Journal of Zhejiang University SCIENCE A
ISSN 1673-565X (Print); ISSN 1862-1775 (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

Cascading failures in local-world evolving networks*

Zhe-jing BAO[†1], Yi-jia CAO[1,2]

([1]*School of Electrical Engineering, Zhejiang University, Hangzhou 310027, China*)

([2]*College of Electrical and Information Engineering, Hunan University, Changsha 410082, China*)

[†]E-mail: zjbao.zju@gmail.com

Received May 1, 2008; revision accepted Aug. 17, 2008

Abstract: The local-world (LW) evolving network model shows a transition for the degree distribution between the exponential and power-law distributions, depending on the LW size. Cascading failures under intentional attacks in LW network models with different LW sizes were investigated using the cascading failures load model. We found that the LW size has a significant impact on the network's robustness against deliberate attacks. It is much easier to trigger cascading failures in LW evolving networks with a larger LW size. Therefore, to avoid cascading failures in real networks with local preferential attachment such as the Internet, the World Trade Web and the multi-agent system, the LW size should be as small as possible.

Key words: Complex network, Local world (LW), Cascading failures, Power-law, Attack
doi:10.1631/jzus.A0820336 **Document code:** A **CLC number:** N94; TP393

INTRODUCTION

In recent years, the discovery of scale-free properties of many natural and artificial complex networks, achieved by the pioneering Barabási-Albert (BA) model (Barabási and Albert, 1999), has stimulated a great deal of interest in studying the underlying growth mechanisms and the functioning of complex networks (Dorogovtsev *et al.*, 2000; Dorogovtsev and Mendes, 2002; Barrat *et al.*, 2004a; 2004b). Li and Chen (2003) made significant progress in research on scale-free evolving network models. These models represent an important feature in the evolution of many real-world complex networks, including the Internet, the World Trade Web (WTW), the protein-protein interaction network, etc. The researchers suggested that the preferential attachment mechanisms work only within a local world (LW) of each node and not the global network as in the BA model, and investigated an evolving model based on LW preferential linking. The LW model shows a transition between exponential network and power-law scale-free network with respect to connectivity distribution by varying the LW size.

The behavior and dynamics of complex networks have recently attracted the attention of researchers in different areas (Albert *et al.*, 2000; Motter and Lai, 2002; Zhao *et al.*, 2004; Sun *et al.*, 2007). Scale-free networks are robust yet fragile: they are robust against random failures of nodes but fragile to intentional attacks, the effect of cascades. Cascading failures are initiated when a heavily loaded node is lost for some reason, and the load on that node must be redistributed to other nodes, as a result subsequent failures can occur. This step-by-step process is what we call a 'cascading failure', or a 'cascade'. It can stop after a few steps but it can also propagate and shutdown a considerable fraction of the whole network. Cascading failures have been observed in many real large-scale infrastructure networks. For instance, in October 1986 during the first documented Internet congestion collapse, the speed of the connection between the Lawrence Berkeley Laboratory and the University of California at Berkeley, two places

* Project supported by the National Basic Research Program (973) of China (No. 2004CB217902), the National Natural Science Foundation of China (Nos. 60421002 and 60804045) and the Postdoctoral Science Foundation of China (No. 20070421163)

separated by only 200 m, dropped by a factor 100 (Jacobson, 1988; Guimerà *et al.*, 2002). On 14 August 2003 an initial disturbance in Ohio triggered the largest blackout in U.S. history, in which millions of people remained without electricity for as long as 15 h (Glanz and Perez-Pena, 2003). Cascading failures in complex networks, caused by either random breakdowns or intentional attacks, have been studied (Crucitti *et al.*, 2004; Zhao *et al.*, 2005; Lai *et al.*, 2005; Xu and Wang, 2005; Wu *et al.*, 2006). Such studies have focused mainly on the properties of the scale-free networks and Erdös-Rényi (ER) random graphs, showing that the removal of a group of nodes altogether can have important consequences. Sun *et al.* (2007) presented only a static analysis on the topological aspects of the LW networks' response under node removal, without considering the effect of cascading failures. To our knowledge, there are no publications concerning cascading failures in LW evolving networks. The robustness of networks generated by the LW model, which is a measure of how well these networks work under intentional attacks, is of great concern because the local preferential attachment mechanism is common to many real-life complex systems.

