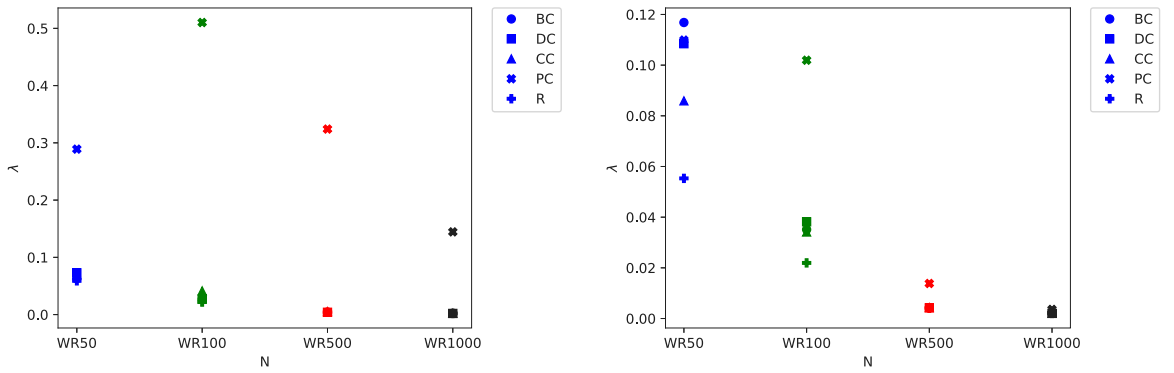


Fig. 6. Comparison of severity (λ) of different attack strategies in random-weighted small world networks of sizes 50, 100, 500 and 1000.

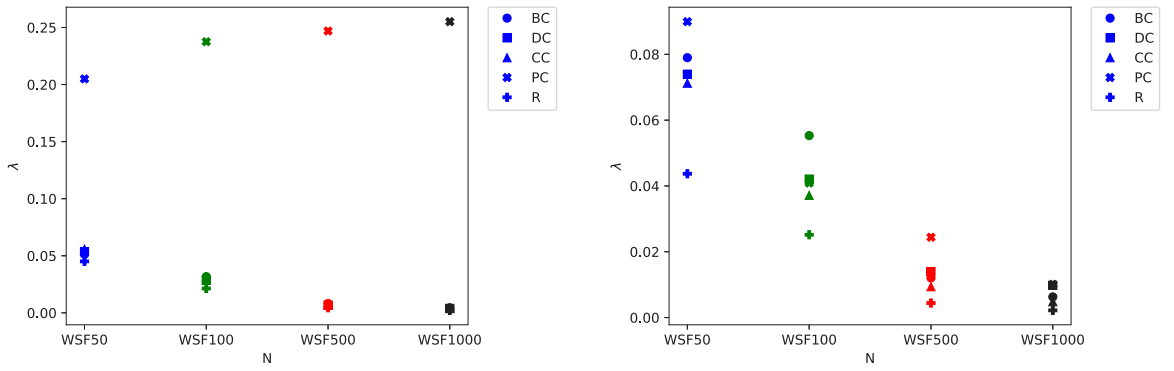
observed two network properties, the disintegration of giant components and updates in the average geodesic distance, to assess the severity of attacks. Our major findings based on the results of simulations are as follows:

- **Relevance of CC attacks in weighted networks:** BC and DC-based attacks are the most hazardous when the severity of attack is measured on the basis of *LCC*, a topological property. But, if the severity is computed based on the average geodesic distance, the CC-based attacks found to be equally relevant. We show that sequential attacks based on CC are effective in crippling link-weighted networks. This observation indicates that a *CC* attack can induce delayed communications into the network system and hence cripple the coordination within obnoxious networks like terrorist networks.
- **Fallback strategy in protected, weighted networks:** When the critical nodes (nodes with high BC and DC) in the network are protected, we show that the fallback strategy based on profile closeness is indeed a reasonable approach for attacking protected, link-weighted networks. When *PC* attacks were introduced in [21], it was established that this strategy is better when the most critical parts (*BC*, *DC*) of a binary network are protected. In our work, we experimented similar attacks on weighted networks. Here also, similar results were observed in the case of simultaneous attacks. But, in the case of sequential attacks, the severity of *PC* attack is only comparable to that of *BC* and *DC* attacks.
- **Significance of simultaneous PC attacks:** From literature, we know that recalculated attacks are more realistic and have severe effect on networks than initial attacks. But, from our results (see Fig. 12), this is not true in the case of PC-based attacks.



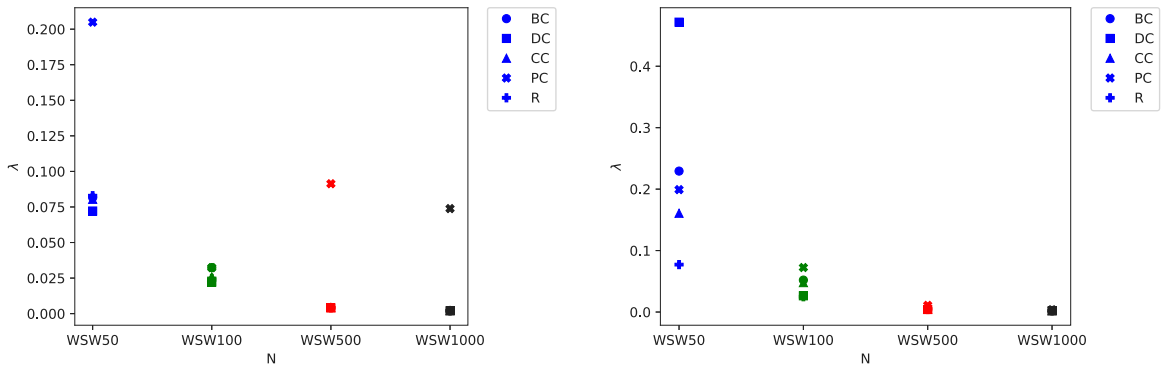
(a) Simultaneous attacks (b) Sequential attacks

Fig. 7. Comparison of severity (λ) of different attack strategies in clustering-weighted random networks of sizes 50, 100, 500 and 1000.



(a) Simultaneous attacks (b) Sequential attacks

Fig. 8. Comparison of severity (λ) of different attack strategies in clustering-weighted Scale Free networks of sizes 50, 100, 500 and 1000.



(a) Simultaneous attacks (b) Sequential attacks

Fig. 9. Comparison of severity (λ) of different attack strategies in clustering-weighted small world networks of sizes 50, 100, 500 and 1000.

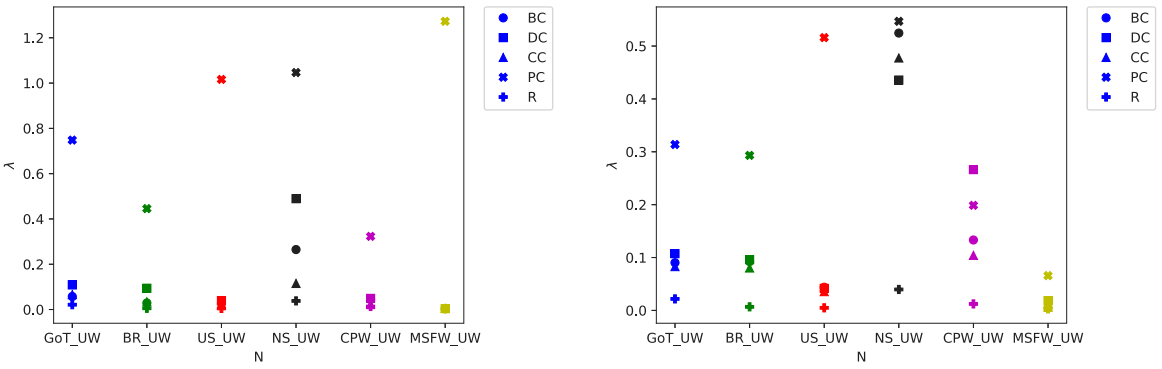


Fig. 10. Comparison of severity (λ) of different attack strategies in 6 different binary real world networks.

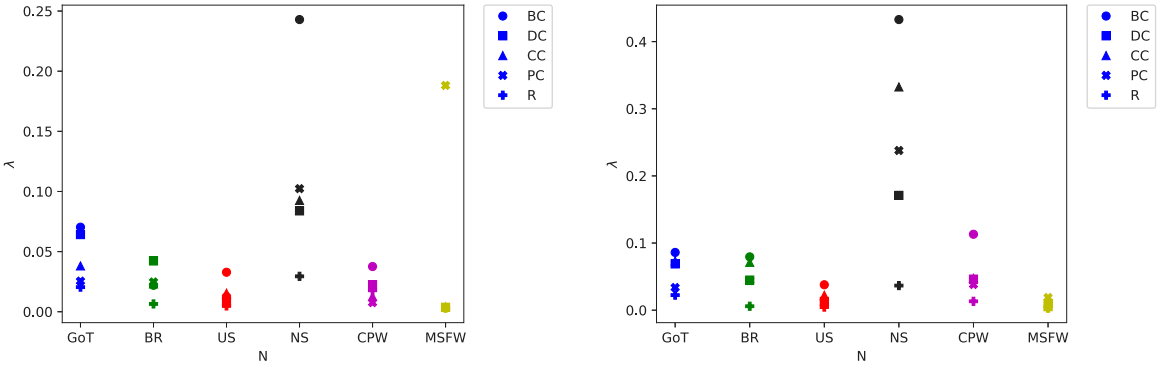


Fig. 11. Comparison of severity (λ) of different attack strategies in weighted real world networks.

In PC-attacks, we are considering our targets as the nodes having more access to a prominent fraction (here, BC and DC of network) of the network. This prominent fraction of nodes also change in each iteration of attack. So we need to re-identify the high-profile nodes and recompute the closeness to this set of nodes to find our targets in each iteration. However, after each iteration the connectivity of remaining network will be lesser and hence finding the nodes closer to the high-profile ones will not be relevant. Hence, we cannot assume that PC attacks behave in the same manner as other central attack strategies.

However, this behavior happens to be advantageous since the recalculated PC attacks are very costly to execute. So, simultaneous PC attack is a better choice when we need to impart maximum destruction to a protected network and when we have difficulty in accessing network information after an attempt of attack. This can be considered as equivalent to a one-time effort on attempting attacks on a protected network.

