Vol 18 No 11, November 2009
1674-1056/2009/18(11)/4754-06

Chinese Physics B

© 2009 Chin. Phys. Soc.
and IOP Publishing Ltd

Cascading failures in congested complex networks with feedback*

Zheng Jian-Feng(郑建风)[a)†], Gao Zi-You(高自友)[a)‡],
Fu Bai-Bai(傅白白)[b)], and Li Feng(李 峰)[b)]

[a)] *Institute of System Science, School of Traffic and Transportation, Beijing Jiaotong University, Beijing* 100044, *China*

[b)] *State Key Laboratory of Rail Traffic Control and Safety, Beijing Jiaotong University, Beijing* 100044, *China*

(Received 14 November 2008; revised manuscript received 7 March 2009)

In this article, we investigate cascading failures in complex networks by introducing a feedback. To characterize the effect of the feedback, we define a procedure that involves a self-organization of trip distribution during the process of cascading failures. For this purpose, user equilibrium with variable demand is used as an alternative way to determine the traffic flow pattern throughout the network. Under the attack, cost function dynamics are introduced to discuss edge overload in complex networks, where each edge is assigned a finite capacity (controlled by parameter α). We find that scale-free networks without considering the effect of the feedback are expected to be very sensitive to α as compared with random networks, while this situation is largely improved after introducing the feedback.

Keywords: complex networks, cascading failures, feedback

PACC: 0560

1. Introduction

Complex networks arise in natural systems and they are also an essential part of modern society. Many real complex networks were found to be heterogeneous with power-law degree distribution.[1−3] The scale-free character of these networks gives rise to many unexpected results in many properties, as compared with regular networks or random networks.[3] Because of the ubiquity of scale-free networks in natural and manmade systems, the security of these networks has been of great interest. In Ref.[4], it is demonstrated that scale-free networks possess a robust-yet-fragile property. That is, they are robust against random failures of nodes but fragile to intentional attacks. In addition, the absence of percolation[5] also prompts an exceptional tolerance to random failures.

The above properties of scale-free networks only refer to the static topological connectivity properties. On the other hand, in communication networks such as the Internet, many instabilities are due to traffic congestion or load redistribution. That is, the traffic load carried on the overloaded nodes or edges is automatically diverted to alternative paths on the networks and instabilities can spread by an avalanche of traffic congestions. These instabilities are thus of a dynamical nature and depend on how objects (e.g. information, etc.) are routed and distributed in the network. Recently, there have been many studies on cascading failures generated by the redistribution of traffic load due to edge or node overload in complex networks.[6−13]

Unlike previous studies, we introduce a feedback procedure during the process of cascading failures in complex networks. In order to clearly describe the feedback, we can take urban traffic networks for example to illustrate how the feedback affects the operation of traffic dynamics during the process of cascading failures. When traffic congestion occurs, (i.e., cascading failures occur) it may result in traffic accidents, or some traffic facilities may be destroyed. As a result, some users may decide to shift the time of travel, or forgo some trips altogether, in order to avoid the congestion. This problem statement suggests that we

*Project partly supported by National Basic Research Program of China (Grant No 2006CB705500), National Natural Science Foundation of China (Grant Nos 70631001, 70671008 and 70801005) and the Innovation Foundation of Science and Technology for Excellent Doctorial Candidate of Beijing Jiaotong University (Grant No 48033).

†Corresponding author. E-mail: zhengjianfeng002@163.com

‡Corresponding author. E-mail: zygao@center.njtu.edu.cn

ought to focus on finding a suitable or variable trip distribution in order to relieve the congestion of the network. This line of thinking leads us to define a feedback procedure that involves a self-organization of trip distribution to relieve the congestion during the process of cascading failures. An alternative way is that, different from betweenness centrality,[14] we introduce user equilibrium with variable demand[15] to determine traffic flow pattern. In the case of user equilibrium with variable demand, the trip distribution can be seriously affected by increased traffic flows or congestion. As a result, when congestion develops, the trip distribution can be suitably transformed.

As will be shown below, our main finding is that the effect of the feedback can effectively reduce the discrepancy of cascading failures between random networks and scale-free networks.

The rest of this paper is organized as follows: Section 2 provides a description of traffic dynamics and definitions. Simulations and results are given in Section 3. Finally, some summaries and conclusions are shown in Section 4.

2. Traffic dynamics and definitions

The proposed feedback procedure for cascading failures is depicted in Fig.1, where the dotted arrow corresponds to the case of process for cascading failures investigated in many previous studies, such as Refs.[6]–[13]. It is clear that the feedback procedure involves a self-organization of trip distribution. As mentioned above, the feedback can be described by user equilibrium with variable demand, which will be introduced below.

