Cascading Failure Tolerance of Modular Small-World Networks

Mahmoudreza Babaei, Hamed Ghassemieh, and Mahdi Jalili, *Member, IEEE*

***Abstract*—Many real-world networks have a modular structure, and their component may undergo random errors and/or intentional attacks. More devastating situations may happen if the network components have a limited load capacity; the errors and attacks may lead to a cascading component removal process, and consequently, the network may lose its desired performance. In this brief, we investigate the tolerance of cascading errors and attacks in modular small-world networks. This brief studies the size of the largest connected component of the networks when cascading errors or attacks occur. The robustness of the network is tested as a function of both the intermodular connection and intramodular rewiring probabilities, i.e., the rewiring probability of original Watts–Strogatz networks that the individual modules are based on. We find that intermodular connections play an important role in determining the robustness of the networks against cascading failures. We also study cascaded failure in a number of real networks with different modularity levels and find that the more the modularity level of a network, the less its robustness against cascaded failures.**

***Index Terms*—Betweenness centrality measure, cascading failure, modular networks, robustness, small-world networks.**

I. Introduction

COMPLEX networks have attracted a great deal of attention in the past decade, and many of their applications have been explored [1]. A number of universal features are common in various real-world networks, e.g., many of these networks show a small-world property [2]. These common properties influence the evolution of a dynamical process happening on the networks [3]. Complex networks may undergo component variations, and one of the important features of many engineering and biological networks is robustness against component tolerances [4].

Much of the infrastructures in modern societies are based on complex networks, and failure in the component of such networks may cause a lot of troubles in the infrastructures' performance and servicing issues. For example, large blackouts may happen in power networks as a consequence of accidental or intentional attacks [5], and thus, the network structure should be designed in a way that allows the network to have proper resiliency against such attacks. The component failure in complex networks is, in general, of two types, namely, the failure of randomly chosen components (nodes and/or edges), i.e., errors, and the intentional failure in components with special property such as those with high degrees, i.e., attacks [6], [7]. Networks undergoing intentional attacks may also experience a more catastrophic situation when cascading failures happen [8], [9]. Indeed, when the intrinsic dynamics of network flows are taken into account, the intentional removal of network components can have a much more devastating consequence than the case of normal errors [9]. There are various examples of such cascade failures in technological systems such as power systems and the Internet [10]–[12]. Many real-world systems may be interdependent networks, where failure of nodes in one network may lead to failure of dependent nodes in other networks, i.e., cascade of failures [7].

A simple mechanism of cascaded failure might be as following [8], [9], [13]. The network loses the node with the highest amount of load. As the component is removed from the network, its load is redistributed in the network. This redistribution may cause some components to exceed their capacity and, consequently, be removed from the network. This repeated process may end up with a network with lost functionality, e.g., a disconnected network.

The cascade failures have been investigated in a number of model networks, including scale-free [14] and Watts–Strogatz small-world [15] ones. Several measures have been proposed for measuring the robustness of the networks against attacks and errors. The size of the largest connected component and/or the efficiency of communication in the network are typical measures for such a purpose [6]. As a random or intentional cascaded attack occurs in the networks, its efficiency and/or the size of the largest connected component is monitored. The profile of the variations of these parameters as a function of the attack parameters displays the robustness of the network against such attacks.

Many real-world networks have a modular structure. In this brief, we investigate the cascaded failure in modular small-world networks. The considered modular networks consist of densely connected modules, each with the Watts–Strogatz network structure [2]. Furthermore, the modules are sparsely interconnected. We investigate the influence of cascaded failures on the size of the largest connected component of the network as a function of two important parameters of the modular networks, i.e., the intramodular rewiring probability of the Watts–Strogatz model and the probability of existing intermodular links. We find that the probability of intermodular connections has the dominant influence.

