Cascaded failures in weighted networks

Baharan Mirzasoleiman, Mahmoudreza Babaei, Mahdi Jalili*, and MohammadAli Safari

***Abstract*— Many technological networks might experience random and/or systematic failures in their components. More destructive situation can happen if the components have limited capacity, which the failure in one of them might lead to a cascade of failures in other components, and consequently break down the whole network. In this paper, the tolerance of cascaded failures was investigated in weighted networks. Three weighting strategies were considered including the betweenness centrality of the edges, the product of the degrees of the end nodes, and the product of their betweenness centralities. Then, the effect of the cascaded attack was investigated by considering the local weighted flow redistribution rule. The capacity of the edges was considered to be proportional to their initial weight distribution. The size of the survived part of the attacked network was determined in model networks as well as in a number of real-world networks including the power grid, the Internet in the level of autonomous system, the railway network of Europe, and the US airports network. We found that the networks in which the weight of each edge is the multiplication of the betweenness centrality of the end nodes had the best robustness against cascaded failures. In other words, the case where the load of the links is considered to be the power-law function of the product of the of the betweenness centrality of the end nodes is favored for the robustness of the network against cascaded failures.**

***Index Terms*— Complex networks, betweenness centrality, cascaded failure, robustness.**

I. Introduction

NETWORK science has attracted much attention in recent years, primarily due to its application in many areas ranging from biology to medicine, engineering and social sciences [1, 2]. Research in network science starts by observing a phenomenon in real data and then tries to construct models to mimic its behavior. Many real-world networks share some common structural properties such as scale-free degree distribution, small-worldness and modularity. The dynamic behavior of networks largely depends on their structural properties [3, 4]. For example, how the nodes coordinate their dynamical behavior or how a dynamical process such as cooperation evolves in the network, depends on the structure of the network [5, 6]. One of the topics that have attracted much attention in this context is robustness of networks against random and systematic component failures [7-9]. Networks might undergo failures in a number of their components, i.e. nodes and edges, and consequently lose proper functionality [10, 11]. The failure in a network can be random or systematic. When a random failure, i.e. error, occurs in a network, a number of its components are randomly removed from the network. While, in a systematic failure, i.e. attack, the components are systematically broken down [7, 12]. For example, the hub nodes might be target to attacks. When the intrinsic dynamics of network flows are taken into account, the systematic removal of the components can have a much more devastating consequence than random removal [13].

The modern societies are largely dependent on networked structures such as power grids, information communication networks, the Internet, and transportation networks. Failure in such networks might collapse the normal daily life and result in chaos in the society. Evidence has shown that locally emerging random or systematic failures in the networks can influence the entire network, often resulting in large-scale collapse in the network. Examples include large black out in the USA due to failure in the power grid [14], and break-down of the Internet [15]. Indeed, a cascaded failure happened in such cases [11, 13]. A possible mechanism for the cascaded failure can be as follows [11, 13, 16]. The network loses a component (e.g. a node with the highest value of the load). The load passing through this component is redistributed among other components. This process may lead some other components overflow, and consequently, fail. This repeated process may end up the network to completely lose the functionality. For example, the network becomes disconnected with many isolated islands as a consequence of cascaded failures. Cascaded failures may also happen in interdependent networks, where failures in the nodes of one networks may lead a cascade of failures in dependent nodes in other networks [12].

The influence of the cascaded failure in the size of the largest connected component has been investigated in a number of model networks including preferential attachment scale-free [17], Watts-Strogatz small-world [18], and modular networks [19]. In many of the studies, as a component fails, the load are recalculated and the components whose load exceeding their capacity are removed from the network. The process is repeated until the loads of all remaining components are below their capacity [17-19]. However, this might not be realistic in some applications. For example, consider the Internet. It is natural that the load passing through a failed component is redistributed among its neighboring components. To this end, a Local Weighted Flow Redistribution Rule (LWFRR) has been proposed [20]. In this model, the cascaded failure is triggered by removing the edge with maximal load.

The authors are with the Department of Computer Engineering, Sharif University of Technology, Tehran, Iran.

As an edge is removed from the network, its load is redistributed among the neighbors. Studying model networks with scale-free and small-world properties and by applying LWFRR, Wang and Chen found the strongest robustness against cascaded failure at a specific weighting strength [20].

In this paper we investigated a number of factors influencing the robustness of the networks against cascaded failures. An important question in this context is “which component has the largest cascaded effect on the network?” We considered cascaded effect of failures in the edges. Furthermore, the networks were weighted according to different rules due to the fact that many real-world networks are inherently weighted. We used three weighting strategy: the betweenness centrality of the edge as its weight, the power-law function of the product of the degrees of the end nodes, and the power-law function of the product of their betweenness centrality. The numerical simulations were performed on a number of model networks such as preferential attachment scale-free [21], Newman-Watts small-world [22], Erdos-Renyi [23], and modular networks [19]. Furthermore, we considered a number of real-world networks including the power grid, the internet in the level of autonomous systems, the railway network of Europe and the US airports network. We found that the networks whose weights are the product of the betweenness centrality of the end nodes have the most robustness against cascaded failures. This study suggests that in order to enhance the robustness of the networks against cascaded failures, one could take the loads (weights) of the edges as the product of the betweenness centrality of the end nodes.

II. Local Weighted Flow Redistribution Rule

Local Weighted Flow Redistribution Rule (LWFRR) has been recently introduced and studied by Wang and Chen [20]. In this model, when an edge is subject to attack and removed from the network, the flow passing through this edge is redistributed to its nearest neighbor edges [20, 24]. As a consequence, the load of each neighbor edge increases proportional to its weight. More precisely,

$$\Delta F_{im} = F_{ij} \frac{w_{im}}{\sum_{a\in\Gamma_i} w_{ia} + \sum_{b\in\Gamma j} w_{jb}} \qquad (1)$$

where e_{ij} is the attacked edge, Γ_i and Γ_j are the set of neighbors of nodes i and j, respectively. F_{ij} is the flow on e_{ij} before being broken and ΔF_{im} is the additional flow that the e_{im} receives.