In this paper, based on the recently addressed problem of 'local world' and 'cascades' in complex networks, we attempt to explore the cascading failures in LW evolving networks and study the effect of LW size on cascades by introducing the cascade failures load model to the LW complex network.

LOCAL-WORLD EVOLVING MODEL

The LW evolving network model originated from the BA scale-free model. It differs from the BA scale-free model and some other models, in that it introduces a novel preferential attachment mechanism—local preferential attachment (Li and Chen, 2003). In local preferential attachment, the linking probability between the new node and node i is valued only within the LW of the new node. The local preferential attachment mechanism captures the localization effect of real-world complex networks. For example, in the Internet a router in one autonomous system (AS) will favor a connection of the shortest path within the same AS (Sun *et al.*, 2007); and in the WTW an enterprise always wants to contact those companies within its relevant business fields (Xuan *et al.*, 2007). These phenomena indicate the existence of preferential attachment mechanisms within LW rather than within the whole network.

The iterative algorithm of an LW evolving model, proposed by Li and Chen (2003), is described as follows:

(1) Growth: starting from a small number m_0 of isolated nodes, at each time step t, add a new node with m edges connecting to the network.

(2) Local preferential attachment: at each time step t, before connecting the new incoming node to m existing nodes, randomly select M nodes referred to as the LW; then, add edges between the new node and m nodes in the LW. The linking probability between the new node and node i in the LW is

$$\Pi_{\text{loc}}(i)=\frac{M}{m_0+t}\frac{k_i}{\sum_{\text{loc}}k_j}. \tag{1}$$

After T steps (the designed total iteration steps), the algorithm results in a connected network with $N=m_0+T$ nodes and $E=mT$ links. Thus, the average node degree is $\langle k\rangle=2m$.

According to the algorithm above, the parameter M contributes to the connectivity pattern of the final network. It is obvious that at every time step t, with respect to M there are two limiting cases in the LW evolving network model: $M=m$ and $M=t+m_0$.

Case A: $M=m\ll T$. In this limiting case, the preferential attachment in the LW does not take effect; at the same time, the LW is randomly selected. Consequently, the model results in an exponentially decayed degree distribution, as $P(k)\sim e^{-k/m}$.

Case B: $M\geq t+m_0$. In this special case, at each time step, the LW is the same as the whole network. Hence, the LW model reduces to a BA scale-free model with $P(k)\sim k^{-3}$.

Li and Chen (2003) have given the analytical expression of degree distribution based on the mean-field theory for the LW model. Varying LW size M, the model shows a transition for degree distribution between the exponential and power-law distributions. Especially when $m\ll M\ll m_0+t$, the model can follow a power-law degree distribution as the BA scale-free model.

CASCADING FAILURES LOAD MODEL FOR THE LOCAL-WORLD MODEL

We consider the model of overload failures introduced by Motter and Lai (2002). For a given network W, suppose that at each time step one unit of a physical quantity, a so-called 'packet' (which can be information, energy, etc.) is sent from node i to node j, for every ordered pair of nodes (i, j) belonging to the same connected component of W. We assume that the packet is transmitted along the shortest path connecting nodes i and j. If there is more than one shortest path connecting two given nodes, the packet is divided evenly at each branching point (Motter, 2004). The load L_k on a node k is the total amount of packets passing that node per unit of time. Let S_k denote the connected component of node k and $L_k^{(i,j)}$ denote the contribution of the ordered pair (i, j) to the load on k. The load on node k is then

$$L_k = \sum_{i,j} L_k^{(i,j)}, \tag{2}$$

where the sum is over all ordered pairs of nodes in S_k. Each node k is assigned a finite capacity C_k. The capacity of a node is the maximum load that the node can handle. In man-made networks, the capacity is severely limited by cost. The node operates in a normal state if $L_k \le C_k$; otherwise the node is assumed to fail and is removed from the network. Now consider that $W=W(0)$ is an initially connected network. The initial load $L_k=L_k(0)$ is given by Eq.(2) with $S_k=W(0)$. It is natural to assume that the capacity C_k of node k is proportional to its initial load $L_k(0)$:

$$C_k = (1+\alpha)L_k(0), \quad k = 1, 2, ..., N, \tag{3}$$

where $\alpha \ge 0$ is the tolerance parameter, and N is the number of nodes in the network.