- **Extrapolating results from network models:** Another prime observation is that *CC* attacks were not having considerable effect in the case of weighted synthetic networks. See Appendix: Figs. 13, 14, 15, and 16. On the contrary, *CC* attacks were found to be instrumental in increasing the geodesics in weighted real-world networks. See Appendix: Figs. 19, 20, 21, and 22. This inconsistency in results demonstrates that the study on synthetic network models alone cannot be generalized to give an adequate representation of real-world systems.
- **Dependence of attack severity on link weights:** In weighted networks where weight is a direct measure of the connectivity, as in GoT, BR, NS and CPW networks, different strategies have highly varying severity. If the weight is not a direct measure of connectivity, as in US and MSFW networks, the severity is almost same irrespective of the strategy adopted.

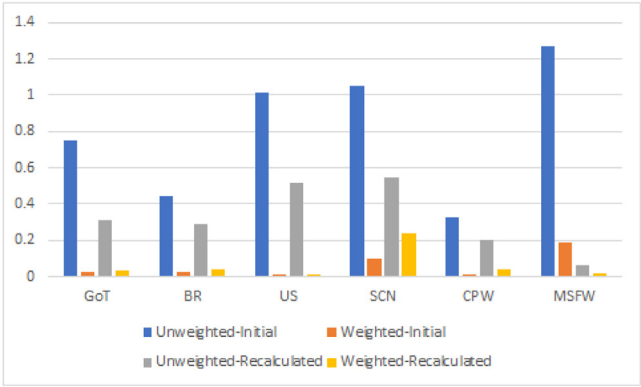


Fig. 12. Comparison of severity (λ) of initial and recalculated PC attacks in unweighted and weighted real world networks.

6. Summary

Identifying the most influential components (nodes or links) of a network is vital for its analysis. An attack on these components may alter the entire network structure. However, the impact of destructing different parts varies with their influence on the network as a whole. Centrality is a network notion which can measure this influence. There are different types of centrality measures.

The study of centrality-based attacks remains relevant in many application-areas like epidemic spreading, terrorist communication network, and fake news alerts. Pertinent many studies are centered on the connectivity between different network entities. However, a more sensible approach is to include all relevant details about the entity relationships. Edge-weighted networks are thus more realistic representations for real-world systems.

We analyzed the relevance of central attacks and a fallback attack strategy in weighted networks. We calculated the severity of attacks based on average geodesics since this measure gives information about the communication delays that can be implanted into a system. Using this metric, we established the relevance of sequential CC attacks in weighted networks. Also, we state that the fallback approach is suitable for protected weighted networks as a one-time attack strategy.

CRediT authorship contribution statement

Divya P.B.: Conceptualization, Investigation, Methodology, Visualization, Writing – original draft, Writing – review and editing. **Divya Sindhu Lekha:** Conceptualization, Investigation, Methodology, Visualization, Writing – original draft, Writing – review and editing. **T.P. Johnson:** Supervision, Validation. **Kannan Balakrishnan:** Conceptualization, Investigation, Methodology, Supervision, Validation, Writing – review and editing.

Declaration of competing interest

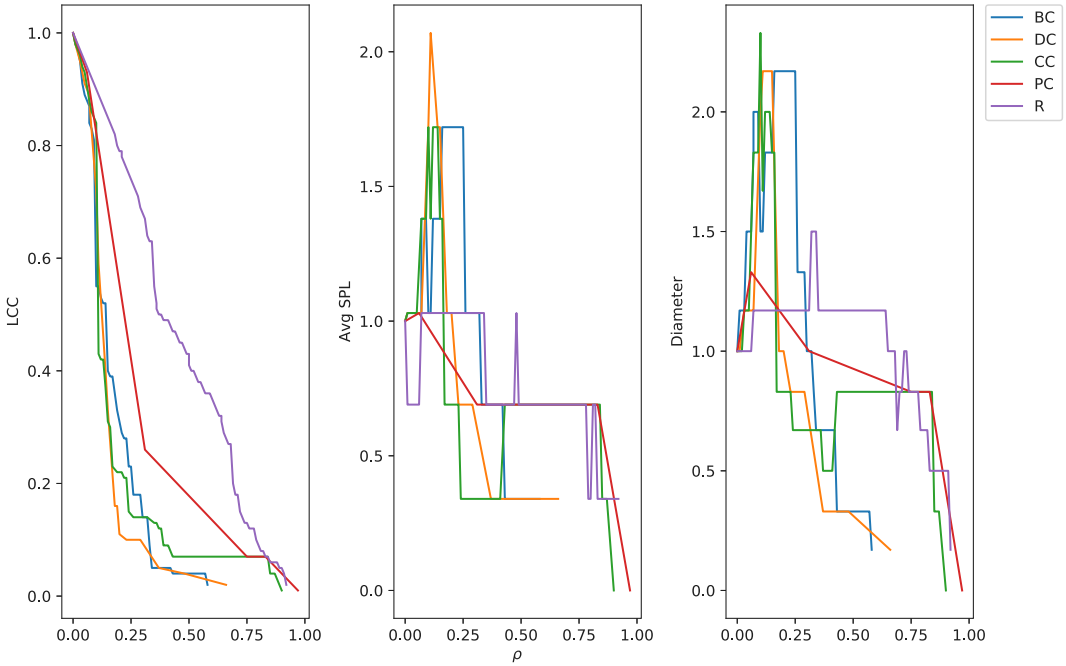
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgment

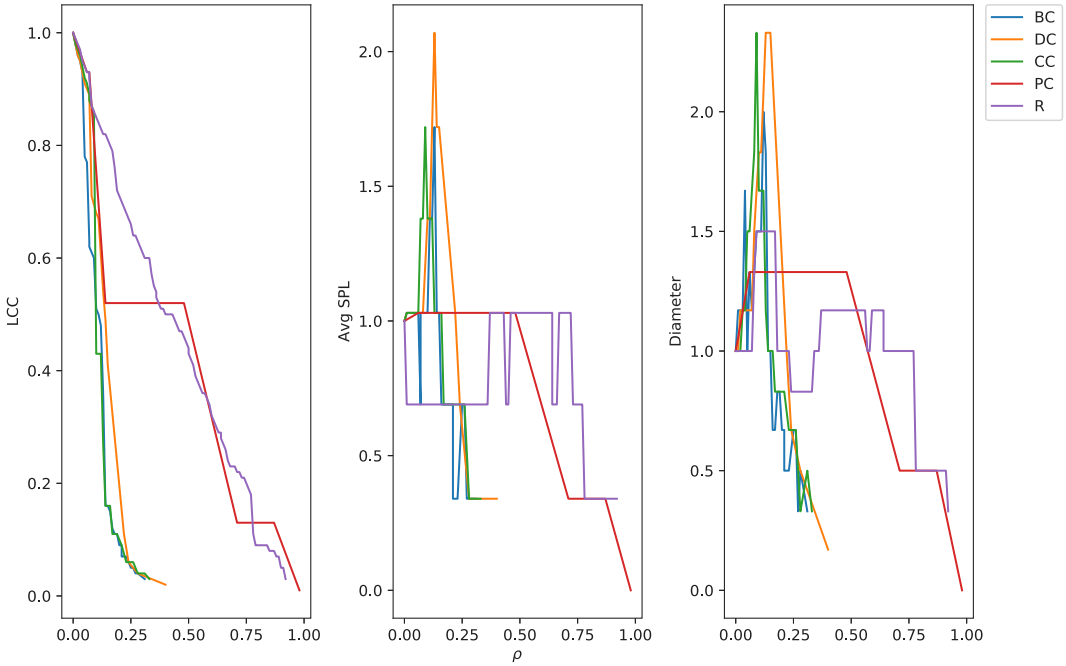
This work was partially supported by the post doctoral fellowship from Cochin University of Science and Technology, 2019–2020.

Appendix

See Tables 6–10 and Figs. 13–24.