Every edge e_{ij} has some limited capacity C_{ij} determining the maximum load that the edge can handle. The capacity C_{ij} of the edge e_{ij} is assumed to be proportional to the initial load of the edge w_{ij}, i.e. $C_{ij}=Tw_{ij}$. That is, there exist a constant threshold value $T > 1$ such that if

$$F_{im} + \Delta F_{im} > Tw_{im} = C_{im} \qquad (2)$$

then, the edge e_{im} cannot tolerate the additional flow and will break apart. As a result, the network faces further redistribution of the flows, and consequently, more edges might break. Cascading failure continues as long as there is no edge e_{uv} whose flow dominates its capacity, i.e. $F_{uv} > Tw_{uv}$.

The threshold parameter is usually limited by the cost in many networks. Thus, the number of edges that will be broken at a given threshold is of great importance. The lower the number of broken edges, the more robust the network is against attacks. There exists a minimum threshold at which removal of an edge does not lead to cascading failure any more. A phase transition is occurred at this critical threshold (T_c), where for $T < T_c$ the network preserves its robustness against any random or systematic failure. On the other hand, for $T < T_c$ failure of a part can trigger the failure of successive parts of the network and cascading failure suddenly emerges. T_c is a significant measure in determining a network’s robustness; the lower the value of T_c is the stronger the robustness of the network is against removal of its components.

In real-world networks, cascading failure is often studied in order to protect many infrastructure networks. Computer networks and the Internet are such examples that should be protected against cascaded failures [25, 26]. Protecting electrical grid against failures and a society against spread of an infectious disease are other examples where the studies in this context can be beneficial for. Let us consider a computer network. If a few important cables break down, the traffic should be rerouted either globally or locally towards the destination. This will lead to redistribution of the traffic in the network. When a line receives extra traffic, its total flow may exceed its bandwidth (threshold) and cause congestion. As a result, an avalanche of overloads emerges on the network and cascading failure might occur. As another example, suppose a disease appears in a region. It might spread to other regions through infected individuals traveling across the regions. It is obvious that immunization of individuals who travels from populated regions prevents the wide-spread distribution of the disease. Consequently, spending more money for vaccinating these individuals seems a reasonable action. In the power grid example, when an element (completely or partially) fails, its load shifts to nearby elements in the system. Some of those nearby elements may be pushed beyond their capacity and become overloaded; thus get broken and shift their load onto other neighbor elements. This surge current can induce the already overloaded nodes into failure, setting off more overloads and thereby taking down the entire system in a very short time. This failure process cascades through the elements of the system like a ripple on a pond and continues until a substantial magnitude of elements in the system are compromised and/or the system becomes functionally disconnected from the source of its load. Under certain conditions, a large power grid might collapse after the failure of a single transformer. All these networks are examples of weighted networks in which the weight of each edge can be interpreted as either its capacity or cost of immunization and failure of an edge causes an immediate increase of the load of its nearest neighbor edges.

III. Weighting Methods

In network characterization, the centrality of an element is a significant measure and plays a fundamental role in studying cascading failure [27]. The degree of a node is an obvious topological metric that can be used for determining its connectivity as well as centrality. The degree of the node *i* is defined as

$$k_i = \sum_1^N a_{ij} \tag{3}$$

where *N* is the size of the network and $A = (a_{ij})$, $i, j = 1, \ldots, N$, is the adjacency matrix of an undirected and unweighted network. However, there may exist some nodes that play a crucial role in connecting different parts of the network despite their small degree. Such nodes are called bridges or local bridges and connect parts of the network that would become disconnected otherwise. Because of their topological positions in the network, many shortest paths (often the only plausible route between many pairs of nodes) pass through these nodes. These reasons motivated to introduce another measure for centrality of a node in the network, i.e. node betweenness centrality. Node betweenness centrality is defined as the number of shortest paths between pairs of nodes that pass through a given node [28]. More precisely,

$$B_i = \sum_{p \neq i \neq q} \left(\Gamma_{pq}(i) / \Gamma_{pq} \right) \tag{4}$$

where Γ_{pq} is the number of shortest paths from the node *p* to node *q* and $\Gamma_{pq}(i)$ is the number of these shortest paths making use of node *i*. The betweenness centrality of a node is indeed the load of shortest paths making use of the node, i.e. the larger the betweenness centrality of a node is, the more its significance is in the formation of the shortest paths in the network.

Another measure of centrality is edge betweenness centrality and has been widely used to model the traffic load or weight of an edge; it is defined similar to node betweenness centrality. The edge betweenness centrality of an edge is the number of shortest paths between pairs of nodes that pass through the edge e_{ij} [28]; That is,

$$B_{ij} = \sum_{p \neq q} \left(\Gamma_{pq}(ij) / \Gamma_{pq} \right) \tag{5}$$

where $\Gamma_{pq}(i)$ is the number of shortest paths that go through the edge *ij*.

These centrality measures can be used to determine the loads in an unweighted network or estimate the weights in a weighted real network. Wang and Chen [20] used node degrees to model the traffic on a network and study cascading failure. They used the power-law function of degrees of the two ends of an edge as measure for edge centrality and obtained several experimental results on different real word networks. According to their definition, the weight of an edge is modeled by

$$w_{ij} = (k_i k_j)^q . \tag{6}$$

where k_i is the degree of node *i* and θ is a tuning parameter. They showed that $\theta = 1$ leads to strongest robustness on various networks.

We introduce a new weighting method based on node betweenness centrality. Our studies showed that this weighting method is in accordance with the weights of many real networks. The intuition for the new weighting method is based on the observation that an edge is important in a network when its two end nodes are important. As an example, assume one is flying from London to Melbourne. He probably chooses some central cities such as Dubai or Kuala Lumpur and flies through them in his way to Melbourne. Therefore, an edge is chosen when its two ends have high centrality. A similar observation can be made for packet routing on the Internet. The links between central points are more probable to be chosen when sending a packet. Based on the above observation, one can take into account the centrality of both end nodes of an edge and define the weight of an edge e_{ij} as

$$w_{ij} = (B_i B_j)^q . \tag{7}$$

In this method, the weight of an edge has a power law dependence on the product of betweenness centrality of the its two end nodes. This is indeed somehow the case in many real-world networks, where the weights of the links do not follow the betweenness centrality of the edges. However, it shows high correlation by the weights introduced through equations (6) and (7). We showed the correlation between the above two weighting strategies on a number of real-world networks including:

US Airlines: An airlines connection network in the USA collected in 1997. This network consists of 332 nodes and 1063 edges**.** The weights correspond to the number of seats available on the scheduled flights [29].