A cascade can be regarded as a step-by-step process, initiated by an intentional attack. We start with $W=W(0)$ at time 0. The condition $\alpha \ge 0$ guarantees that all nodes of $W(0)$ operate in normal states. It is assumed that a deliberate attack on the node with the largest load is performed at time 1. Thus, the removal of the node changes the distribution of the shortest paths. As a result, the loads of a fraction of nodes increase and become larger than their corresponding capacities, and then these overloaded nodes are removed simultaneously from $W(0)$ and the resulting network is denoted by $W(1)$. The removals lead to a global redistribution of loads among the remaining nodes in the network. Consequently, the updated load $L_k(1)$ on node k of $W(1)$ may become larger than the capacity C_k. A new round of the removal of the overloaded nodes from $W(1)$ occurs and the resulting network is denoted by $W(2)$, and so on. This cascading process stops at time n when the loads of all nodes of $W(n)$ satisfy $L_k(n) \le C_k$.

Usually, the propagation of cascading failures is investigated to demonstrate a network's robustness against deliberate attacks. The LW size M contributes to the connectivity pattern of the network, and therefore probably has a significant impact on the propagation of cascading failures. Furthermore, from the cascading failures load model, we can see that the damage size of a cascading failure is closely related to the tolerance parameter α. In the following, we will discuss the relationship between the cascading failures of the LW network and the model parameters M and α by simulation. The damage caused by a cascade is quantified by measuring three kinds of properties as follows:

(1) The relative size S of the largest connected component, defined as

$$S=N'/N, \tag{4}$$

where N and N' are the number of nodes in the largest component before and after the cascade, respectively.

(2) The properties of isolated clusters, including the total number N_s of isolated clusters and the average size $\langle s \rangle$ of isolated clusters that break off the main network.

(3) The global efficiency e of the unconnected network, defined as the average of the efficiencies over all couples of nodes:

$$e = \frac{1}{N(N-1)} \sum_{i \ne j} \frac{1}{d_{ij}}, \tag{5}$$

where d_{ij} is the shortest path length between nodes i and j, and N is the number of nodes in the network. If there is no path between i and j, $d_{ij}=+\infty$.

We will investigate how the model parameters M and α affect these four measured quantities S, N_s, $\langle s \rangle$ and e when an LW evolving network is deliberately attacked.

In simulation, cascading failures are triggered by removing the node with the largest load. We performed numerical simulations with different parameter values of N, m_0, m, M and α. Here, we show the simulation results with $m_0=m=2$, $N=2000$ and different values of M and α, i.e., M=2, 10, 20, 100, 200, 2000 and α=0, 0.1, 0.2, ..., 0.9. The relative size S of the largest connected component, the global efficiency e of the network, the average size $\langle s \rangle$ and the total number N_s of isolated clusters are shown in Figs.1, 2, 3 and 4, respectively, to characterize the cascading failures.

Fig.1 shows the transitional cascading failure behaviors of the LW model with different LW sizes M under a deliberate attack. With the same M the relative size S of the largest connected component increases as α increases, which is in agreement with intuition. With the same α, the measured quantity S increases as M decreases. This result is reasonable because the network becomes more and more homogeneous with the decrease of M. Thereby, the network becomes more and more robust against the deliberate attack.

Fig.2 also illustrates the conclusion that with the same α the scale of damage caused by cascading failures decreases in terms of global efficiency, as M decreases. The transitional cascading failure behaviors of the LW model are somewhat different from those in Fig.1 when $\alpha \geq 0.7$. The reason is that in the cases of M=2, 10 the largest connected component is larger than 0.9 when $\alpha \geq 0.7$. Then the zero efficiencies of node pairs with no path connecting them contribute less to the global efficiency e. Consequently the global efficiency e depends mainly on the largest connected component, and the efficiency of the largest connected component increases with the increase of M, determined by the statistical property of the LW evolving model.