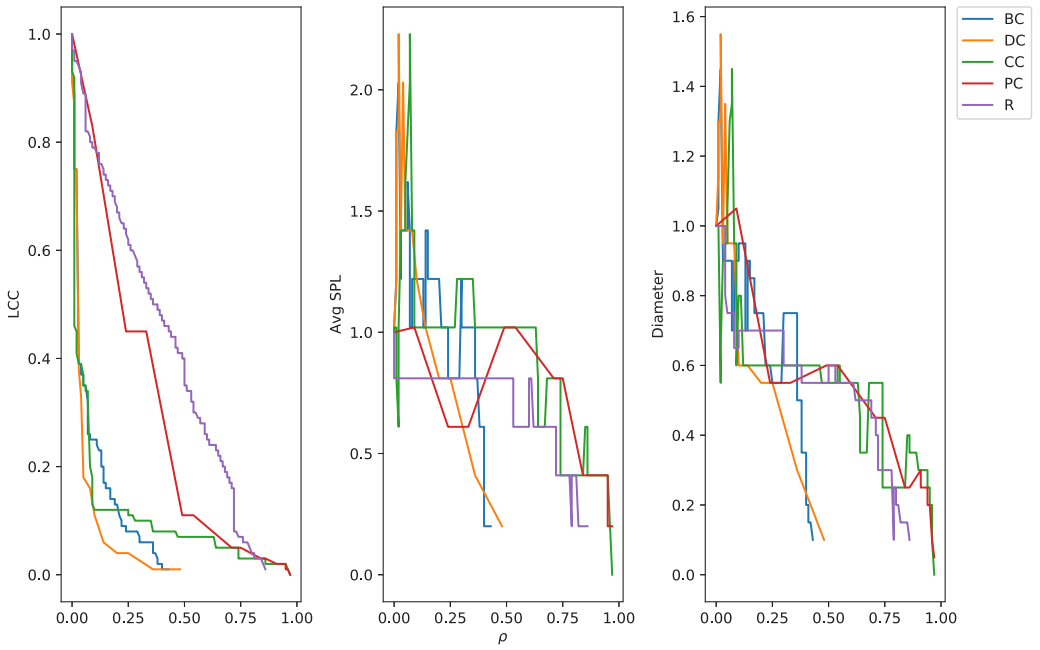


(a) Simultaneous central attacks

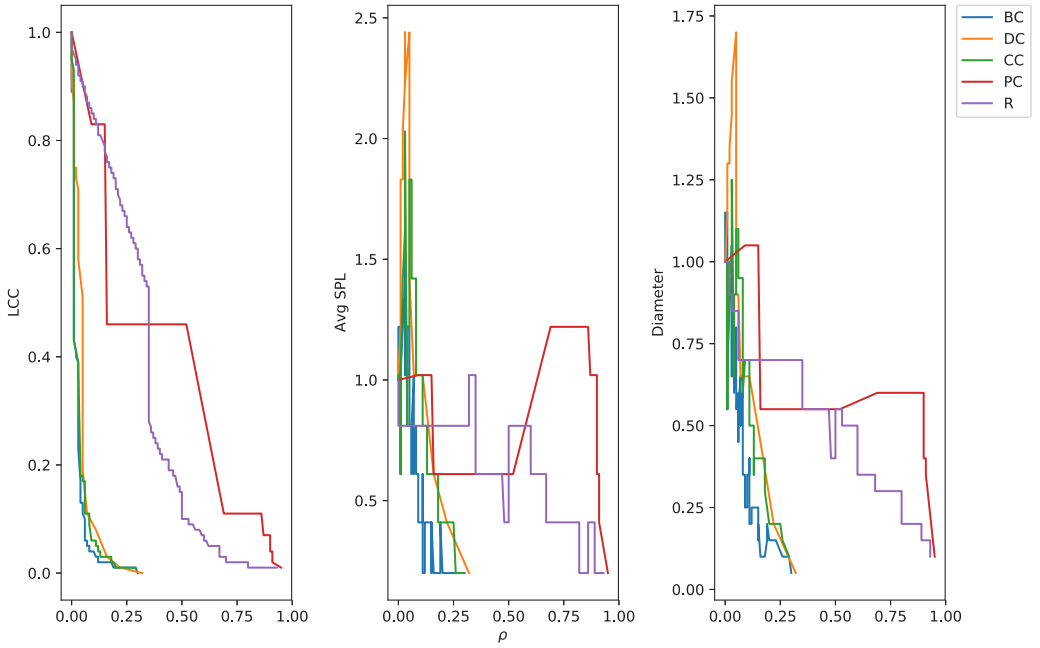


(b) Sequential central attacks

Fig. 13. Comparison of updates in LCC, average shortest path length and diameter against ρ, fraction of nodes removed, in central attacks on unweighted *Game of Thrones co appearances Network*.

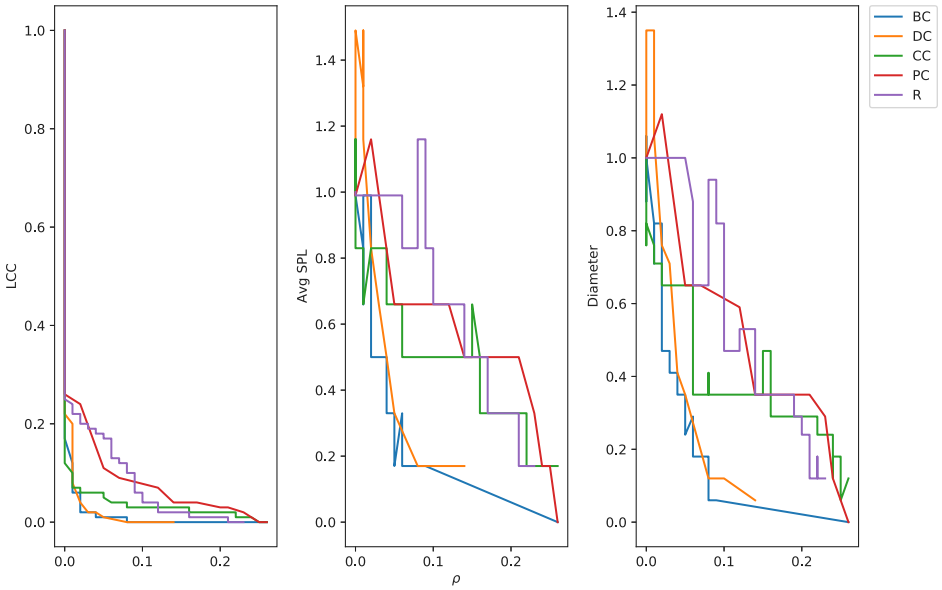


(a) Simultaneous central attacks

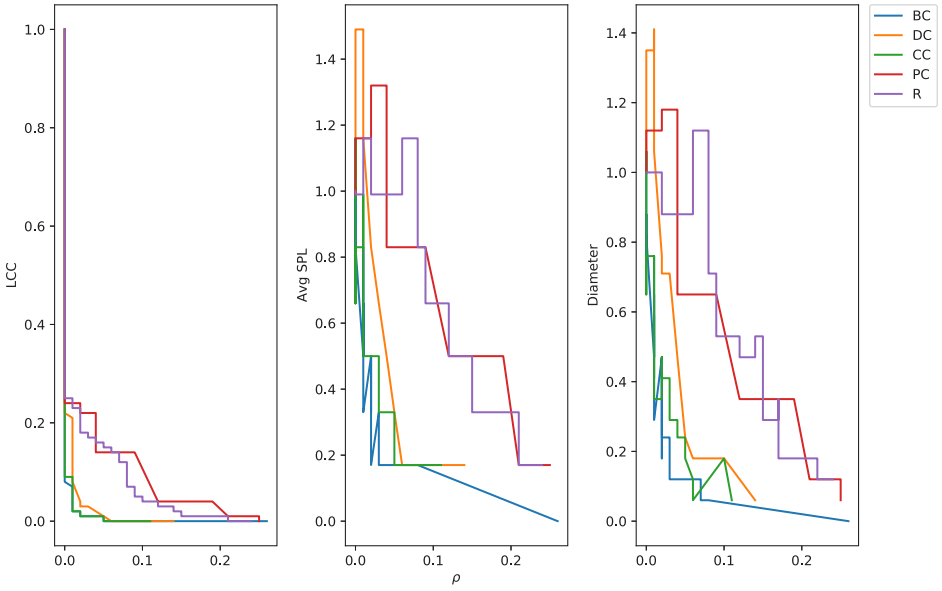


(b) Sequential central attacks

Fig. 14. Comparison of updates in LCC, average shortest path length and diameter against ρ, fraction of nodes removed, in central attacks on unweighted *Brain network*.

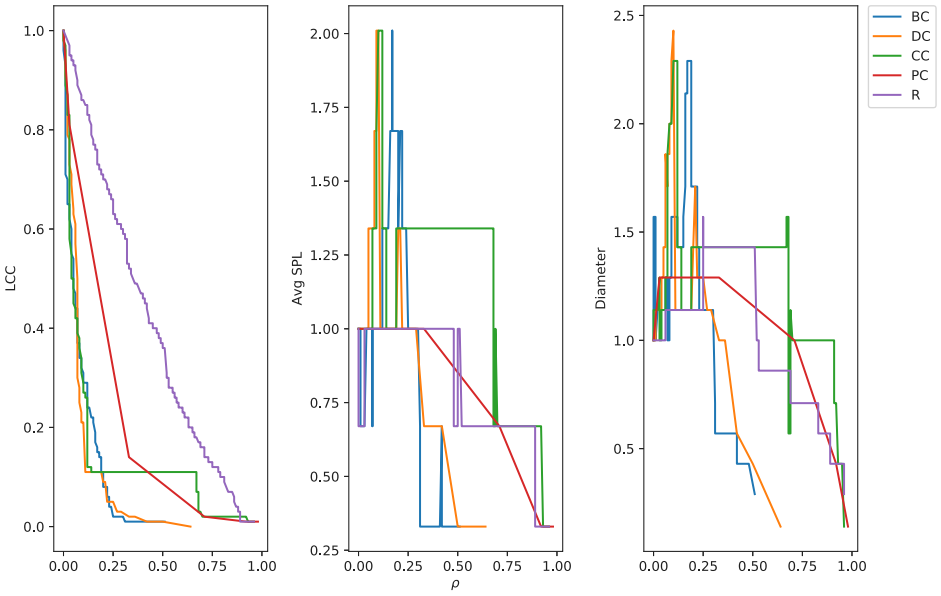


(a) Simultaneous central attacks

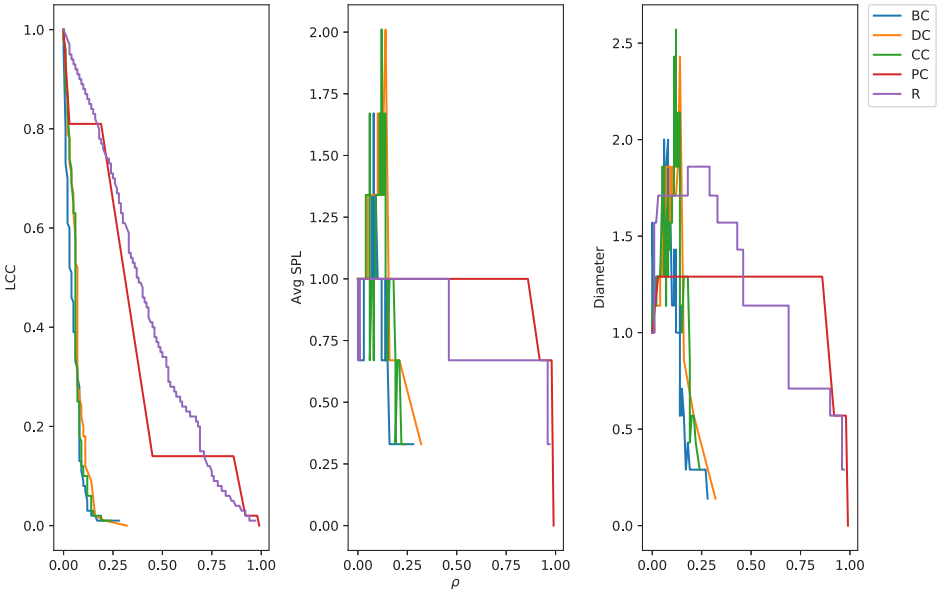


(b) Sequential central attacks

Fig. 15. Comparison of updates in LCC, average shortest path length and diameter against ρ, fraction of nodes removed, in central attacks on unweighted *Scientific Collaborations in Network Science*.

