Cascaded failures in weighted networks

Baharan Mirzasoleiman, Mahmoudreza Babaei, Mahdi Jalili,* and MohammadAli Safari
Department of Computer Engineering, Sharif University of Technology, Tehran, Iran
(Received 14 August 2011; published 25 October 2011)

Many technological networks can experience random and/or systematic failures in their components. More destructive situations can happen if the components have limited capacity, where the failure in one of them might lead to a cascade of failures in other components, and consequently break down the structure of the 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 United States 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 product of the betweenness centrality of the end nodes is favored for the robustness of the network against cascaded failures.

DOI: 10.1103/PhysRevE.84.046114 PACS number(s): 89.75.Fb, 89.75.Hc

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]. One of the topics that has attracted much attention in this context is the robustness of networks against random and systematic component failures [5–7]. Networks might undergo failures in a number of their components (i.e., nodes and edges) and consequently lose proper functionality [8,9]. 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 [5,10]. For example, the hub nodes might be targets for 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 [11].

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 normal daily life and result in chaos in the society. Evidence has shown that locally emerging random or systematic failures in networks can influence the entire network, often resulting in large-scale collapse in the network. Examples include large blackouts in the United States due to failure in the power grid [12] and breakdowns of the internet [13]. Indeed, a cascaded failure has happened in such cases [9,11].

Several studies have been devoted to the concept of controlling cascaded failures [14–17]. For example, islanding or separating the survivable parts of a grid has long been used to allow a transmission grid to continue its functionality. Building a system for allocating competing resources during an extended failure is another solution for controlling such failures. While these are applicable solutions, they cannot eliminate all failures [15]. Therefore, it is desired to design a network that is robust against cascaded failures. The influence of the cascaded failure in the size of the largest connected component has been investigated in a number of network models including preferential attachment scale-free [18], Watts-Strogatz small-world [19], and modular networks [20]. In many of the studies, as a component fails, the loads are recalculated and the components whose loads exceed their capacity are removed from the network. The process is repeated until the loads of all remaining components are below their capacity [18–20]. However, this might not be realistic in some applications. For example, let us 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 has been proposed [21]. In this model, the cascaded failure is triggered by removing the edge with the maximal load. 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 the local weighted flow redistribution rule, Wang and Chen found the strongest robustness against cascaded failure at a specific weighting strength [21].

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 the cascaded effect of failures in the edges. Furthermore, the

*Corresponding author: mjalili@sharif.edu

networks were weighted according to different rules due to the fact that many real-world networks are inherently weighted. We used three weighting strategies: the betweenness centrality of the edges, the product of the degrees of the end nodes, and the product of their betweenness centrality. The numerical simulations were performed on a number of model networks such as preferential attachment scale-free [22], Newman-Watts small-world [23], Erdős-Rényi [24], and modular networks [20]. 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 United States 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

The local weighted flow redistribution rule (LWFRR) has been recently introduced and studied by Wang and Chen [21]. In this model, when an edge is subject to an attack and removed from the network, the flow passing through this edge is redistributed to its nearest-neighbor edges [21,25]. As a consequence, the load of each neighbor edge increases proportional to its weight. More precisely,

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

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., $C_{ij} = \mathrm{T}w_{ij}$). That is, there exists a constant threshold value $\mathrm{T} > 1$ such that if

$$F_{im} + \Delta F_{im} > T w_{im} = C_{im} \tag{2}$$

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., $F_{uv} > T w_{uv}$).

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 anymore. 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 [26,27]. Protecting electrical grids against failures and a society against spread of an infectious disease are other examples where the studies in this context can be beneficial. 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 travel from populated regions prevents the widespread 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 might be pushed beyond their capacity and become overloaded; thus get broken and shift their load onto other neighboring 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. 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 [28]. 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 that 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 the introduction of 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 [29]. More precisely,

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

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 larger the betweenness centrality of a node is, the more its significance in the formation of the shortest paths in the network.

Another measure of centrality is edge betweenness centrality, which 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} [29], that is,

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

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 [21] used node degrees to model the traffic on a network and studied 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-world networks. According to their definition, the weight of an edge is modeled by

$$w_{ij} = (k_i k_j)^{\theta}, \tag{6}$$

where k_i is the degree of node i and θ is a tuning parameter. They showed that $\theta = 1$ leads to the strongest robustness on various networks [21].

We introduce a 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 this 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 on 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

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

In this method, the weight of an edge has a power-law dependence on the product of betweenness centrality of 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 with the weights introduced through Eqs. (6) and (7). We showed the correlation between the above weighting strategies in a number of real-world networks including:

US airlines. An airlines connection network in the USA consists of 332 nodes and 1063 edges. The weights correspond to the number of seats available on the scheduled flights [30].

US airports network. This is the network of the 500 busiest commercial airports in the USA. The weights correspond to the number of seats available on the scheduled flights [31]. This network has 2980 edges.

Lesmis. Coappearance network of characters in the novel *Les Miserables*. This network has 77 nodes and 127 edges [32].

Netscience. Coauthorship network of scientists working in the field of network theory and experiment. This network contains 1589 nodes and 1371 edges [33].

Bkham. The network of human interactions in bounded groups and on the actors' ability to recall those interactions. This network consists of 44 nodes and 153 edges [34].

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, $B_i B_j$, and the product of the degree of the end nodes $k_i k_j$. 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) are not necessarily the edge betweenness centrality and can be appropriately designed. Next we investigate which of the weighting strategies has the best robustness against cascaded failures.

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.

TABLE I. Person correlation coefficients between real weights and different metrics including the betweenness centrality of the edges B_{ij}, the product of the betweenness centrality of the end nodes, $B_i \mathrm{B}_j$, and the product of the degree of the end nodes $k_i \mathrm{k}_j$ in a number of real-world networks.

Network	Correlation with $B_i B_j$	Correlation with $k_i k_j$	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