II. Modular Small-World Networks

Many real-world systems show a modular structure in their underlying connection network characterized by dense

Manuscript received August 18, 2010; revised December 10, 2010, February 7, 2011 and April 18, 2011; accepted May 2, 2011. Date of publication July 5, 2011; date of current version August 17, 2011. This paper was recommended by Associate Editor I. Belykh.

The authors are with the Department of Computer Engineering, Sharif University of Technology, Tehran 11365-9363, Iran (e-mail: mjalili@sharif.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSII.2011.2158718

intramodular connections, whereas the intermodular connections are sparse [16]. In this brief, we consider the modular Watts–Strogatz networks, where each module has the Watts–Strogatz network structure. Furthermore, the nodes in each module communicate with the nodes of other models with a uniform intermodular probability.

Watts and Strogatz in their seminal paper [2] discovered that many real-world networks are neither random nor regular but somewhere in between, and they proposed a method for constructing such networks, i.e., Watts–Strogatz networks [2], [17]. Indeed, many real-world networks have a structure that falls between the structure of purely random and regular graphs. Watts–Strogatz networks have a characteristic path length as small as the pure random graphs (scales by $\log N$). At the same time, their clustering coefficient is comparable with that of the regular graphs, which is much more than that of the random graphs [2]. For the construction of Watts–Strogatz networks, we have used the original random rewiring algorithm proposed by Watts and Strogatz [2]. Consider a ring graph with N nodes each connected to its m-nearest neighbors by undirected edges. The edges are renamed from 1 to M, where M is the total number of edges in the network that is $M = 2mN$. The rewiring algorithm runs for M steps, and at step i, edges i are selected and rewired with probability P, provided that self-loops and multiplication of edges are prohibited. The resulting graph is such that, for the value of $P = 0$, we will have the original ring graph, whereas the value of $P = 1$ produces a pure random graph. Essentially, the average degree will be $\langle k \rangle = 2m$. This rewiring probability is indeed the intramodular rewiring probability in the modular network model.

In order to construct modular networks, first, n isolated modules, each with the Watts–Strogatz structure with the same N, m, and P, are constructed. Then, with probability P_{inter}, intramodular links are disconnected, and intermodular connections are created. In other words, with probability P_{inter}, each intramodular link is disconnected, and a connection is created between a randomly chosen node of a randomly chosen module i and another randomly chosen node of a randomly chosen module j, where $i \neq j$. This way, the average degree of the network is kept constant at $2m$. For some small values of P_{inter}, the resulting network would be a modular network in the sense that it will have dense intramodular connections, whereas the intermodular connections are sparse.

III. Random and Intentional Cascading Failures

When nodes are sensitive to overloading, massive breakdowns over the network are significant. If removal of a small fraction of nodes or even of a single node starts from the network either by a random error or an intentional attack, the balance of flows changes. In other words, as a number of nodes are removed as a consequence of errors or attacks, the loads are calculated again, neglecting the removed nodes. Therefore, after the occurrence of the error/attack, the traffic that was making use of the removed nodes has to find other components to go through. As a consequence, a global redistribution of loads over the entire network pans out. In some cases, this overloading flow is not tolerated by some of the network components, and it may cause triggering a cascade of overload failures [9], [13], [15], [18].

Cascading failure is a process in which removing of nodes continues until there is no overloaded nodes in the network. In other words, the failure causes another redistribution of the traffic load. Indeed, the network components can bear the flows up to a range. If a random error or an intentional attack occurs in a number of components, the betweenness centrality of the nodes and edges has to be recalculated. The components with the values of the betweenness centrality more than their capacity will essentially fail. This process is repeated until all components have allowed an amount of load. The cascade failure might make the network lose its functionality, e.g., to be disconnected or inefficient.

The component removal might be random or intentional. The random failure in the network components is called error, whereas the intentional failure is called attack. There are a number of criteria to choose a node to attack. For example, one strategy is to remove the hub nodes with the highest degree. Another strategy is to select those with high betweenness centrality and remove them from the network. In cascading failures, often the latter is used, i.e., when an intentional attack occurs in the network, a node with the highest value of the betweenness centrality measure is removed from the network [9], [13], [15], [18]–[20].