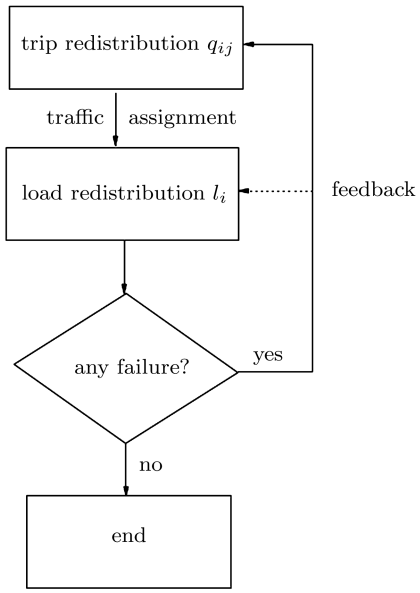


Fig.1. Feedback procedure for cascading failures in complex networks. The dotted arrow corresponds to the case without considering the effect of the feedback, which is considered in previous studies on cascading failures.

2.1. User equilibrium with variable demand

Betweenness centrality (BC) is often used to estimate the load on the node or edge in many previous studies. In this paper, we introduce user equilibrium to determine the load on the node. Based on user equilibrium, the effect of congestion is introduced to affect the route choice strategy. So we hope that the congestion of some important nodes or edges may be largely relieved, leading to an efficient transport.

The demand, q_{rs} (i.e., the trip distribution mentioned above), between every origin–destination (O–D) pair r–s in the network can be assumed to be a function of travel time between r and s. In other words,

$$q_{rs} = D_{rs}(\omega_{rs}) \forall r, s, \tag{1}$$

where ω_{rs} is the minimum travel time between r and s, and $D_{rs}(\cdot)$ is the demand function between r and s. Typically, the form of the demand function will be the same for all O–D pairs.

User equilibrium with variable demand can be described by a mathematical program,[15] given as:

$$\min Z(\boldsymbol{X}, q) = \sum_{(i,j)} \int_0^{x_{ij}} w_{ij}(x)\ \mathrm{d}x - \sum_{rs} \int_0^{q_{rs}} D_{rs}^{-1}(x)\ \mathrm{d}x, \tag{2}$$

$$\text{s.t.} \sum_k f_k^{rs} = q_{rs}\ \forall r, s, \tag{3}$$

$$f_k^{rs} \geq 0\ ,\quad \forall r, s, k, \tag{4}$$

$$q_{rs} \geq 0\ ,\quad \forall r, s, \tag{5}$$

$$x_{ij} = \sum_r \sum_s \sum_k f_k^{rs} \delta_{ij,k}^{rs},\ \forall i, j, \tag{6}$$

where $\boldsymbol{X}$ is the matrix of link flow x_{ij} on the link (i, j), q is the matrix of O–D demand q_{rs}, $w_{ij}(\cdot)$ is the cost function, which maps link flow to travel time on the link (i, j), $D_{rs}^{-1}(\cdot)$ is the inverse of the demand function associated with O–D pair r–s, the path flow f_k^{rs} is the flow of the path k connecting origin r and

destination s, $\delta_{ij,k}^{rs} = 1$ if link (i,j) is a part of path k, and $\delta_{ij,k}^{rs} = 0$ otherwise. Equation (2) is the objective function, viewed as a mathematical construct utilized to solve equilibrium problems. Equation (3) represents a set of flow conservation constraints that the flow on all paths connecting each r–s pair has to equal its traffic volume. The nonnegativity conditions in Eqs.(4) and (5) are required to ensure that the solution of the program will be physically meaningful. Equation (6) means that the flow on each link is the sum of flows on all paths going through the link.

The effect of congestion can be described by cost functions, in which BPR (the Bureau of Public Roads) formula[16] is the most widely used,

$$w_{ij} = w_{ij}^0 \left(1 + a\left(\frac{x_{ij}}{C_{ij}}\right)^b\right), \tag{7}$$

where $a = 0.15$ and $b = 4$ are typically used, w_{ij}^0 denotes the cost on the link (i,j) when there is no flows, C_{ij} is the 'practical capacity' of link (i,j).

2.2. The model and definitions

Unlike most previous studies, we investigate edge overload rather than node overload, since we assume that traffic flows (e.g., vehicles) always travel on the edge and may chose another edge at the node without any delay.