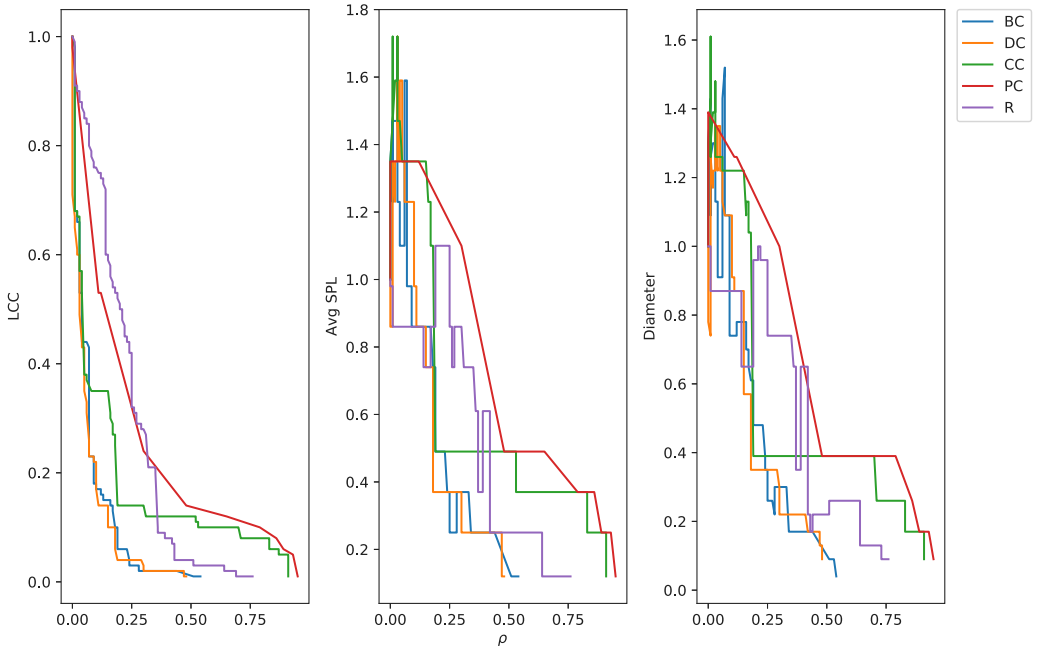


(a) Simultaneous central attacks

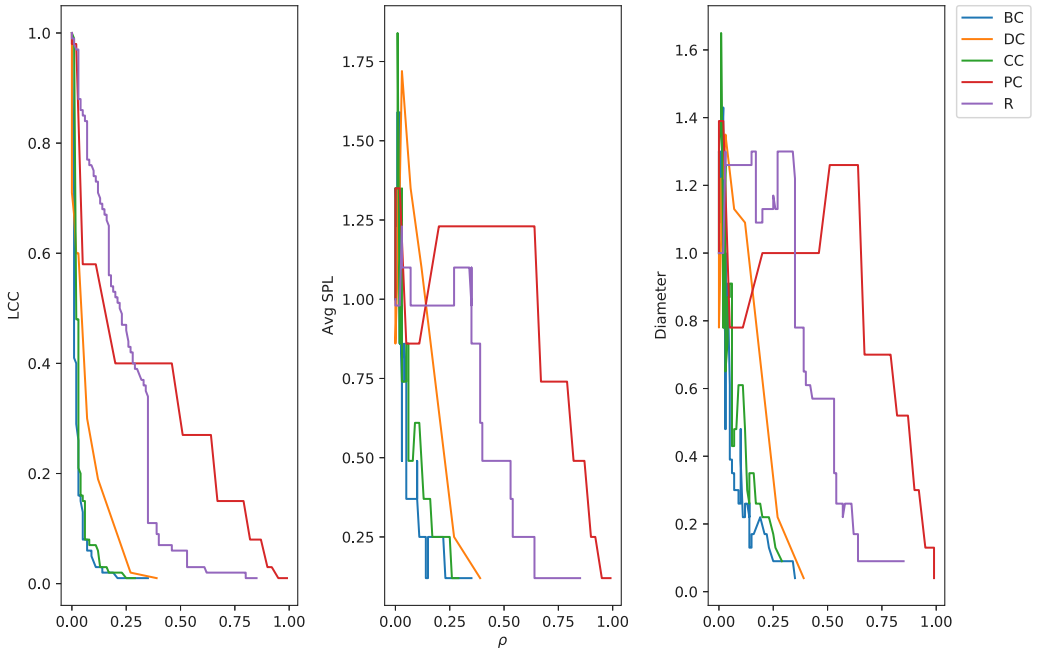


(b) Sequential central attacks

Fig. 16. Comparison of updates in LCC, average shortest path length and diameter against ρ, fraction of nodes removed, in central attacks on unweighted *US Airport network*.

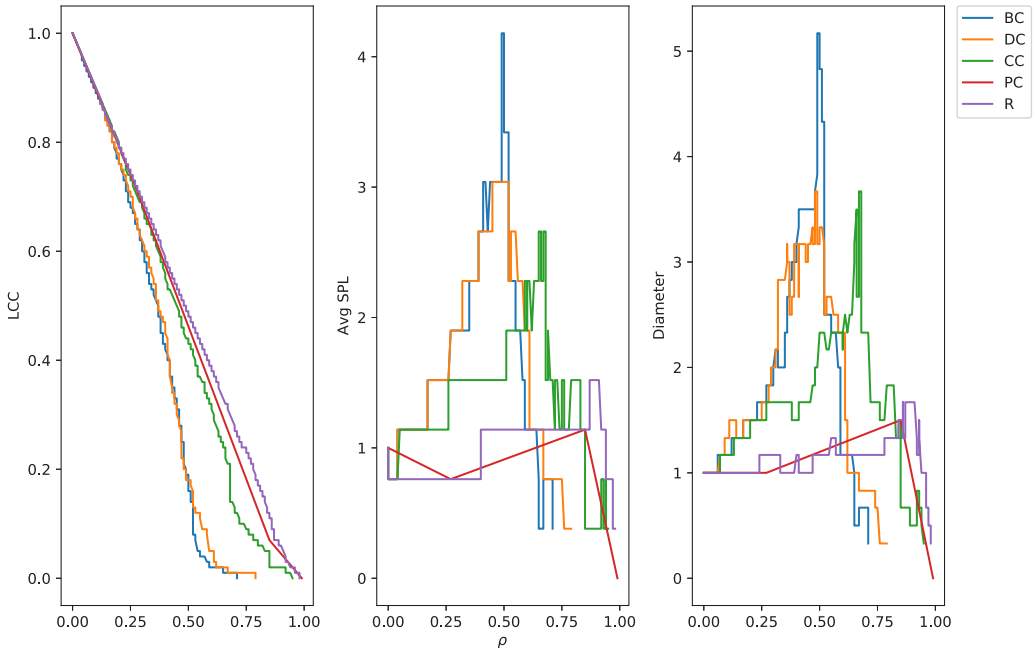


(a) Simultaneous central attacks

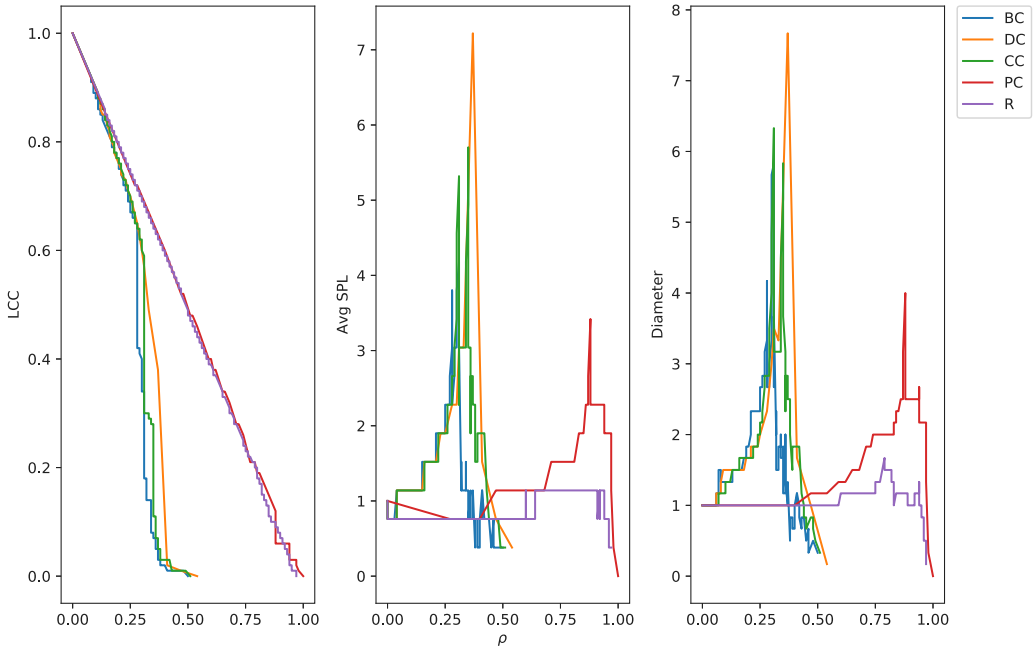


(b) Sequential central attacks

Fig. 17. Comparison of updates in LCC, average shortest path length and diameter against ρ, fraction of nodes removed, in central attacks on unweighted *Central Chilean Power Grid (CPW) network*.