Motter and Lai have introduced a simple model for cascades of overload failures [9]. This model is based on the assumption that the relevant quantity is exchanged between every couple of nodes and transmitted along the shortest path connecting them. The number of packets a node i can tolerate at time t is equal to its betweenness centrality $b_i(t)$. Node betweenness centrality b_i is a centrality measure of the ith node in a graph, which counts the number of shortest paths making use of that node (except shortest paths between the ith and other nodes) [21]. More precisely

$$b_i = \Sigma_{p \neq i \neq q} \left(\Gamma_{pq}(i)/\Gamma_{pq}\right) \tag{1}$$

where Γ_{pq} is the number of shortest paths from the pth to the qth node, and $\Gamma_{pq}(i)$ is the number of these shortest paths making use of the ith node.

Node i is characterized by a limited capacity, which is defined as maximum load C_i that the node can handle [9]. This implies that, if $b_i(t) \leq C_i$, for all i (i.e., $i = 1, 2, 3 \ldots N$, where N is the network size), then the network works in free flow, which means that the network works without overloaded nodes. The capacity of a node is assumed to be proportional to the initial load of the node. In other words

$$C_i = (1 + \alpha) \cdot b_i(t = 0) \tag{2}$$

with $1 \geq \alpha \geq 0$, where α is a tolerance parameter of the network. Under this condition (i.e., $1 \geq \alpha \geq 0$ and $t = 0$) no node is overloaded, and the system is working accurately.

It should be mentioned that the linear relation between the load and the capacity is not always the case in real systems [22]. Due to weak efficiency of resource allocation in many real networks, they have large unoccupied portions of capacities [22]. Although the load–capacity relation in real systems is nonlinear, here we considered a linear relation that is valid in large value of the load [22].

The shortest paths between the nodes change by removing the nodes, and as a consequence, overloading on a number of nodes may occur. Since the overloaded nodes cannot tolerate their load, all of them are simultaneously removed from the network. Removing all the overloaded nodes again changes the distribution of the load, and a number of new nodes may overload with the new load distribution. Then, the overloaded nodes are removed from the network. The process of overloading, as well as removing the new nodes and redistribution, goes on until, at a certain time t, all the remaining nodes satisfy the condition $b_i(t) \leq C_i$. At this time, no further node is removed from the network, and the network reaches its steady state. The size of the largest connected component of the final network is used as a measure of the robustness of the network against the error/attack; the larger the size of the largest connected component of the network, the better its robustness in response to the error/attack.

It has been shown that the robustness of the networks against random errors is better than that against intentional attacks [9], [13]. Furthermore, degree and load heterogeneity are important factors influencing the degree of robustness of a network against error/attack. For example, scale-free networks that are typical for their degree-heterogeneous behavior are robust in response to random cascading errors while showing fragility against intentional cascading attacks [15]. Watts–Strogatz networks that are degree homogeneous show a shadow of the profile of the scale-free networks in response to cascading failure that is mainly linked to their heterogeneous load distribution [15]. Whereas, Erdös–Rényi graphs that are pure random networks are robust against both random and intentional cascading failures [15].

IV. Simulation Results

In order to investigate the robustness of modular small-world networks against cascading errors or attacks, we performed a number of computer simulations. In our simulations, we constructed modular networks with five modules, each based on the Watts–Strogatz model. The modules had 150, 200, 250, 300, and 350 nodes and 300, 400, 500, 600, and 700 edges, respectively. We were interested in the dependence of the size of the largest connected component on two network parameters, namely, the intermodular connection P_{inter} and the rewiring probabilities P of the Watts–Strogatz model within each module. To have better statistics, each simulation was repeated 20 times, and the averages were displayed.