As shown in Fig.3, when M=2, 10 the average size $\langle s \rangle$ of isolated clusters fluctuates a little; and when $M \geq 20$ with the increase of α from 0 to 0.9, $\langle s \rangle$ first increases to a peak value when α=0.1, and then decreases. We first discuss the cases of α=0 and α=0.9. At α=0, the scale of damage caused by cascading failure is very large and the relative size S of the largest connected component is almost equal to 0

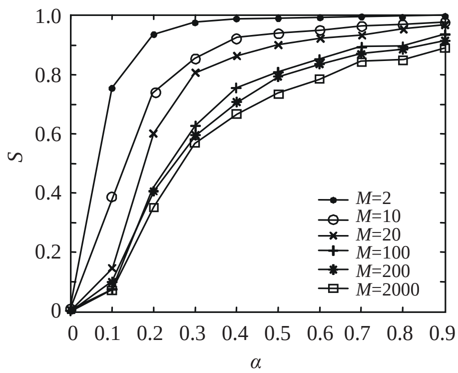

Fig.1 Relative size of the largest connected component under deliberate attack vs the tolerance parameter *α*

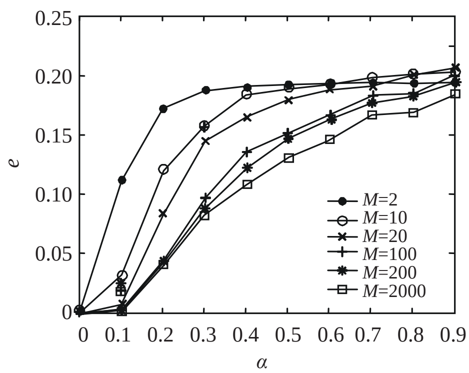

Fig.2 Global efficiency of the unconnected network under deliberate attack vs the tolerance parameter *α*

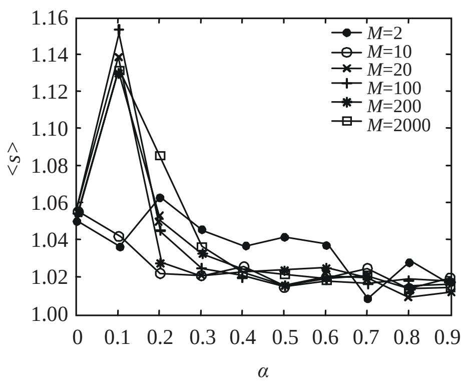

Fig.3 Average size of isolated clusters under deliberate attack vs the tolerance parameter *α*

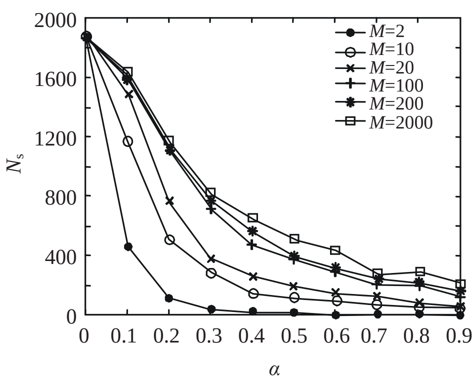

Fig.4 Total number of isolated clusters under deliberate attack vs the tolerance parameter *α*

(Fig.1), thus <s> is near 1. At α=0.9, single nodes break off from the main body, so <s>≈1. At α=0.1, in the cases of M≥20 the relative size S of the largest connected component is about 0.1 (Fig.1) and there are some isolated clusters with larger sizes, therefore <s> peaks.

Fig.4 also shows that the transitional cascading failure behaviors of the LW model depend on M. At α=0, it is easy for the failure to propagate throughout the entire network and large numbers of small pieces fall off the main system, so N_s is nearly equal to the size N of the network.

CONCLUSION

We investigated the cascading failures in LW evolving network models with different LW sizes using a cascading failures load model. Three kinds of properties were used to characterize the damage of a cascading failure triggered by removing the node with the largest load. Simulation results indicated that the size of the LW has a significant impact on the network's robustness against deliberate attacks and that it is much easier for the failures to propagate in the LW evolving network with a larger LW size. This result suggests that to avoid cascading failures in real networks with local preferential attachment, the LW size should be as small as possible.

In this study, we assume that all the nodes have the same tolerance parameter α. However, recent research indicates a nonlinear relationship between the capacity and the load of some real complex networks (Kim and Motter, 2008), which may further increase the frequency of overloads compared with those predicted in this paper. Therefore, our further work will focus on cascading failure dynamics in LW evolving networks with the fluctuation-driven capacity distribution introduced by Kim and Motter (2008).