Let $x_{ij}(t)$ denote the total flow passing through the edge (i,j) at time t. Each edge is characterized by a capacity defined as the maximum flow that edge can handle. Similar to Ref.[6], we assume the capacity Ce_{ij} of edge (i,j) to be proportional to its initial flow x_{ij}^0:

$$Ce_{ij} = (1+\alpha)x_{ij}^0, \quad \forall i,j, \tag{8}$$

where constant $\alpha \geq 0$ is the tolerance parameter. When all edges are in normal states, each edge has its initial flow. But the attack to the network in general changes the distribution of the flow, i.e., the flow on the edge will be recalculated. If it increases and becomes larger than the capacity, the edge fails. Any failure leads to a new recalculation of flow on every edge, and as a result, subsequent failures can occur. In addition, due to any overload, each object (e.g., vehicles or information, etc) will use an alternative path to avoid the congestion. For this purpose, similar to Refs.[7] and [12], we consider cost function dynamics as follows,

$$C_{ij}(t+1) = \begin{cases} C_{ij}(0)\dfrac{Ce_{ij}}{x_{ij}(t)}, & \text{if } x_{ij}(t) > Ce_{ij}, \\ C_{ij}(0), & \text{if } x_{ij}(t) \leq Ce_{ij}, \end{cases} \tag{9}$$

where $C_{ij}(0)$ is the initial 'practical capacity' of link (i,j).

Note that Eq.(9) in the present article is quite different from that in Refs.[7] and [12]. In Refs.[7] and [12], researchers investigated cascading failures due to node overload, i.e., congestion occurs at the node. When congestion occurs at a node, all objects (e.g., vehicles) may make a detour to avoid all edges connecting to the congested node, regardless of the congestion of edges. That is, those un-congested edges will also be avoided if they are connecting to a congested node, which may reduce the efficiency of the network. According to the above equation, it is clear that we focus on diverting traffic flows only on congested edges.

To measure the performance of the network we consider three quantities, the efficiency of the network E, the degree of congestion of the network FC, and the number of overloaded edges in the network Num. Following Ref.[17], the efficiency of the network is defined as

$$E = \frac{2}{N(N-1)} \sum_{i>j} \frac{1}{\omega_{ij}}, \tag{10}$$

where N is the size of the network. Following Refs.[12] and [15], the degree of congestion of the network is expressed as

$$\mathrm{FC} = \frac{\sum_{i>j} x_{ij} w_{ij}}{\sum_{i>j} x_{ij} w_{ij}^0}. \tag{11}$$

In the following, we will illustrate how the tolerance parameter affects three quantities in random and scale-free networks.

3. Simulations and results

In our simulations, we consider random networks and scale-free networks. The network size is $N = 1000$, and the average degree is $\langle k \rangle = 6$. Random networks can be generated by the binomial model,[2] where each pair of nodes is linked with probability $\langle k \rangle / N$. To generate scale-free networks, we use the standard Barábasi–Albert (BA) scale-free model.[1] For simplicity, for each link (i,j), $C_{ij}(0) = 1$ and $w_{ij}^0 = 1$ are typically considered. In general, the demand function between r and s can be expressed as

$q_{rs} = A_r B_s f(\omega_{rs})$, where A_r and B_s are known parameters associated with origin r and destination s, respectively, and $f(\omega_{rs})$ is a monotonically decreasing function of ω_{rs} . Here we consider a simple form, given as

$$q_{rs} = k_r k_s \frac{1}{\omega_{rs}^2}, \tag{12}$$

where k_r and k_s are the degrees of node r and s, respectively. All the resulting data are averaged over 10 realizations. In order to study cascading failures under attack, we focus on removing a single node with the largest degree in the network.

In order to clearly show the operation of the feedback procedure, we firstly investigate cascading failures in complex networks for the case without considering the effect of the feedback, i.e., the case of the dotted arrow in Fig.1. User equilibrium with fixed unity demand[15] is typically considered. The simulations are plotted in Fig.2. The results are compared between random networks and scale-free networks, since the topology effect may play an important role in instabilities. For comparison, we show the ratios of different indices in Figs.2 and 3, where $E(0.6)$, FC(0) and Num(0) mean $E(\alpha = 0.6)$, FC($\alpha = 0$) and Num($\alpha = 0$), respectively. For random networks, E basically stays in a steady state, independent of tolerance parameter α, while for scale-free networks, E is expected to monotonously increase with the tolerance parameter α. In other words, scale-free networks are very sensitive to the tolerance parameter α. The other two quantities reflect similar behaviour: FC is also independent of tolerance parameter α for random networks; while it keeps decreasing with the increase of tolerance parameter α for scale-free networks. Num quickly drops to zero for random networks (i.e., approaches zero for the tolerance parameter $\alpha > \alpha_c$, where $\alpha_c \approx 0.1$), while it slowly decreases for scale-free networks with the increase of tolerance parameter α. The reason for this behaviour results from the fragile property of scale-free networks and the robust feature of random networks to intentional attack.