Fig. 1 shows the normalized size of the largest connected component G, i.e., the size of the largest connected component of the network divided by the size of the original network, as a function of the tolerance parameter α and the intermodular connection probability P_{inter} for modular small-world networks. The rewiring probability of the Watts–Strogatz model in each module was fixed at $P = 0.2$. As it is shown, as tolerance parameter α increases, and hence, the capacity of the nodes increases, G increases, i.e., the robustness of the network enhances. This is expected somehow, since by increasing the capacity of the nodes, fewer nodes are removed, and the connected component of the final steady-state network has more connected nodes. The robustness of the network against the cascading random errors [see Fig. 1(b)] is much better compared with that against the cascading intentional attacks [see Fig. 1(a)]. In other words, the situations, where the profile of G is 1 in the random error cases, are much more than those in the intentional attacks.

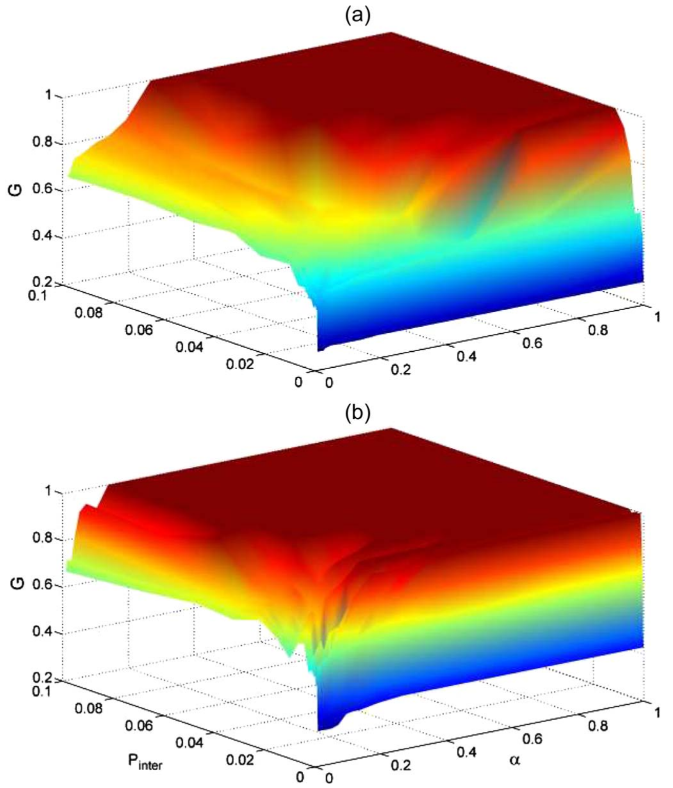

Fig. 1. Normalized size of the largest connected component G as a function of the tolerance parameter α and the intermodular connection probability P_{inter} for modular small-world networks. The modular networks have five modules with 150, 200, 250, 300, and 350 nodes and 300, 400, 500, 600, and 700 edges, respectively. The rewiring probability of the Watts–Strogatz model in each module is fixed at $P = 0.2$. The results are (a) for cascading intentional attack and (b) for cascading random error. Data show averages over 20 realizations.

In order to better illustrate the influence of the intermodular connection probability on the network robustness, the profile of G as a function of α was displayed for a number of small and high values of P_{inter} (see Fig. 2). It is shown that by increasing P_{inter}, the robustness of the network is improved in response to both random and intentional failures. As P_{inter} increases, the number of intermodular links also increases. These links carry a large amount of load, and thus, the heterogeneity of the network decreases by increasing P_{inter}. As a result, as more cascading attacks happen, fewer nodes are removed due to their limited capacity. Therefore, modular networks with larger number of intermodular links have better robustness against intentional attacks. Surprisingly, although less pronounced, the same story is true for the random errors [see Fig. 1(b)]. Scale-free networks, which are heterogeneous graphs, showed a robust behavior in response to cascading random errors, and their heterogeneity played no role in the amount of robustness against random failures [9], [14], [15], [20]. Whereas, networks with decreased heterogeneity, i.e., increased P_{inter}, showed improved robustness [see Fig. 2(b)].