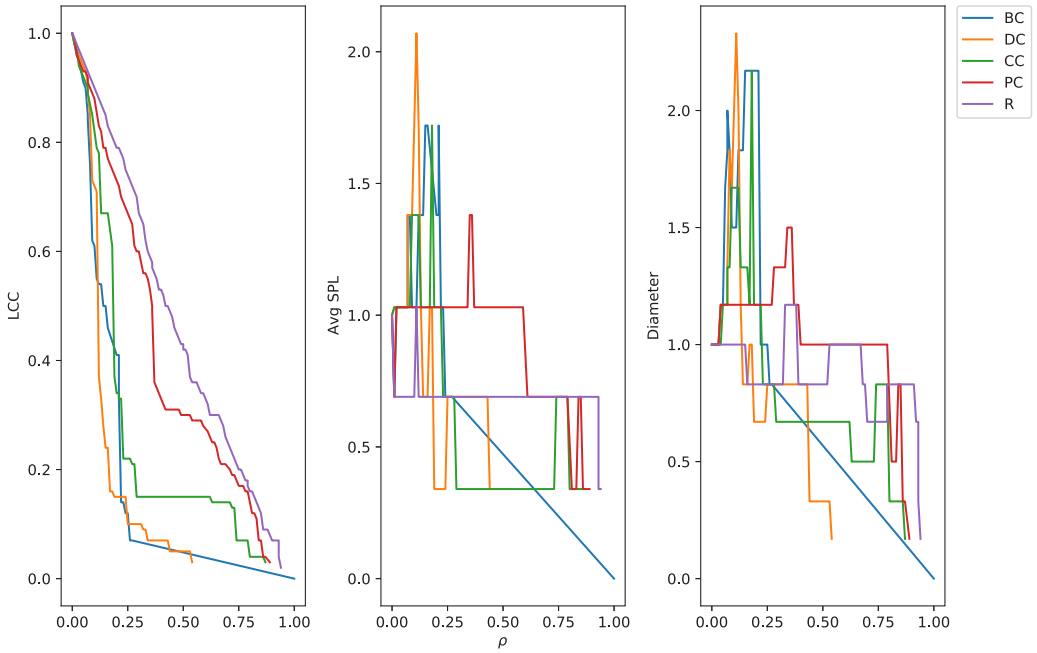


(a) Simultaneous central attacks

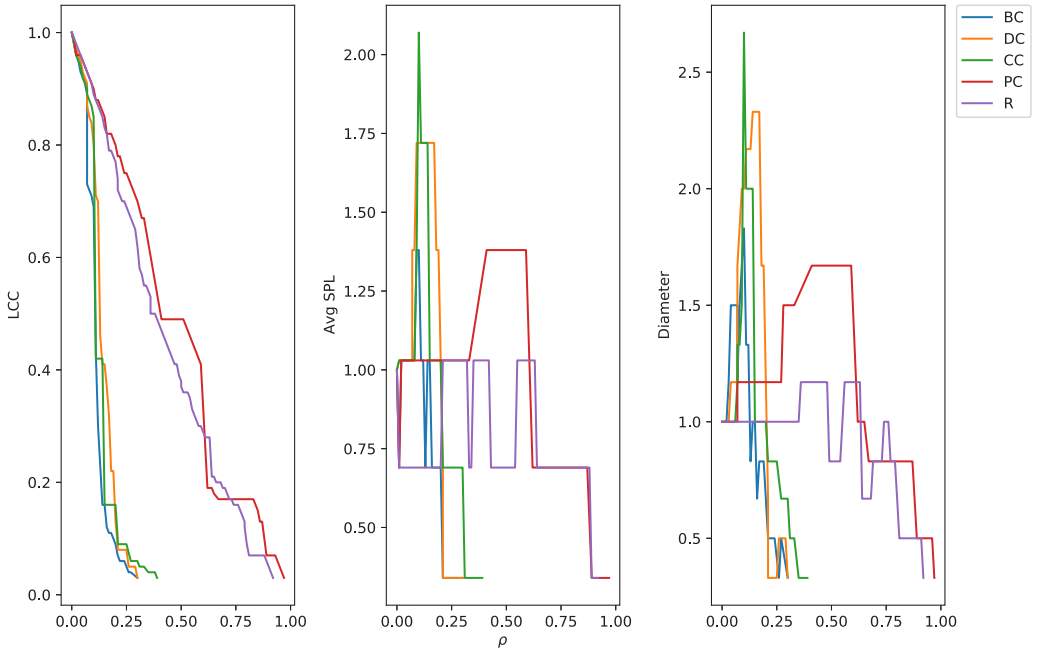


(b) Sequential central attacks

Fig. 18. Comparison of updates in LCC, average shortest path length and diameter against ρ, fraction of nodes removed, in central attacks on unweighted *Messel Shale Food Web (MSFW) network*.

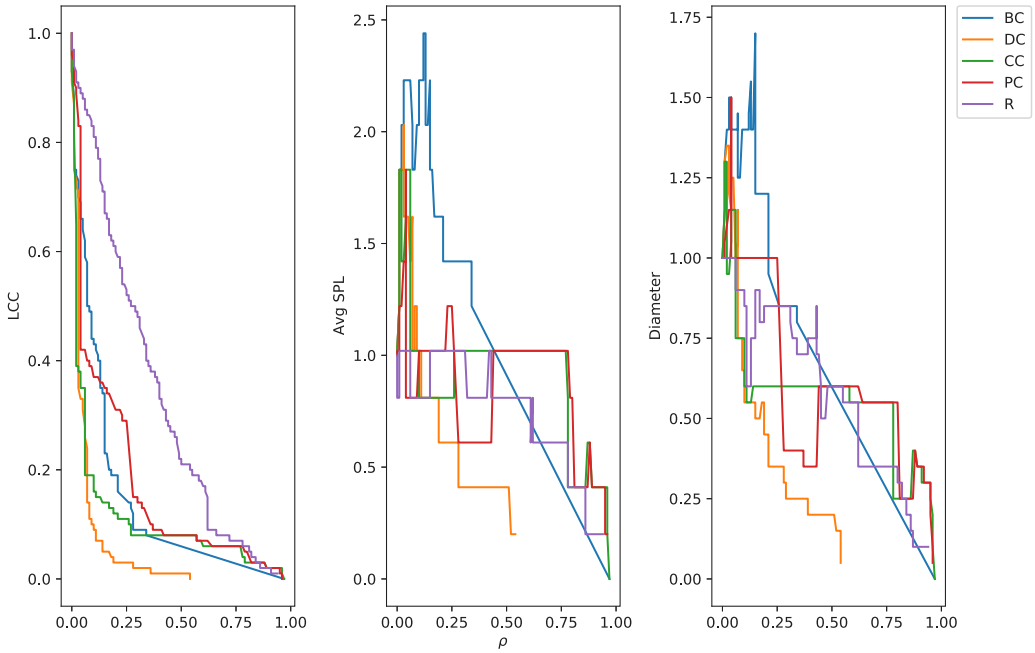


(a) Simultaneous central attacks

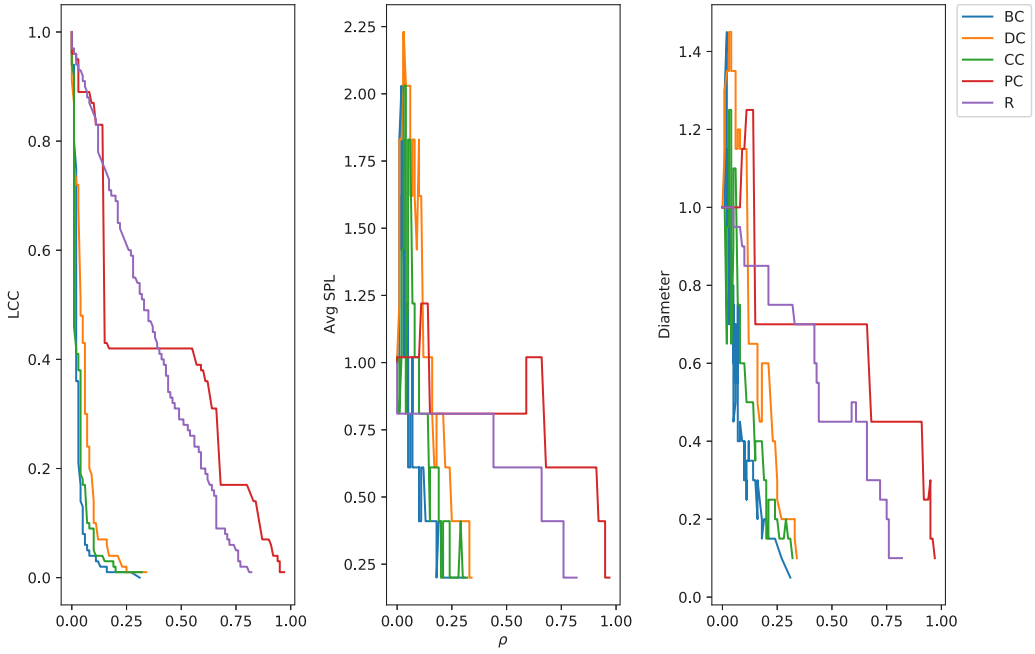


(b) Sequential central attacks

Fig. 19. Comparison of updates in LCC, average shortest path length and diameter against ρ, fraction of nodes removed, in central attacks on weighted *Game of Thrones co appearances Network*.