US Airports network: This is the network of 500 busiest commercial airports in the USA. An edge between two airports indicates that a flight was scheduled between them in 2002.

The weights correspond to the number of seats available on the scheduled flights [30]. This network has 2980 edges.

Lesmis: Coappearance network of characters in the novel *Les Miserables*. This network has 77 nodes and 127 edges [31].

Netscience: coauthorship network of scientists working in the field of network theory and experiment. This network contains 1589 nodes and 1371 edegs [32].

Bkham: The network of human interactions in bounded groups and on the actors' ability to recall those interactions. This network consists of 44 node and 153 edges [33].

Table I shows the Pearson correlation coefficients between the real weights and different metrics including the betweenness centrality of the edges B_{ij}, the product of the betweenness centrality of the end nodes, B_iB_j, and the product if the degree of the end nodes k_ik_j. As it is seen, except for Netscience the edge betweenness centrality has almost no correlation with the real weights, whereas, the product of the degrees and the node betweenness centralities showed significant correlation with the real weights. The results indicate that these two measures could be a good candidate for the weights of the edges. This issue is important especially in designing technological networks where the link weights (or loads) can be appropriately designed. Next we investigate which of the weighting strategies has the best robustness against cascaded failures.

TABLE I.PEARSON CORRELATION COEFFICENTS BETWEEN REAL WEIGHTS AND DEFFERENT METRICS(THE BETWEENNESS CENTRALITY OF THE EDGES B_{ij}, THE PRODUCT OF THE BETWEENNESS CENTRALITY F THE END NODES, B_iB_j,AND THE PRODUCT OF THE DEGREE OF THE END NODES k_ik_j) IN A NUMBER OF REAL-WORLD NETWORKS.

Network	Correlation with B_iB_j	Correlation with k_ik_j	Correlation with E_{ij}
USAir97	0.24	0.28	0.08
USAirport500	0.29	0.61	-0.04
Lesmis	0.25	0.36	-0.04
Netscience	0.21	0.10	0.19
Bkham	0.54	0.63	0.05

IV. NETWORK DATA

In this section, the cascaded failure is investigated in artificially constructed model networks as well as in a number of real networks, weighted through different strategies.

A. *Model Networks*

We considered a number of models to produce artificially constructed networks. Networks with power-law degree distribution, i.e. scale-free networks, are abundant in real systems. Random scale-free networks were generated using the original preferential attachment algorithm proposed by Barabasi and Albert in their seminal paper [34]. Starting with a number of all-to-all connected nodes, the network grows by adding new nodes. These nodes are connected to the old nodes with probability proportional to their degree. The resulting network has degree distribution that is power-law with exponent 3. Scale-free networks are widely observed in natural and man-made systems, including the Internet, the World Wide Web, citation networks, and some social networks.

The degree distribution of scale-free networks is heterogeneous; however, many real networks have homogeneous degree sequence. In order to construct such networks, we considered two other models, namely, Newman-Watts and Erdös-Rényi models. The Newman-Watts networks were constructed as follows [35]. Starting with a regular ring graph with nodes connected to their m-nearest neighbors, the non-connected nodes get connected with a probability P. In order to construct Erdös-Rényi random networks, in a network with N nodes, the nodes are connected with a probability P, where for the values of $P = 1$ an all-to-all connected network is obtained [36].

It has been shown that many real networks have modular structure [37, 38]. We also considered modular networks constructed through an algorithm as follows [19]. First n isolated modules each with preferential attachment scale-free structure are built. Then, with probability P the intra-modular links are disconnected and inter-modular connections are created. In other words, with probability P each intra-modular link is disconnected and a connection is created between two random nodes from two randomly chosen modules.

B. *Real Networks*

Although model networks are useful in understanding how real systems behave, they cannot capture many of the structural properties of the real networks. Therefore, we also considered a number of real networks and applied the cascaded failure on them. We consider four technological networks where the weights of the links (and the traffic as well) can be designed.

US Airports network. We analyze the USA airports network containing the 500 busiest commercial airports in the United States [30]. A link between two airports indicates that a flight was scheduled between them in 2002. Even though this networks is naturally directed, the networks are highly symmetric [39]. We considered the network with real weights as well as the unweighted version that is if there exist a link from one airport towards the one, there is a reciprocal link between these nodes. The network has 500 nodes and 2980 links.

Internet. Sometimes, Internet is considered as a network of routers connected by links. Each router belongs to some autonomous system (AS), this dataset simultaneously studies the router and AS level topology; and thus, both routers and AS's are considered as nodes. It contains 2062 nodes and 4233 links [40].

Transportation network. The railway network used in this work is formed by major trains and stations in the central European region [41]. This network dataset is compiled from traffics flows from timetables of public mass transportation systems. The set of nodes is defined by the set of all train stations. Two stations are considered to be connected by a link when there is at least one vehicle that stops at both stations. The network consists of 2488 nodes and 6691 edges.

Electrical power grid. This network is an undirected and unweighted network representing the topology of the western states high-voltage power grid of the United States [42]. In construction of the network, the transformers, substations, and generators are considered as nodes, and the links are high-voltage transmission lines. The network is composed of 4941 nodes and 6549 links.

V. Simulation Results

In order to investigate the profile of robustness against cascaded failures, the behavior of the network is studied as a function of the threshold parameter *T*. We considered different weighting strategies in the networks as follows:

1) $w_{ij} = (B_iB_j)^\theta$, where w_{ij} is the weight of edge e_{ij} and B_i is the betweenness centrality of nodes *i*.
2) $w_{ij} = B_{ij}$, where B_{ij} is edge betweenness of edge e_{ij}.
3) $w_{ij} = (k_ik_j)^\theta$, where k_i is the degree of nodes *i*.