We further investigated the dependence of cascading error/attack vulnerability on the rewiring probability P of the Watts–Strogatz model in Fig. 3(a) and (b). P determines the degree of intramodular heterogeneity and, to a less extent, the degree of the heterogeneity of the whole network. In order to perform the

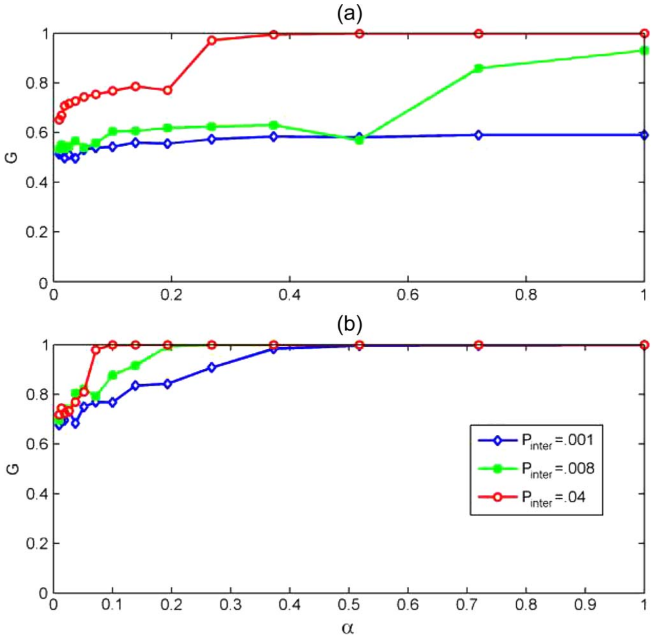

Fig. 2. Normalized size of G as a function of tolerance parameter α and small/large values of P_{inter}. The network parameters are as Fig. 1. The results are (a) for cascading intentional attack and (b) for cascading random error. Data show averages over 20 realizations.

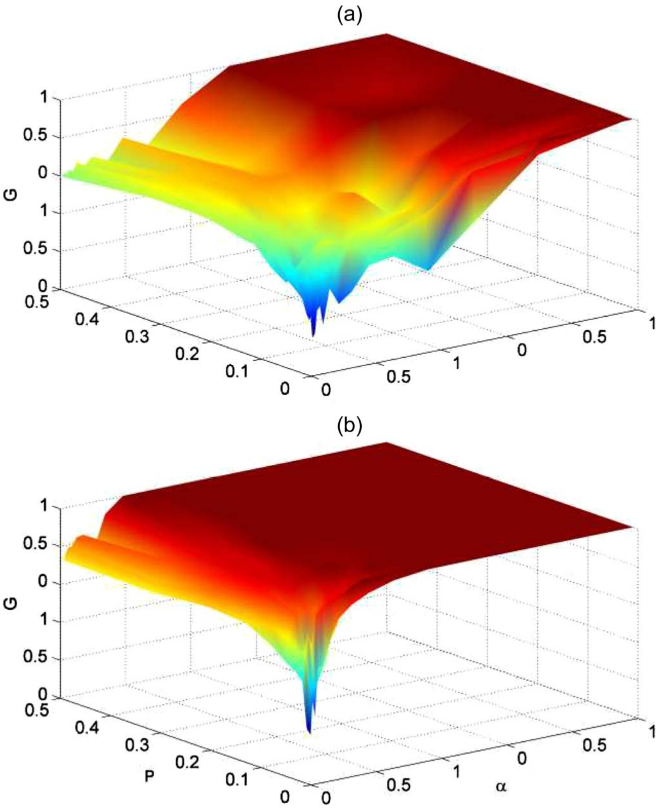

Fig. 3. Normalized size of G as a function of the tolerance parameter α and the rewiring probabilities P of the Watts–Strogatz model. The network parameters are as Fig. 1, and the intermodular connection probability is fixed at $P_{\text{inter}} = 0.002$. The results are (a) for cascading intentional attack and (b) for cascading random error. Data show averages over 20 realizations.