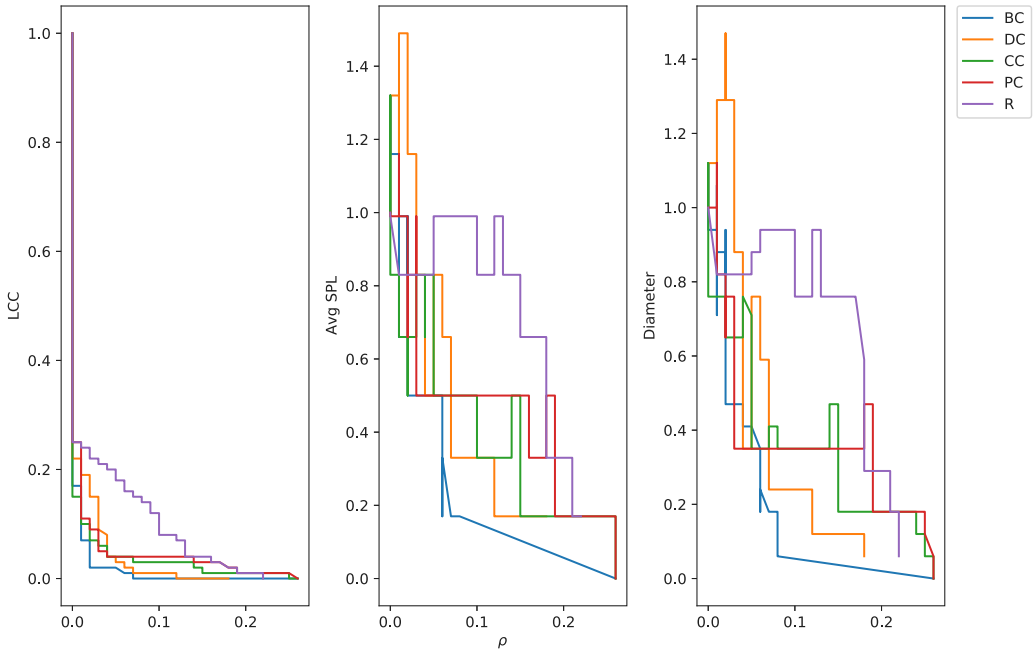


(a) Simultaneous central attacks

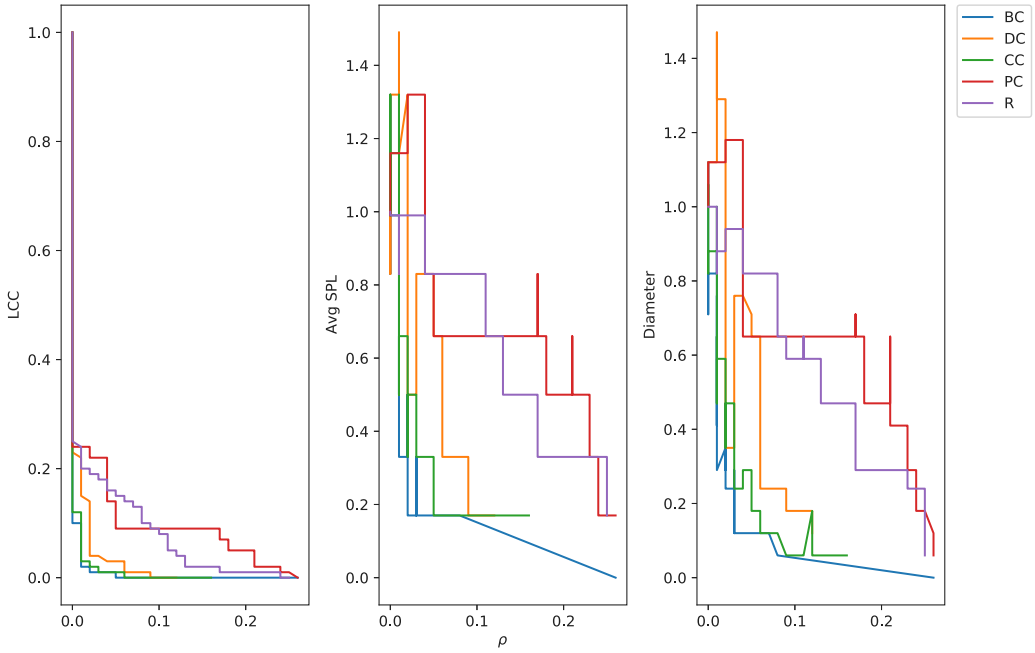


(b) Sequential central attacks

Fig. 20. Comparison of updates in LCC, average shortest path length and diameter against ρ, fraction of nodes removed, in central attacks on weighted *Brain network*.

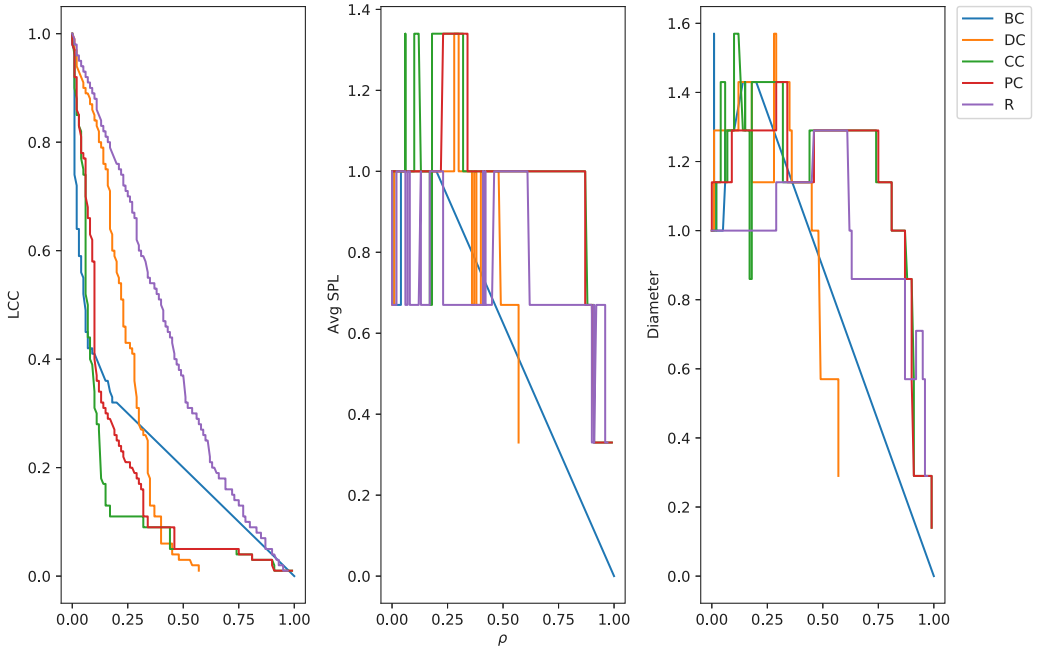


(a) Simultaneous central attacks

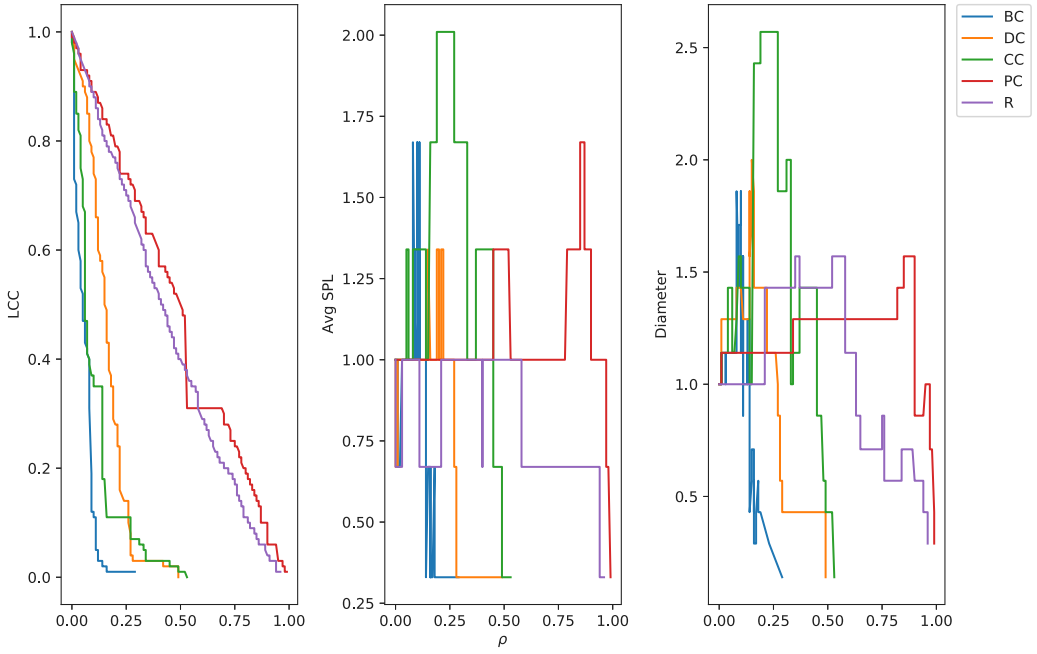


(b) Sequential central attacks

Fig. 21. Comparison of updates in LCC, average shortest path length and diameter against ρ, fraction of nodes removed, in central attacks on weighted *Scientific Collaborations in Network Science*.

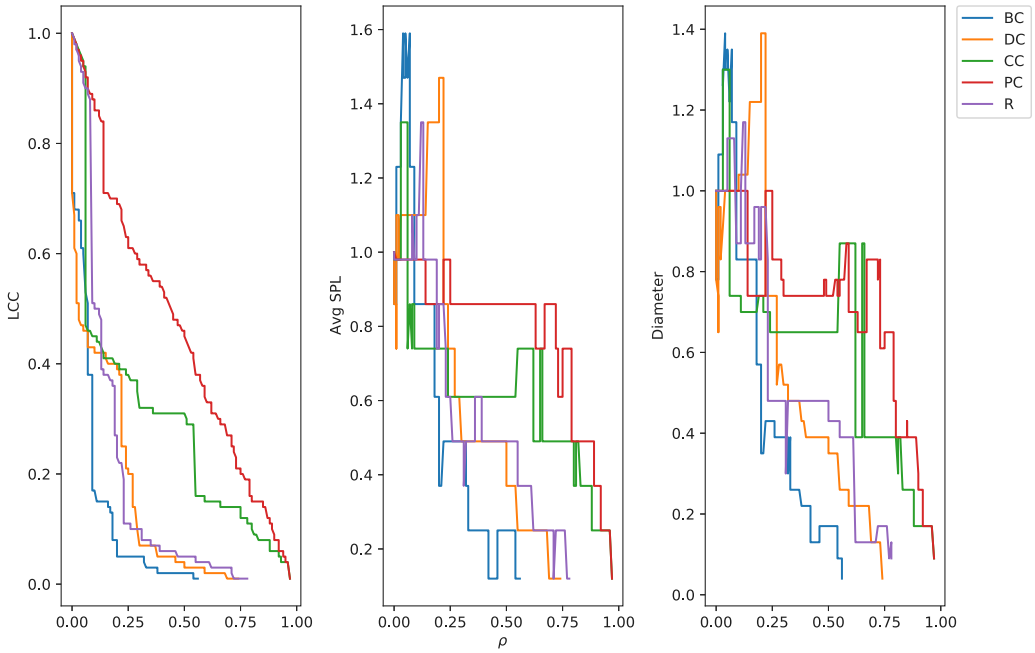


(a) Simultaneous central attacks

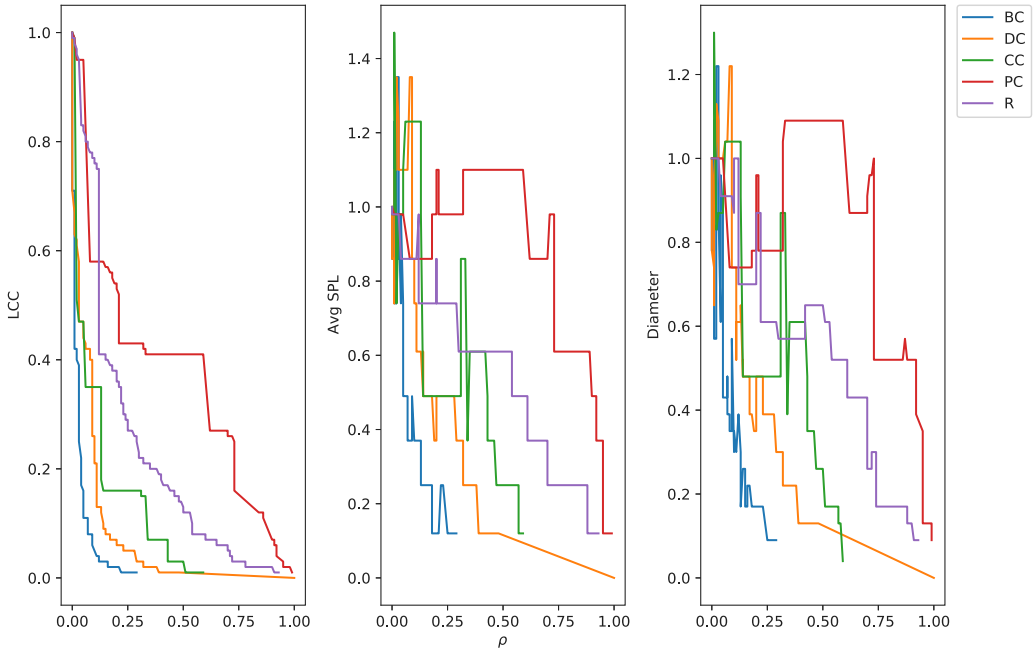


(b) Sequential central attacks

Fig. 22. Comparison of updates in LCC, average shortest path length and diameter against ρ, fraction of nodes removed, in central attacks on weighted *US Airport network*.