In order to study the effect of a small initial attack on the cascading model, we cut an edge e_{ij} and compute the number of broken edges once the process of cascading failure is over. Then, we compute the expected of this value according to the following formula:

$$S_N = \frac{\sum_i \sum_j s_{ij}}{E} \qquad (8)$$

where E is the number of edges in the network, s_{ij} is the normalized avalanche size, i.e. the number of broken edges, by cutting edge e_{ij} and S_N is averaged over all normalized avalanche sizes. Note that as one edge gets broken and its weight is locally redistributed, other edges get broken if their new load become more than their capacity that is proportional to their initial weight. In other words, the initial load of the edges is considered to be their weight.

Let us first study the influence of the parameter θ on the critical threshold T_c. It has been shown that the values of $\theta \cong 1$ are optimal for the weighting method (3), where the weights of the edges are the product of the degrees of the end nodes [20]. Fig. 1 shows T_c as a function of θ in scale-free and Newman-Watts networks with the weights assigned as the method (1), i.e. the product of the betweenness centralities of the end nodes. This figure shows that weighting the networks with $\theta \cong 1$ results in optimal T_c. Although $\theta > 1$ assigning stronger weights to the links between central nodes, it might make the networks more robust against cascading failure for smaller values of *T*, it also increases the critical threshold (T_c). Since optimal T_c is important in the robustness of the networks against cascaded failures, we adopted $\theta = 1$ for the numerical simulations. Next we also derive some theoretical foundation for this choice.

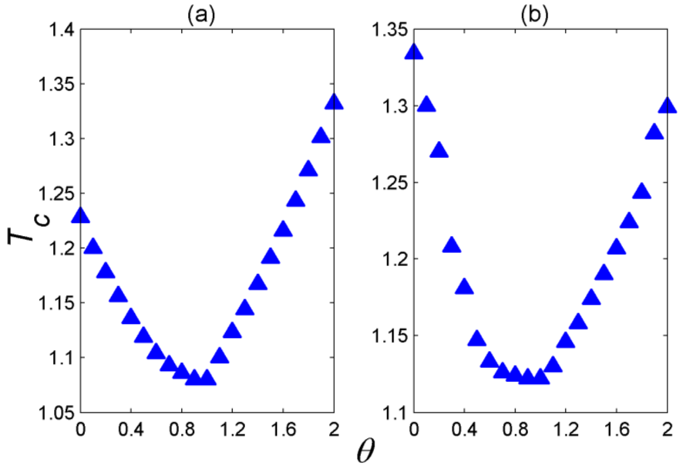

Fig. 1.The critical threshold T_c as a function of θ for (a), scale-free with 1000 nodes and m = 3 (b), Newman-Watts networks with 1000 nodes, k = 3 and p = 0.1. Data shows averages over 10 realizations.

Attacking an edge subjects its neighboring edges to receive an overload proportional to their current flow. In order to avoid cascading failure in a network, the flow passing from each edge after flow redistribution should remain less than its capacity, see Eq. (2). From Eqs. (1)-(2) and using the weighting method as $w_{ij} = (B_iB_j)^\theta$, one can drive

$$\frac{(B_iB_j)^\theta (B_iB_m)^\theta}{\sum_{a\in\Gamma_i}(B_iB_a)^\theta + \sum_{b\in\Gamma_j}(B_jB_b)^\theta} + (B_iB_j)^\theta < T(B_iB_j)^\theta \qquad (9)$$

where Γ_i and Γ_j are the set of neighbors of nodes *i* and *j*, respectively.

Now let us define $P(B'|B_i)$ as the conditional probability that a node with betweenness centrality B_i is connected to a node with betweenness centrality B'. Using Bayes' rule [43] we get

$$\sum_{a\in\Gamma_i}(B_iB_j)^\theta = B_i^\theta \sum_{B'=B_{\min}}^{B_{\max}} B_iP(B'|B_i)B'^\theta \qquad (10)$$

where B_{max} and B_{min} are the minimum and maximum node betweenness centralities.

It has been shown that the networks constructed through preferential attachment and Newman-Watts algorithms do not show assortative or disassortative behavior, i.e. no degree-degree correlations [44, 45] . Similarly we numerically computed the betweenness-betweenness correlations for the networks. The scale-free networks were constructed with $N = 1000$ and $m = 3$, and the Newman-Watts networks with $N = 1000$, $m = 3$, and $P = 0.1$. Then, the correlation coefficient among the betweenness centrality of the nodes was computed. Averaging over 100 realizations, the betweenness-betweenness correlations were obtained as -0.03 for scale-free networks and

0.01 for Newman-Watts networks. Similar results were obtained for networks of other sizes and topological parameters (Data not shown here). Therefore, these networks do not show any significant betweenness-betweenness correlations, and thus, one can write

$$P(B'|B_i) = B'P(B')\langle B\rangle \tag{11}$$

From Eqs. (10) and (11) we have:

$$B_i^{\theta+1}\sum_{B'=B_{\min}}^{B_{\max}}\frac{B'^{\theta+1}P(B')}{\langle B\rangle} = \frac{B_i^{\theta+1}\langle B^{\theta+1}\rangle}{\langle B\rangle}\,. \tag{12}$$

Therefore, one may rewrite Eq. (9) as

$$\frac{\langle B\rangle}{\langle B^{\theta+1}\rangle}\frac{B_i^{\theta}B_j^{\theta}}{B_i^{\theta+1}+B_j^{\theta+1}} + 1 < T\ . \tag{13}$$

Using Geometric inequality $B_i^{\theta+1}+B_j^{\theta+1} \geq 2(B_iB_j)^{(\theta+1)/2}$, Eq. (13) can be rewritten as

$$\frac{\langle B\rangle (B_iB_j)^{(\theta-1)/2}}{2\langle B^{\theta+1}\rangle} + 1 < T \tag{14}$$