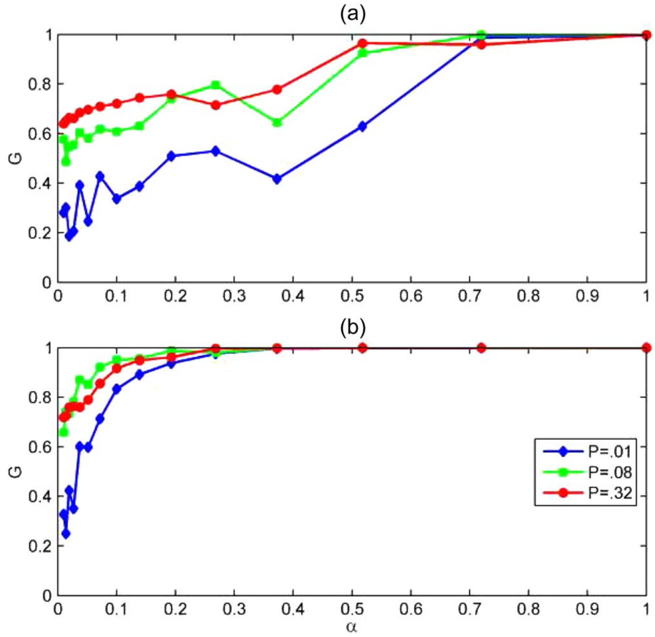

Fig. 4. Normalized size of G as a function of tolerance parameter α and small/large values of P. The network parameters are as Fig. 3. The results are (a) for cascading intentional attack and (b) for cascading random error. Data show averages over 20 realizations.

simulations, we fixed the intermodular connection probability at $P_{\text{inter}} = 0.002$. Fig. 4 shows the normalized size of the largest connected component G as a function of α and P for attacks and errors, respectively. Similar to the previous case, the robustness against random errors is much better than that of the case when intentional attacks occur. It is shown that by increasing P, the robustness slightly improved both for random errors and intentional attacks. We know that as P increases, the intramodular degree heterogeneity also increases; however, the same is not true for the load distribution [15]. Unlike scale-free networks, where increasing heterogeneity worsens robustness against attacks, increasing P in small-world networks, i.e., which itself increases heterogeneity, enhances robustness. These results are in agreement with those of [15], where this behavior has been linked to the heterogeneity in the load distribution.

We also applied the cascading failure strategy to a number of real networks with small-world connectivity and different levels of modularity (MO) (see Fig. 5). The small-worldness (SW) of the networks was calculated using the algorithm proposed in [26]. Networks with SW larger than one tend to have small-world connectivity; however, the larger a network is, the more its SW is [26]. The algorithm proposed by Newman [27] was used to maximize the MO of the networks, in which larger values of the MO shows a stronger MO structure in the network. As it is shown from the results, the stronger the MO structure in a network is, i.e., the more the MO, the more the influence of the cascade is (see Fig. 5). The results show that the community structure in the networks, in general, decreases its robustness against the cascaded failures.