References

Albert, R., Jeong, H., Barabási, A.L., 2000. Error and attack tolerance of complex networks. *Nature*, **406**:378-382. [doi:10.1038/35019019]

Barabási, A.L., Albert, R., 1999. Emergence of scaling in random networks. *Science*, **286**:509-512. [doi:10.1126/science.286.5439.509]

Barrat, A., Barthélemy, M., Satorras, R.P., Vespignani, A., 2004a. The architecture of complex weighted networks. *PNAS*, **101**:3747-3752. [doi:10.1073/pnas.0400087101]

Barrat, A., Barthélemy, M., Vespignani, A., 2004b. Weighted evolving networks: coupling topology and weight dynamics. *Phys. Rev. Lett.*, **92**(22):228701. [doi:10.1103/PhysRevLett.92.228701]

Crucitti, P., Latora, V., Marchiori, M., 2004. Model for cascading failures in complex networks. *Phys. Rev. E*, **69**(4):045104. [doi:10.1103/PhysRevE.69.045104]

Dorogovtsev, S.N., Mendes, J.F., 2002. Evolution of networks. *Adv. Phys.*, **51**(4):1079-1187. [doi:10.1080/00018730110112519]

Dorogovtsev, S.N., Mendes, J.F., Samukhin, A.N., 2000. Structure of growing networks with preferential linking. *Phys. Rev. Lett.*, **85**(21):4633-4636. [doi:10.1103/PhysRevLett.85.4633]

Glanz, J., Perez-Pena, R., 2003. 90 Seconds That Left Tens of Millions of People in the Dark. *New York Times*, August 26, New York.

Guimerà, R., Arenas, A., Díaz-Guilera, A., Giralt, F., 2002. Dynamical properties of model communication networks. *Phys. Rev. E*, **66**(2):026704. [doi:10.1103/PhysRevE.66.026704]

Jacobson, V., 1988. Congestion avoidance and control. *ACM SIGCOMM Comput. Commun. Rev.*, **18**(4):314-329. [doi:10.1145/52325.52356]

Kim, D.H., Motter, A.E., 2008. Fluctuation-driven capacity distribution in complex networks. *New J. Phys.*, **10**(5):053022. [doi:10.1088/1367-2630/10/5/053022]

Lai, Y.C., Motter, A., Nishikawa, T., Park, K., Zhao, L., 2005. Complex networks: dynamics and security. *Pramana-J. Phys.*, **64**(4):483-502. [doi:10.1007/BF02706197]

Li, X., Chen, G.R., 2003. A local-world evolving network model. *Phys. A*, **328**(1-2):274-286. [doi:10.1016/S0378-4371(03)00604-6]

Motter, A.E., 2004. Cascade control and defense in complex networks. *Phys. Rev. Lett.*, **93**(9):098701. [doi:10.1103/PhysRevLett.93.098701]

Motter, A.E., Lai, Y.C., 2002. Cascade-based attacks on complex networks. *Phys. Rev. E*, **66**(6):065102. [doi:10.1103/PhysRevE.66.065102]

Sun, S.W., Liu, Z.X., Chen, Z.Q., Yuan, Z.Z., 2007. Error and attack tolerance of evolving networks with local preferential attachment. *Phys. A*, **373**:851-860. [doi:10.1016/j.physa.2006.05.049]

Wu, J.J., Gao, Z.Y., Sun, H.J., 2006. Cascade and breakdown in scale-free networks with community structure. *Phys. Rev. E*, **74**(6):066111. [doi:10.1103/PhysRevE.74.066111]

Xu, J., Wang, X.F., 2005. Cascading failures in scale-free coupled map lattices. *Phys. A*, **349**(3-4):685-692. [doi:10.1016/j.physa.2004.10.030]

Xuan, Q., Li, Y.J., Wu, T.J., 2007. A local-world network model based on inter-node correlation degree. *Phys. A*, **378**(2):561-572. [doi:10.1016/j.physa.2006.11.070]

Zhao, L., Park, K., Lai, Y.C., 2004. Attack vulnerability of scale-free networks due to cascading breakdown. *Phys. Rev. E*, **70**(3):035101. [doi:10.1103/PhysRevE.70.035101]

Zhao, L., Park, K., Lai, Y.C., Ye, N., 2005. Tolerance of scale-free networks against attack-induced cascades. *Phys. Rev. E*, **72**(2):025104. [doi:10.1103/PhysRevE.72.025104]