From Eq. (14), we can derive the solution for T_c by dividing θ into three regions as

$$T_c = \begin{cases} B_{\max}^{\theta-1}\langle B\rangle/(2\langle B^{\theta+1}\rangle)+1, & \theta>1 \\ \langle B\rangle/(2\langle B^2\rangle)+1, & \theta=1 \\ B_{\min}^{\theta-1}\langle B\rangle/(2\langle B^{\theta+1}\rangle)+1, & \theta<1 \end{cases} \tag{15}$$

where $B_{\min}$ and $B_{\max}$ are the minimum and maximum node betweenness centralities. First, we calculate the minimum value of T_c for $\theta > 1$ in Eq. (15)

$$\begin{aligned} T_c(\theta>1)-1 &= \frac{B_{\max}^{\theta-1}\langle B\rangle}{2\langle B^{\theta+1}\rangle} = \frac{B_{\max}^{\theta-1}\langle B\rangle}{(2/N)\sum_{i=1}^{N}B_i^{\theta+1}} \\ &= \frac{\langle B\rangle}{(2/N)\sum_{i=1}^{N}B_i^2(B_i/B_{\max})^{\theta-1}} > \frac{\langle B\rangle}{(2/N)\sum_{i=1}^{N}B_i^2} = \frac{\langle B\rangle}{2\langle B^2\rangle} \end{aligned} \tag{16}$$

With a similar reasoning for $\theta < 1$, we have

$$\begin{aligned} T_c(\theta<1)-1 &= \frac{B_{\min}^{\theta-1}\langle B\rangle}{2\langle B^{\theta+1}\rangle} = \frac{B_{\min}^{\theta-1}\langle B\rangle}{(2/N)\sum_{i=1}^{N}B_i^{\theta+1}} \\ &= \frac{\langle B\rangle}{(2/N)\sum_{i=1}^{N}B_i^2(B_i/B_{\min})^{\theta-1}} > \frac{\langle B\rangle}{(2/N)\sum_{i=1}^{N}B_i^2} = \frac{\langle B\rangle}{2\langle B^2\rangle} \end{aligned} \tag{17}$$

As we can see, $T_c(\theta > 1) > T_c(\theta = 1)$ and $T_c(\theta < 1) > T_c(\theta = 1)$. Apparently, the system reaches its strongest robustness level at $\theta = 1$.

To confirm that our weighting strategy (strategy 1) can result the strongest robustness of the network against random or systematic failures, we compare the critical threshold of our weighting method at $\theta = 1$ with the other strategies (note that the $\theta = 1$ has been previously obtained as the optimal case for the weighting strategy 3 [20]). The critical thresholds for each weighting strategy are listed in table II. As it is seen the weighting based on the product of the betweenness centrality of the end nodes resulted in the least critical threshold for these networks (the less the critical threshold of a network is the more desirable its behavior is against cascaded failures). In other words the strongest level of robustness for the networks is resulted from the weighting strategy 1, and hence, weighting strategy 1 results in the strongest level of robustness for any choice of parameter T.

TABLE II. CRITICAL THRESHOLD OF SCALE-FREE NETWORK WITH 1000 NODES AND m = 3, AND NEMAN-WATTS NETWORK WITH 1000 NODES AND k = 3 AND p = 0.1. THE RESULTS ARE SHOWN AT $\theta = 1$ FOR WEIGHTING STRATEGY 1-3. EACH DATA POINT IS AVERAGED OVER TEN DIFFERENT NETWORK REALIZATIONS.

Network	$\boldsymbol{w_{ij} = B_iB_j}$	$\boldsymbol{w_{ij} = B_{ij}}$	$\boldsymbol{w_{ij} = k_ik_j}$
Scale-free	1.080	1.318	1.138
Newman-Watts	1.122	1.255	1.137

Hereafter, we study the profile of cascaded failure in model networks including scale-free, Newman-Watts, Erdös-Rényi, and modular scale-free networks. Fig. 2 shows the value of S_N as a function of the threshold parameter for networks with size $N = 1000$. These networks were weighted with the three weighting strategies discussed above. To have more reliable statistics, each simulation was repeated 10 times and the average was shown. As it is seen, the networks weighted through the product of the node betweenness centralities, i.e. the weighting strategy (1), have the best robustness against cascaded failure. In other words, for a fixed value of the threshold T, the S_N for the networks weighted based on strategy (1) is smaller than the other two cases; the smaller the value of S_N is the more the robustness of the network against the cascaded failure is.

Interestingly, the difference between the profiles of different weighting methods was more pronounced for scale-free and modular scale-free networks as compared to Newman-Watts and random graphs Fig. 2. This can be explained by the fact that unlike random and small-world networks that have homogeneous betweenness centrality distribution, scale-free networks have heterogeneous betweenness centrality. Thus, there are some nodes that have much higher betweenness centrality than other nodes in such networks. This means a high number of shortest paths in the network pass through these central nodes and extremely overloads them. Consequently, assigning more weight to the links between these central nodes is a more realistic solution and significantly improves the robustness of the network against random or systematic failures. This explanation may raise this question that if assigning higher weights to those edges which their end nodes have higher betweenness centrality improve the robustness of the network against cascading failure, why increasing θ in Eqs. (6) and (7) does not have the same effect. Indeed, increasing θ makes the network more robust for $T<T_c$ (results not shown here); however, as shown in Fig. 1, T_c increases by increasing θ that is not desirable.