A number of methods have been proposed to control the effect of a cascaded failure by reducing the size of cascades of overload failures [28], [29]. For example, the size of the cascade can be drastically reduced by intentionally removing the nodes having small load and/or edges having large excess of load [28]. Our results showed that modular networks are more vulnerable to cascading failures. It would be interesting

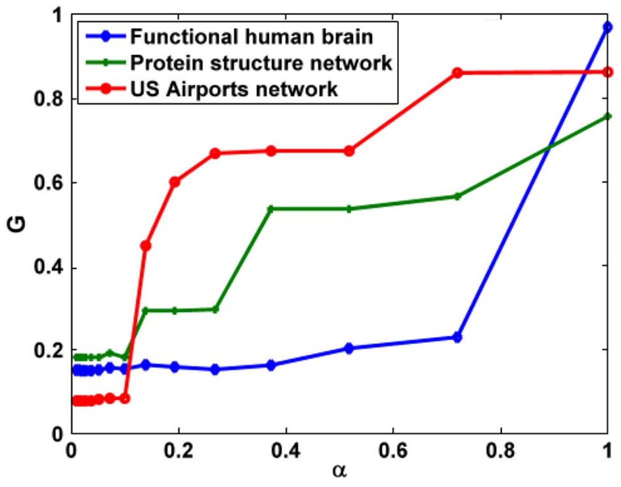

Fig. 5. Normalized size of G as a function of the tolerance parameter α for real networks. The networks are the protein structure [23] $(MO = 0.65, \mathrm{SW} = 5)$, unweighted version of the US airports [24] $(MO = 0.27, \mathrm{SW} = 21.76)$, and the brain functional networks extracted from functional magnetic resonance imaging [25] $(MO = 0.74, \mathrm{SW} = 35.73)$.

to investigate whether they are easier to control or not. Easily controllable networks will lead them to be effectively more robust in response to cascading failures.

V. Conclusion

In this brief, we have investigated the robustness profile of modular small-world networks against cascading random errors and intentional attacks. We used Watts–Strogatz networks to construct each module. Furthermore, with probability P_{inter}, the intramodular links were disconnected, and intermodular connections were created, keeping the average degree of the network unchanged. The normalized size of the largest connected component of the networks was studied as a function of the intermodular connection probability P_{inter} and the intramodular rewiring probability P of the Watts–Strogatz model. Although P_{inter} and P do not have the same influence on the structural parameters of the network, they showed the same influence on the network robustness against cascading random errors and intentional attacks. However, the influence of P_{inter} was more pronounced, as compared with P, since it is the main factor determining the heterogeneity level of the network. Therefore, the robustness of modular networks against cascading failures is mainly characterized by intermodular links. We have also investigated a number of real networks and found a direct relation between their MO and the influence of cascaded failures, i.e., networks with strong MO were sensitive to failures.

References

[1] X. F. Wang and G. Chen, "Complex networks: Small-world, scale-free and beyond," *IEEE Circuits Syst. Mag.*, vol. 3, no. 1, pp. 6–20, First Quarter, 2003.

[2] D. J. Watts and S. H. Strogatz, "Collective dynamics of "small-world" networks," *Nature*, vol. 393, no. 6684, pp. 440–442, Jun. 1998.

[3] M. Y. Chen, "Chaos synchronization in complex networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 55, no. 5, pp. 1335–1346, Jun. 2008.

[4] N. Barkai and S. Leibler, "Robustness in simple biochemical networks," *Nature*, vol. 387, no. 6636, pp. 913–917, Jun. 1997.

[5] S. Arianos, E. Bompard, A. Carbone, and F. Xue, "Power grid vulnerability: A complex network approach," *Chaos*, vol. 19, no. 1, p. 013119, Mar. 2009.

[6] R. Albert, H. Jeong, and A.-L. Barabasi, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, Jul. 2000.

[7] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, pp. 1025–1028, Apr. 2010.

[8] Y. Xia and D. J. Hill, "Attack vulnerability of complex communication," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 55, no. 1, pp. 65–69, Jan. 2008.

[9] A. E. Motter and Y.-C. Lai, "Cascade-based attacks on complex networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 66, no. 6, p. 065102, Dec. 2002.

[10] S. Mei, Y. Ni, 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 Trans. Power Syst.*, vol. 23, no. 4, pp. 1719–1726, Nov. 2008.