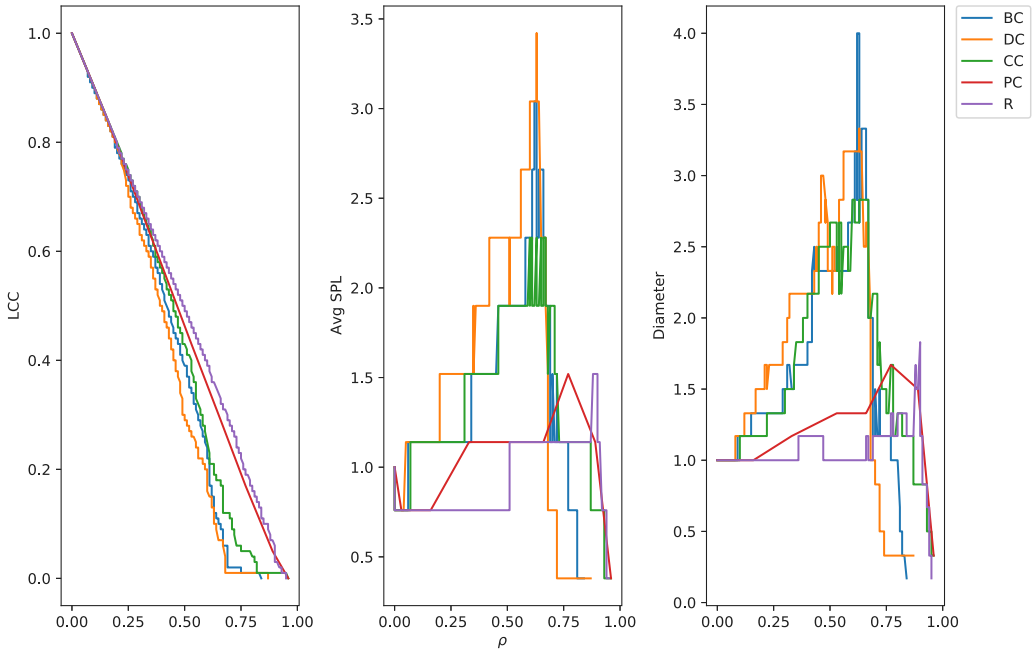


(a) Simultaneous central attacks

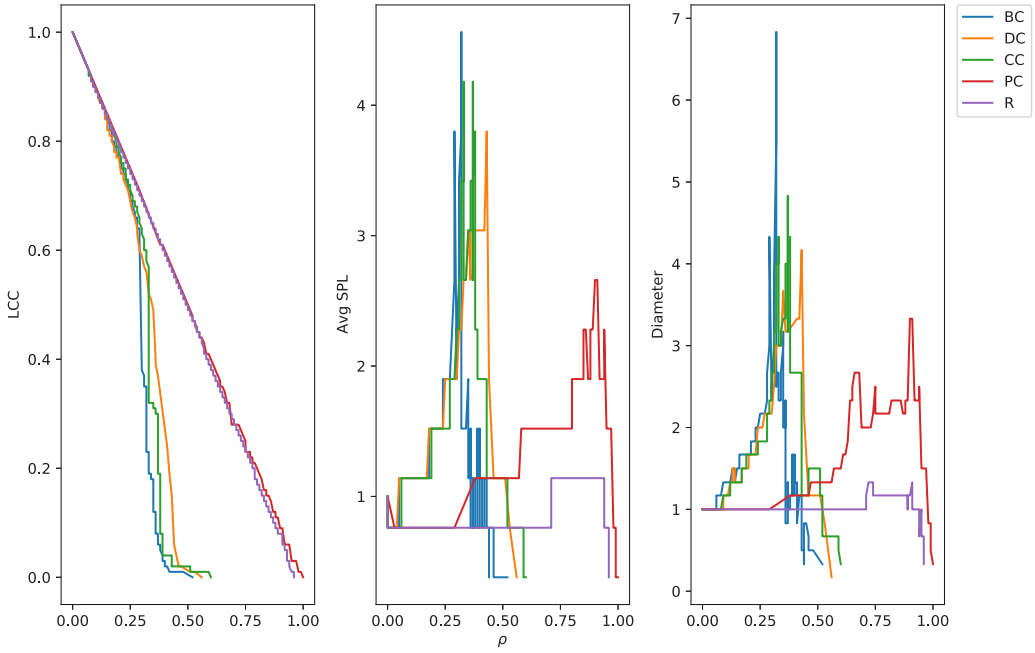


(b) Sequential central attacks

Fig. 23. Comparison of updates in LCC, average shortest path length and diameter against ρ, fraction of nodes removed, in central attacks on weighted *Central Chilean Power Grid (CPW) network*.



(a) Simultaneous central attacks



(b) Sequential central attacks

Fig. 24. Comparison of updates in LCC, average shortest path length and diameter against ρ, fraction of nodes removed, in central attacks on weighted *Messel Shale Food Web (MSFW) network*.

Table 6
Properties of unweighted synthetic networks.

Network	N	LCC	ℓ	ℓ_{max}	Δ	γ
Erdos–Renyi Model	1000	1000	3.26	5	9.904	1.02%
	500	500	2.22	3	24.86	4.94%
	100	98	3.01	6	5.04	4.91%
	50	44	3.79	8	2.72	5.34%
Barabasi–Albert Model	1000	1000	3.49	6	5.98	2.74%
	500	500	3.27	5	5.96	5.09%
	100	100	2.63	4	5.82	12.59%
	50	50	2.30	4	5.64	18.73%
Newman–Watts–Strogatz Model	1000	1000	2.40	3	47.71	52.36%
	500	500	2.57	4	24.15	50.06%
	100	100	3.85	7	4.78	37.24%
	50	50	5.52	12	2.36	3.33%

Table 7
Properties of synthetic networks weighted by clustering coefficient.

Network	N	LCC	ℓ	ℓ_{max}	Δ	γ
Erdos–Renyi Model	1000	1000	0.003	0.15	9.72	1.48%
	500	500	0.0011	0.191	9.63	1.36%
	100	99	0.074	3.62	9.96	1.50%
	50	49	0.224	3.67	5.55	2.84%
Barabasi–Albert Model	1000	1000	0.006	1.62	3.34	0.284%
	500	500	0.016	1.99	3.84	0.40%
	100	100	0.15	3.53	4.91	3.13%
	50	50	0.10	2.2	5.80	3.65%
Newman–Watts–Strogatz Model	1000	1000	0.0012	0.19	9.87	32.01%
	500	500	0.02	.77	9.72	29.95%
	100	100	3.37	7.08	8.07	23.93%
	50	50	0.115	2.86	0.57	2.11%

Table 8
Properties of synthetic networks weighted randomly.

Network	N	LCC	ℓ	ℓ_{max}	Δ	γ
Erdos–Renyi Model	1000	1000	0.143	0.38	24.92	2.09%
	500	500	0.26	0.66	12.43	2.09%
	100	99	0.91	2.85	2.95	2.59%
	50	49	1.524	3.7	2.066	4.86%
Barabasi–Albert Model	1000	1000	0.967	2.65	2.97	1.19%
	500	500	0.908	2.20	3.02	2.30%
	100	100	0.82	2.09	3.003	5.61%
	50	50	0.87	2.12	3.07	8.58%
Newman–Watts–Strogatz Model	1000	1000	0.162	0.46	24.01	21.68%
	500	500	0.298	0.77	11.91	21.37%
	100	100	1.35	2.94	2.46	16.35%
	50	50	3.66	8.06	1.43	2.196%

Table 9
Unweighted empirical networks.

Network	N	LCC	ℓ	ℓ_{max}	Δ	γ
Game of Thrones co-appearances (GoT)	107	107	2.90	6	6.58	55.14%
Human brain functional co-activations (BR)	480	467	4.92	20	4.24	30.88%
US airport network (US)	500	500	2.999	7	11.92	61.75%
Scientific collaborations in network science (SCN)	1461	379	6.04	17	4.82	74.12%
Central Chilean Power Grid (CPW)	347	347	8.15	23	2.56	8.65%
Messel Shale Food Web (MSFW)	700	700	2.63	6	18.35	10.38%

Table 10
Weighted empirical networks.