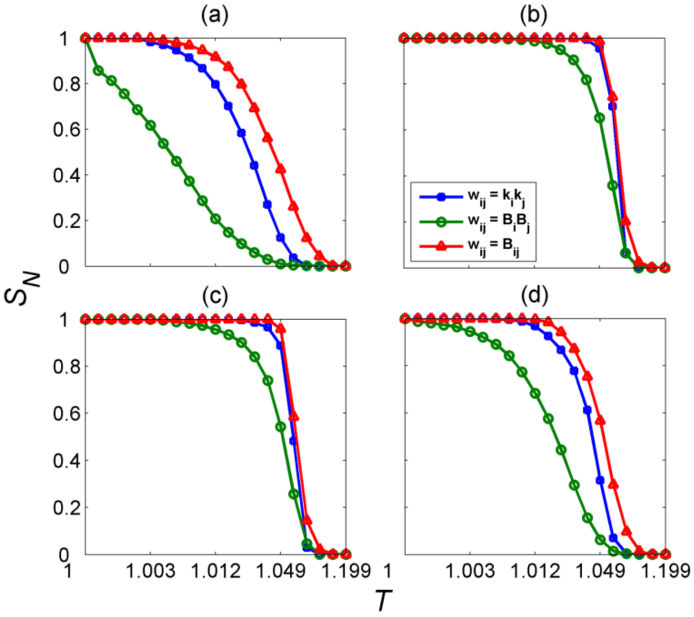

Fig. 2. Normalized average size of the removed edges (S_N) as a function of the threshold parameter (T) for (a) scale-free network with 1000 nodes and m = 3, (b) Newman-Watts network with 1000 nodes, k = 3 and p = 0.1 (c) Erdös-Rényi network with 1000 nodes and p = 0.006, (d) modular networks that has three modules with 200, 300, and 500 nodes and 3000 edges. The red, blue and green lines show the changes in the S_N for weighing methods based on edge Betweenness centrality, degree multiplication, and multiplication of node betweenness centrality, respectively. Data shows averages over 10 realizations.

The cascaded failure process was also investigated in a number of real-world technological networks, where such a failure can broke the whole network down. Such cascaded failures can be due to failure in a central station in the rail transportation network or in a central airport in the network of the airports. In the Internet breaking a few optical cables can lead to congestion in many other links, and consequently, cascaded failures in the network and significantly delayed information transmission. In a power grid, failure of a single transformer that has central role in the network, may overload the nearby elements and causing the entire system to collapse in a very short time.

Fig. 3 shows the S_N for the US airports network. Since the original version of this network is weighted, we also considered the weighted US airports network and run the cascaded failure process. As it is seen, the network weighted based on the product of the betweenness centrality of the end nodes has the best robustness among different weighting methods Fig. 3. For example, for the values of the threshold as T = 1.00305, if the US airports network is weighted according to the product of the betweenness centrality of the end nodes, the average avalanche size is S_N = 0.2, while S_N > 0.6 for other weighting strategies Fig. 3. The network of the US airports has power-law degree distribution [30] and its profile against cascaded failures, as shown in Fig. 3, is similar to the one obtained for scale-free networks (Fig. 2a).

Similar patterns were observed for other real networks including the central European rail network (Fig. 4), the Internet in the level of an autonomous system (Fig. 5), and the power grid (Fig. 6). In all these networks, the weighting strategy based on the product of the betweenness centrality of the end nodes resulted in the best robustness against cascaded failures. The European rail network and the Internet in the level of an autonomous system are scale-free in their degree distribution, and thus, their profile is similar to that of scale-free networks (Fig. 2a). While, the power grid has Poissonian degree distribution, similar to small-world and random networks, and its behavior (Fig. 6) is also similar to these networks (Figs 3b and 3c). In any of these examples, increasing the weights of the links connecting the most central nodes improves the robustness of the network against cascading failures.

This indicates that the robustness of a network against cascaded attacks can be substantially improved by assigning proper weights for the links. Considering this issue while designing networks will make them more robust against cascading failures.

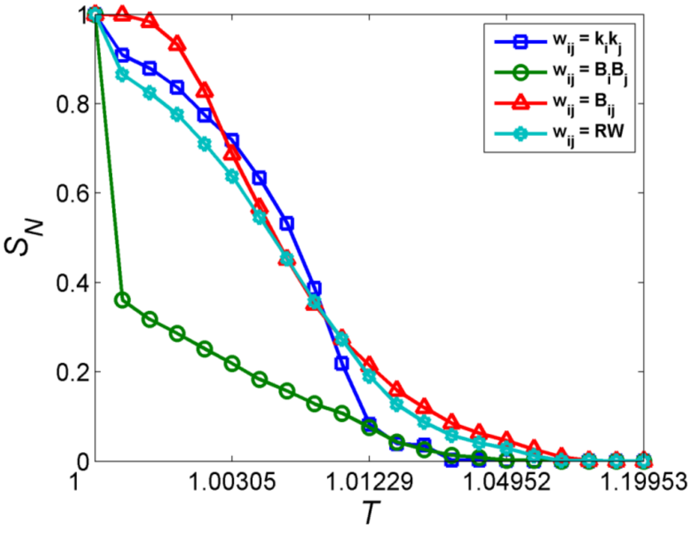

Fig. 3. S_N as a T for the US airports network. The cyan line shows the changes in the S_N for real weights. Other designations are as Fig. 2.

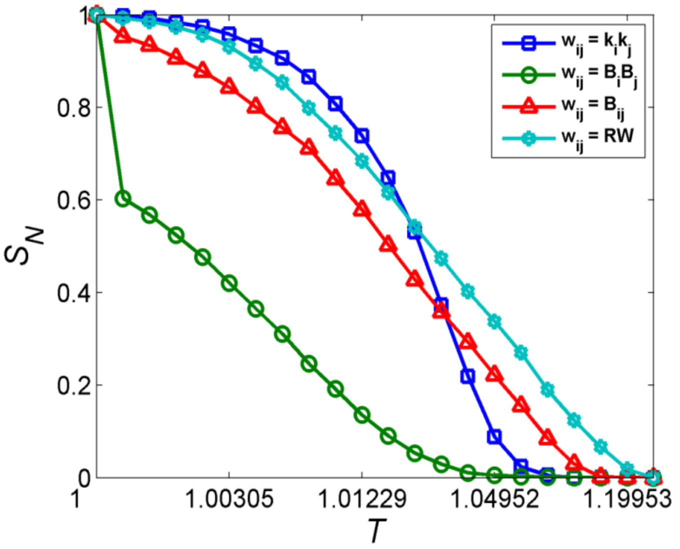

Fig. 4. S_N as a T for the central European rail network. Other designations are as Fig. 3.