[11] H. Ren and I. Dobson, "Using transmission line outage data to estimate cascading failure propagation in an electric power system," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 55, no. 9, pp. 927–931, Sep. 2008.

[12] V. Marbukh, "Can TCP metastability explain cascading failures and justify flow admission control in the Internet?," in *Proc. Int. Conf. Telecommun.*, St. Petersburg, Russia, 2008, pp. 1–6.

[13] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 69, no. 4, p. 045104, Apr. 2004.

[14] L. Zhao, K. Park, and Y.-C. Lai, "Attack vulnerability of scale-free networks due to cascading breakdown," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 70, no. 3, p. 035101, Sep. 2004.

[15] Y. Xia, J. Fan, and D. Hill, "Cascading failure in Watts–Strogatz small-world networks," *Phys. A*, vol. 389, no. 6, pp. 1281–1285, Mar. 2010.

[16] M. Girvan and M. E. J. Newman, "Community structure in social and biological networks," *Proc. Nat. Acad. Sci. U.S.A.*, vol. 99, no. 12, pp. 7821–7826, Jun. 2002.

[17] D. J. Watts, *Small Worlds: The Dynamics of Networks Between Order and Randomness.*, 1st ed. Princeton, NJ: Princeton Univ. Press, 2003.

[18] A. G. Smart, L. A. N. Amaral, and J. M. Ottino, "Cascading failure and robustness in metabolic networks," *Proc. Nat. Acad. Sci. U.S.A.*, vol. 105, no. 36, pp. 13 223–13 228, Sep. 2008.

[19] R. Yang, W.-X. Wang, Y.-C. Lai, and A. G. Chen, "Optimal weighting scheme for suppressing cascades and traffic congestion in complex networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 79, no. 2, p. 026112, Feb. 2009.

[20] W.-X. Wang and Y.-C. Lai, "Abnormal cascading on complex networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 80, no. 3, p. 036109, Sep. 2009.

[21] L. C. Freeman, "Set of measures of centrality based on betweenness," *Sociometry*, vol. 40, no. 1, pp. 35–41, Mar. 1977.

[22] D. Kim and A. E. Motter, "Resource allocation pattern in infrastructure networks," *J. Phys. A: Math. Theor.*, vol. 41, no. 22, p. 224 019, Jun. 2008.

[23] R. Milo, S. Itzkovitz, N. Kashtan, R. Levitt, S. Shen-Orr, I. Ayzenshtat, M. Sheffer, and U. Alon, "Superfamilies of evolved and designed networks," *Science*, vol. 303, no. 5663, pp. 1538–1542, Mar. 2004.

[24] V. Colizza, A. Barrat, M. Barthelemy, and A. Vespignani, "Prediction and predictability of global epidemics: The role of the airline transportation network," *Proc. Nat. Acad. Sci. U.S.A.*, vol. 103, pp. 2015–2020, 2006.

[25] A. Zalesky, A. Fornito, I. H. Harding, L. Cocchi, M. Yücel, C. Pantelis, and E. T. Bullmore, "Whole-brain anatomical networks: Does the choice of nodes matter?" *NeuroImage*, vol. 50, no. 3, pp. 970–983, Apr. 2010.

[26] M. D. Humphries and K. Gurney, "Network 'small-world-ness': A quantitative method for determining canonical network equivalence," *PLoS ONE*, vol. 3, no. 4, p. e0002051, Apr. 2008.

[27] M. E. J. Newman, "Fast algorithm for detecting community structure in networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 69, no. 6, p. 066133, Jun. 2004.

[28] A. E. Motter, "Cascade control and defense in complex networks," *Phys. Rev. Lett.*, vol. 93, no. 9, p. 098 701, Aug. 2004.

[29] M. Schafer, J. Scholz, and M. Greiner, "Proactive robustness control of heterogeneously loaded networks," *Phys. Rev. Lett.*, vol. 96, no. 10, p. 108 701, Mar. 2006.