Network	N	LCC	ℓ	ℓ_{max}	Δ	γ
Game of Thrones co-appearances (GoT)	107	107	0.295	0.782	0.903	23.5%
Human brain functional co-activations (BR)	480	467	1.096	6.782	1.283	7.34%
US airport network (US)	500	500	300.46	7162.99	12826.87	0.048%
Scientific collaborations in network science (SCN)	1461	379	11.48	38.388	14.775	25.05%
Central Chilean Power Grid (CPW)	347	347	25398.22	112438	3464.16	0.63%
Messel Shale Food Web (MSFW)	700	700	1.039	3.499	9.84	5.72%

References

[1] A.L. Barabási, R. Albert, Emergence of scaling in random networks, Science 286 (5439) (1999) 509–512.
[2] R. Albert, A.L. Barabási, Statistical mechanics of complex networks, Rev. Modern Phys. 74 (1) (2002) 47.
[3] M.E. Newman, Clustering and preferential attachment in growing networks, Phys. Rev. E 64 (2) (2001) 025102.
[4] M.E. Newman, S. Forrest, J. Balthrop, Email networks and the spread of computer viruses, Phys. Rev. E 66 (3) (2002) 035101.
[5] R. Albert, H. Jeong, A.L. Barabási, Diameter of the world-wide web, Nature 401 (6749) (1999) 130–131.
[6] A.L. Barabasi, Z.N. Oltvai, Network biology: understanding the cell's functional organization, Nature Rev. Genet. 5 (2) (2004) 101–113.
[7] P.Y. Chen, A.O. Hero, Assessing and safeguarding network resilience to nodal attacks, IEEE Commun. Mag. 52 (11) (2014) 138–143.
[8] M. Girvan, M.E. Newman, Community structure in social and biological networks, Proc. Natl. Acad. Sci. 99 (12) (2002) 7821–7826.
[9] H. Jeong, B. Tombor, R. Albert, Z.N. Oltvai, A.L. Barabási, The large-scale organization of metabolic networks, Nature 407 (6804) (2000) 651–654.
[10] H. Jeong, S.P. Mason, A.L. Barabási, Z.N. Oltvai, Lethality and centrality in protein networks, Nature 411 (6833) (2001) 41–42.
[11] E.M. Jin, M. Girvan, M.E. Newman, Structure of growing social networks, Phys. Rev. E 64 (4) (2001) 046132.
[12] M.E. Newman, The structure of scientific collaboration networks, Proc. Natl. Acad. Sci. 98 (2) (2001) 404–409.
[13] M.E. Newman, Spread of epidemic disease on networks, Phys. Rev. E 66 (1) (2002) 016128.
[14] Z. Zou, Y. Xiao, J. Gao, Robustness analysis of urban transit network based on complex networks theory, Kybernetes 42 (3) (2013) 383–399.
[15] A. Broder, R. Kumar, F. Maghoul, P. Raghavan, S. Rajagopalan, R. …. Stata, J. Wiener, Graph structure in the web, Comput. Netw. 33 (1–6) (2000) 309–320.
[16] M. Bellingeri, D. Bevacqua, F. Scotognella, R. Alfieri, D. Cassi, A comparative analysis of link removal strategies in real complex weighted networks, Sci. Rep. 10 (1) (2020) 1–15.
[17] H. Cetinay, K. Devriendt, P.Van. Mieghem, Nodal vulnerability to targeted attacks in power grids, Appl. Netw. Sci. 3 (1) (2018) 34.
[18] L.K. Gallos, R. Cohen, F. Liljeros, P. Argyrakis, A. Bunde, S. Havlin, Attack strategies on complex networks, in: International Conference on Computational Science, Springer, Berlin, Heidelberg, 2006.
[19] P. Holme, B.J. Kim, C.N. Yoon, S.K. Han, Attack vulnerability of complex networks, Phys. Rev. E 65 (5) (2002) 056109.
[20] S. Iyer, T. Killingback, B. Sundaram, Z. Wang, Attack robustness and centrality of complex networks, PLoS One 8 (4) (2013) e59613.
[21] D.S. Lekha, K. Balakrishnan, Central attacks in complex networks: A revisit with new fallback strategy, Physica A (2020) 124347.
[22] H.A.M. Malik, F. Abid, M.R. Wahiddin, Z. Bhatti, Robustness of dengue complex network under targeted versus random attack, Complexity 2017 (2017).
[23] Q. Nguyen, H.D. Pham, D. Cassi, M. Bellingeri, Conditional attack strategy for real-world complex networks, Physica A 530 (2019) 121561.
[24] Q. Nguyen, D. Cassi, M. Bellingeri, New nodes attack strategies for real complex weighted networks, 2020, arXiv preprint arXiv:2008.02139.
[25] T. Nie, Z. Guo, K. Zhao, Z.M. Lu, New attack strategies for complex networks, Physica A 424 (2015) 248–253.
[26] C.M. Schneider, A.A. Moreira, J.S. Andrade, S. Havlin, H.J. Herrmann, Mitigation of malicious attacks on networks, Proc. Natl. Acad. Sci. 108 (10) (2011) 3838–3841.
[27] D. Zhang, E.K. Cetinkaya, J.P. Sterbenz, Robustness of mobile ad hoc networks under centrality-based attacks, in: 2013 5th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT, IEEE, 2013, pp. 229–235.
[28] S. Zhang, W. Si, T. Qiu, Q. Cao, Toward more effective centrality-based attacks on network topologies, in: ICC 2020-2020 IEEE International Conference on Communications, ICC, IEEE, 2020, pp. 1–6, June.
[29] A. Barrat, M. Barthelemy, R. Pastor-Satorras, A. Vespignani, The architecture of complex weighted networks, Proc. Natl. Acad. Sci. 101 (11) (2004) 3747–3752.
[30] L.C. Freeman, Centrality in social networks conceptual clarification, Social Networks 1 (3) (1978) 215–239.
[31] M.E. Newman, Scientific collaboration networks. II. Shortest paths, weighted networks, and centrality, Phys. Rev. E 64 (1) (2001) 016132.
[32] D.S. Callaway, M.E. Newman, S.H. Strogatz, D.J. Watts, Network robustness and fragility: Percolation on random graphs, Phys. Rev. Lett. 85 (25) (2000) 5468.
[33] R. Albert, H. Jeong, A.L. Barabási, Error and attack tolerance of complex networks, Nature 406 (6794) (2000) 378–382.
[34] I. Gialampoukidis, G. Kalpakis, T. Tsikrika, S. Vrochidis, I. Kompatsiaris, Key player identification in terrorism-related social media networks using centrality measures, in: 2016 European Intelligence and Security Informatics Conference, EISIC, IEEE, 2016, pp. 112–115, August.
[35] D.J. Watts, S.H. Strogatz, Collective dynamics of 'small-world'networks, Nature 393 (6684) (1998) 440–442.
[36] M. Bellingeri, D. Cassi, S. Vincenzi, Efficiency of attack strategies on complex model and real-world networks, Physica A 414 (2014) 174–180.
[37] J. Wu, S.Y. Tan, Z. Liu, Y.J. Tan, X. Lu, Enhancing structural robustness of scale-free networks by information disturbance, Sci. Rep. 7 (1) (2017) 13, 7559.
[38] L.K. Gallos, P. Argyrakis, Scale-free networks resistant to intentional attacks, Europhys. Lett. 80 (5) (2007) 58002.
[39] A.S. Revathy, R.R. Nair, M.R. Chithra, A survey on - how the diameter of a graph is affected by the removal and the addition of edges, Int. J. Appl. Eng. Res. 10 (2015) 37070–37075.
[40] J.M. Kleinberg, Navigation in a small world, Nature 406 (6798) (2000) 845.
[41] D.J. Watts, Six Degrees: The Science of a Connected Age, WW Norton & Company, 2004.
[42] L. Dall'Asta, A. Barrat, M. Barthélemy, A. Vespignani, Vulnerability of weighted networks, J. Stat. Mech. Theory Exp. 2006 (04) (2006) P04006.
[43] P.Y. Chen, A.O. Hero, Node removal vulnerability of the largest component of a network, in: 2013 IEEE Global Conference on Signal and Information Processing, IEEE, 2013, pp. 587–590, December.
[44] M.A. Latif, M. Naveed, F. Zaidi, Resilience of social networks under different attack strategies, in: International Conference on Social Informatics, Springer, Cham, 2013, pp. 16–29, November.
[45] J. Wang, C. Li, C. Xia, Improved centrality indicators to characterize the nodal spreading capability in complex networks, Appl. Math. Comput. 334 (2018) 388–400.

[46] M. Bellingeri, D. Bevacqua, F. Scotognella, R. Alfieri, Q. Nguyen, D. Montepietra, D. Cassi, Link and node removal in real social networks: a review, 2020, pp. 1–7.
[47] M. Bellingeri, D. Cassi, Robustness of weighted networks, Physica A 489 (2018) 47–55.
[48] M. Bellingeri, D. Bevacqua, F. Scotognella, D. Cassi, The heterogeneity in link weights may decrease the robustness of real-world complex weighted networks, Sci. Rep. 9 (1) (2019) 1–13.
[49] N. Wan, F. Zhan, Z. Cai, A spatially weighted degree model for network vulnerability analysis, Geo-Spatial Inf. Sci. 14 (4) (2011) 274–281.
[50] Y. Zhou, J. Wang, G.Q. Huang, Efficiency and robustness of weighted air transport networks, Trans. Res. E Logist. Transp. Rev. 122 (2019) 14–26.
[51] S. Sun, X. Liu, L. Wang, C. Xia, New link attack strategies of complex networks based on k-core decomposition, IEEE Trans. Circuits Syst. II Express Briefs 67 (12) (2020) 3157–3161.
[52] V. Latora, M. Marchiori, Efficient behavior of small-world networks, Phys. Rev. Lett. 87 (19) (2001) 198701.
[53] M. Li, Y. Fan, J. Chen, L. Gao, Z. Di, J. Wu, Weighted networks of scientific communication: the measurement and topological role of weight, Physica A 350 (2–4) (2005) 643–656.
[54] M. Zhu, T. Cao, X. Jiang, Using clustering coefficient to construct weighted networks for supervised link prediction, Soc. Netw. Anal. Min. 4 (1) (2014) 215.
[55] A. Beveridge, J. Shan, Network of thrones, Math. Horiz. 23 (4) (2016) 18–22.
[56] B. Szalkai, C. Kerepesi, B. Varga, V. Grolmusz, The budapest reference connectome server v2. 0., Neurosci. Lett. 595 (2015) 60–62.
[57] V. Colizza, R. Pastor-Satorras, A. Vespignani, Reaction–diffusion processes and metapopulation models in heterogeneous networks, Nat. Phys. 3 (4) (2007) 276–282.
[58] M.E. Newman, Finding community structure in networks using the eigenvectors of matrices, Phys. Rev. E 74 (3) (2006) 036104.
[59] Seung-Woo Son, Heetae Kim, David Olave-Rojas, Eduardo Álvarez-Miranda, Edge information of Chilean power grid with tap. figshare. Dataset, 2018, 10.6084/m9.figshare.6066587.v1.
[60] Labandeira Conrad C., A. Dunne Jennifer, Data from: Highly resolved early eocene food webs show development of modern trophic structure after the end-cretaceous extinction, dryad, dataset, 2015.