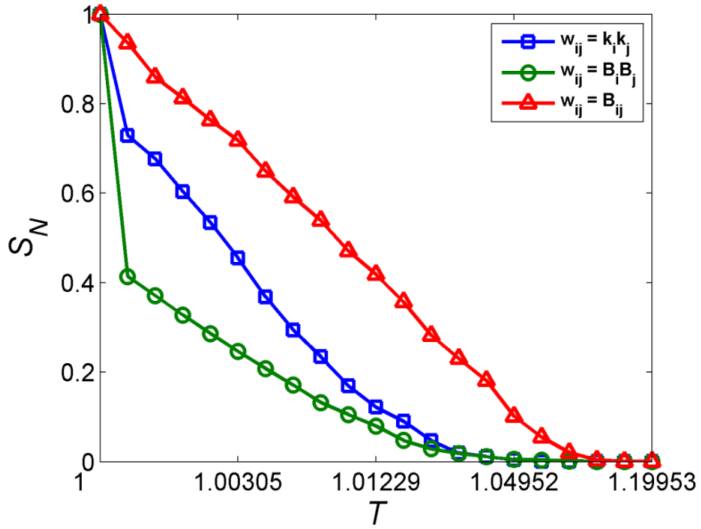

Fig. 5. S_N as a T for the network of the Internet in the level of autonomous system. Other designations are as Fig. 2

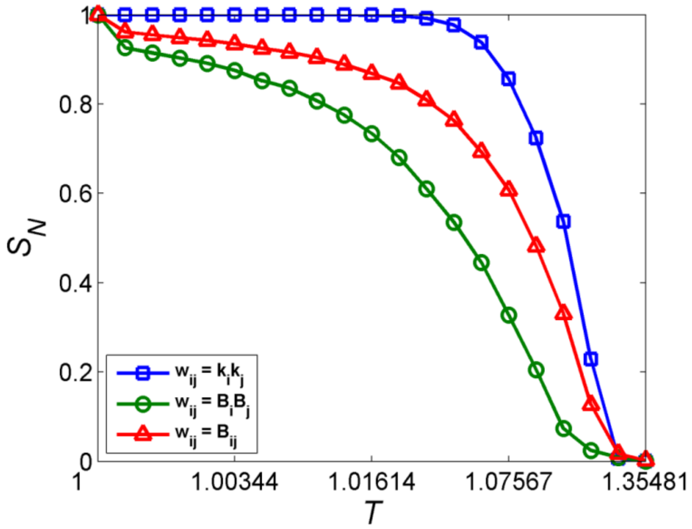

Fig. 6. S_N as a T for the electrical power grid. Other designations are as Fig. 2.

VI. Conclusion

Networks might undergo random or systematic failures in their components. If the components have limited capacity, these failures might lead to a cascade of failures throughout the network and make it lose its proper functionality. Robustness of a network against systematic attacks is an important issue in the field of complex network. In this article, we investigated the profile of the robustness against cascaded failures in weighted networks. A number of model networks as well as real-world one were considered and weighted through different strategies including: the betweenness centrality of the edges, the product of the degrees of the end nodes and the product of the betweenness centrality of the end nodes. Furthermore, the load of the edges was considered to be as their weights and their capacity as a functional of the initial loads, i.e. the initial weight multiplied by some threshold value. By employing the local weighted flow redistribution rule, i.e. redistribution of the load of the broken edge among the neighboring edges proportional to their load, we investigated the average avalanche size and the critical threshold in the networks weighted through different strategies. We found that the networks weighted through the product of the betweenness centrality of the nodes had the best robustness both in case of avalanche size and the critical threshold. The effectiveness of this weighting strategy in improving the robustness of the networks was more pronounced in scale-free networks as compared to small-world and random ones. For some networks, it might be possible to design the connection weights (i.e. loads) and considering our results can make them more robust against cascading failures.

A downside of the weighting based on the node betweenness centrality might be its larger computational complexity as compared to the one based on the degrees. However, recently Ercsey-Ravasz and Toroczkai showed that the betweenness centrality can be well approximated in a local manner [46]. Using this approach, betweenness centrality can be approximately computed for large scale networks with a low computational cost. This makes the weighting based on the node betweenness centralities practical to ameliorate the robustness of large-scale networks against cascaded failures.

VII. References

1. Wang, X.F. and G. Chen, *Complex networks: small-world, scale-free and beyond.* IEEE Circuits and Systems Magazine, 2003. **3**(1): p. 6-20.
2. Tam, W.M., F.C.M. Lau, and C.K. Tse, *Complex-network modeling of a call network.* IEEE Transactions on Circuits and Systems—I: Fundamental theory ad Applications, 2009. **56**(2): p. 416-429.
3. Chen, M.Y., *Chaos synchronization in complex networks. IEEE Transactions on Circuits and Systems-I*, 2008. **55**: p. 1335-1346.
4. J. H. Lu, X.H.Y., G. R. Chen, and D. Z. Cheng, *Characterizing the synchronizability of small-world dynamical networks. IEEE Transactions on Circuits and Systems-I: Fundamental theory ad Applications*, 2004. **51**: p. 787-796.
5. Arenas, A., et al., *Synchronization in complex networks.* Physics Report, 2008. **469**(3): p. 93-153.
6. Olfati-Saber, R., J.A. Fax, and R.M. Murray, *Consensus and cooperation in networked multi-agent systems.* Proceedings of the IEEE, 2007. **95**(1): p. 215 - 233.
7. Albert, R., H. Jeong, and A.-L. Barabasi, *Error and attack tolerance of complex networks.* Nature, 2000. **406**: p. 378-382.
8. Crucitti, P., et al., *Efficiency of scale-free networks: error and attack tolerance.* Physica A, 2003. **320**: p. 622-642.
9. Sun, S., et al., *Error and attack tolerance of evolving networks with local preferential attachment.* Physica A, 2007. **373**: p. 851-860.
10. Barkai, N. and S. Leibler, *Robustness in simple biochemical networks.* Nature, 1997. **387**: p. 913-917.
11. Xia, Y. and D.J. Hill, *Attack vulnerability of complex communication.* IEEE Transactions on Circuits and Systems—II: Express Briefs, 2008. **55**(1): p. 65-69.
12. Buldyrev, S.V., et al., *Catastrophic cascade of failures in interdependent networks.* Nature, 2010. **464**: p. 1025-1028.
13. Motter, A.E. and Y.-C. Lai, *Cascade-based attacks on complex networks.* Physical Review E, 2002. **66**: p. 065102.
14. Sachtjen, M.L., B.A. Carreras, and V.E. Lynch, *Disturbances in a power transmission system.* Phycisal Review E, 2000. **61**: p. 4877-4882.
15. Marbukh, V., *Can TCP metastability explain cascading failures and justify flow admission control in the Internet?*, in *International Conference on Telecommunications*. 2008, IEEE: St. Petersburg, Russia. p. 1-6.
16. Crucitti, P., V. Latora, and M. Marchiori, *Model for cascading failures in complex networks.* Physical Review E, 2004. **69**: p. 045104.
17. Zhao, L., K. Park, and Y.-C. Lai, *Attack vulnerability of scale-free networks due to cascading breakdown.* Physical review E, 2004. **70**: p. 035101.
18. Xia, Y., J. Fan, and D. Hill, *Cascading failure in Watts-Strogatz small-world networks.* Physica A, 2010. **389**: p. 1281-1285.
19. Babaei, M., H. Ghassemieh, and M. Jalili, *Cascading failure tolerance of modular small-world networks.* IEEE Transactions on Circuits and Systems—II: Express Briefs, 2011. **Accepted**.
20. Wang, W.X. and G. Chen, *Universal robustness characteristic of weighted networks against cascading failure.* Physical Review E, 2008. **77**(2): p. 026101.
21. Barabasi, A.-L. and R. Albert, *Emergence of scaling in random networks.* Science, 1999. **286**: p. 5009-5012.
22. Newman, M.E.J. and D.J. Watts, *Renormalization group analysis of the small-world network model.* Physics Letters A, 1999. **263**(4-6): p. 341-346
23. Erdős, P. and A. Rényi, *On the evolution of random graphs.* Publication of the Mathematical Institute of the Hungarian Academy of Sciences, 1960. **5**: p. 17-61.
24. Wu, Z.-X., et al., *Cascading failure spreading on weighted heterogeneous networks.* Journal of Statistical Mechanics: Theory and Experiment, 2008. **5**: p. P05013.
25. S. Mei, Y.N., G. Wang, and S. Wu, *A study of self-organized criticality of power system under cascading failures based on AC-OPF with voltage stability margin. IEEE Transactions on Power Systems*, 2008. **23**: p. 1719-1726.
26. Dobson, H.R.a.I., *Using transmission line outage data to estimate cascading failure propagation in an electric power system. IEEE Transactions on Circuits and Systems-II: Express Briefs*, 2008. **55**: p. 927-931.
27. Holme, P. and B.J. Kim, *Attack vulnerability of complex networks.* Phys. Rev. E, 2002. **65**: p. 056109.
28. Freeman, L.C., *Set of measures of centrality based on betweenness.* Siociometry, 1977. **40**(1): p. 35-41.
29. http://vlado.fmf.uni-lj.si/pub/networks/data/mix/USAir97.net.
30. Colizza, V., R. Pastor-Satorras, and A. Vespignani, *Reaction–diffusion processes and metapopulation models in heterogeneous networks.* Nature Physics, 2007. **3**(4): p. 276-282.
31. Knuth, D.E., *The Stanford GraphBase: a platform for combinatorial computing*. 1993: AcM Press.
32. Newman, M.E.J., *Finding community structure in networks using the eigenvectors of matrices.* Physical Review E, 2006. **74**(3): p. 036104.
33. Bernard, H.R. and P.D. Killworth, *Informant accuracy in social network data II.* Human Communication Research, 1977. **4**(1): p. 3-18.
34. Albert, A.-L.B.a.R., *Emergence of Scaling in Random Networks.* Science, 1999. **286**(5439): p. 509-512.
35. Newman, M.E.J. and D. Watts, *Renormalization group analysis of the small-world network model.* Physics Letters A, 1999. **263**(4-6): p. 341-346.
36. Rényi, P.E.a.A., *On the evolution of random graphs* Publ. Math. Inst. Hung. Acad. Sci. , 1959. **5**: p. 17-60.
37. Girvan, M. and M.E.J. Newman, *Community structure in social and biological networks.* Proceedings of the National Academy of Science of the United States of America, 2002. **99**(12): p. 7821-7826.
38. Newman, M.E.J., *Modularity and community structure in networks.* Proceedings of National Academy of Science of USA, 2006. **103**: p. 8577-8582.
39. Barrat, A., et al., *The architecture of complex weighted networks.* Proceedings of the National Academy of Sciences of the United States of America, 2004. **101**(11): p. 3747.
40. Yook, S.H., H. Jeong, and A.L. Barabasi, *Modeling the Internet's large-scale topology.* Proc. Nat'l Academy of Sciences, 2002. **99**: p. 13382-13386.
41. Kurant, M. and P. Thiran, *Layered complex networks.* Physical review letters, 2006. **96**(13): p. 138701.
42. Watts, D.J. and S.H. Strogatz, *Collective dynamics of 'small-world'networks.* Nature, 1998. **393**(6684): p. 440-442.
43. Howson, C. and P. Urbach, *Scientific reasoning: The Bayesian approach.* . 1993: Open Court Publishing, Ls sale, IL.
44. Nikoloski, Z., N. A Deo, and L. A Kucera. *Degree-correlation of a Scale-free Random Graph Process*. in *Proceedings of the European Conference on Combinatorics, Graph Theory and Applications*. 2005.
45. Zhuang-Xiong, H., W. Xin-Ran, and Z. A Han, *Pair correlations in scale-free networks.* Chinese Physics, 2004. **13**(3): p. 273-278.
46. Ercsey-Ravasz, M. and Z. Toroczkai, *Centrality scaling in large networks.* Physical review letters. **105**(3): p. 38701.