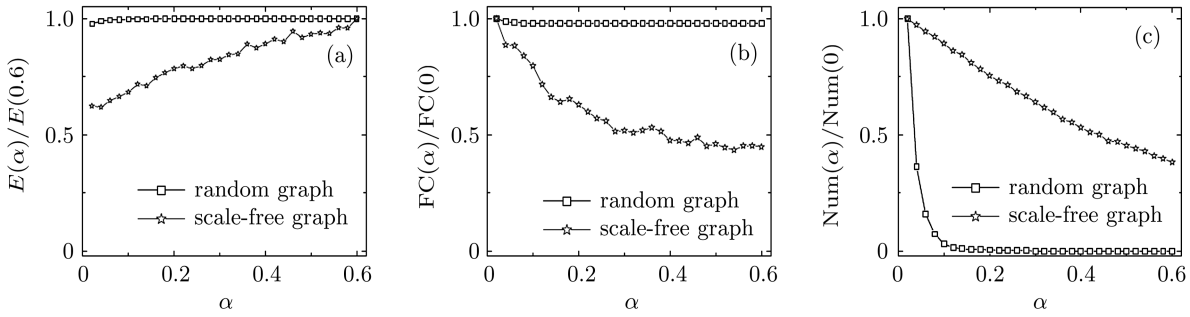


Fig.2. Cascading failures in scale-free and random graphs, as triggered by the initial removal of a single node with the largest degree in the network, for the case without considering a feedback procedure, corresponding to the case of the dotted arrow in Fig.1.

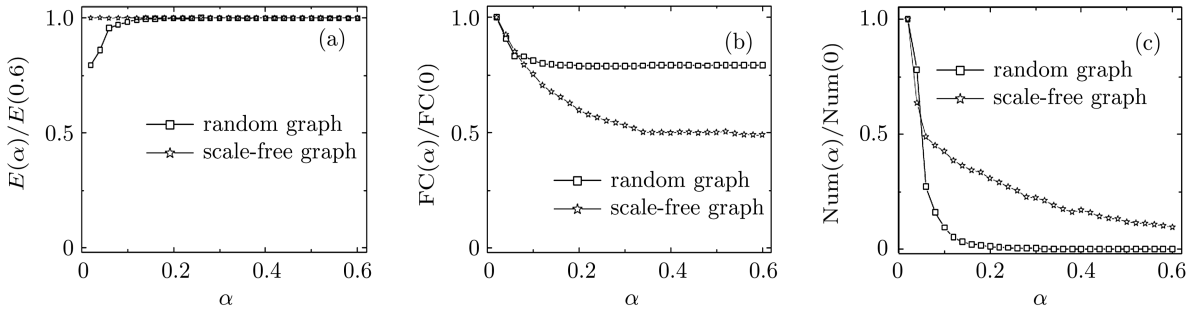


Fig.3. Cascading failures in scale-free and random graphs, as triggered by the initial removal of a single node with the largest degree in the network, for the case considering the effect of the feedback, corresponding to the case of the solid arrow in Fig.1.

In the following, we will consider the effect of a feedback on cascading failures in complex networks. As will be shown below, in this case, the fragile property of scale-free networks to initial intentional attack can be largely improved, which is really different from efficient strategies previously presented to relieve cascading failures in scale-free networks.[18,19]

In Fig.3, we perform the same simulations by considering a feedback procedure, but obtain some different results. As shown in Fig.3(a), for random networks, E basically stays in a steady state, except for the tolerance parameter $\alpha < 0.1$; while for scale-free networks, E remains unchanged, surprisingly independent of tolerance parameter α. Clearly, we can obtain an opposite result for $\alpha < 0.1$ when comparing the simulation in Fig.3(a) with that in Fig.2(a). That is, when $\alpha < 0.1$, scale-free networks become less sensitive to tolerance parameter α as compared with random networks. Similarly, from Fig.3(b), it is clear that, for scale-free networks, FC monotonously decreases for the tolerance parameter α, which is similar to that shown in Fig.2(b), while for random networks, FC also becomes very sensitive to tolerance parameter α when $\alpha < 0.1$, which is different from that shown in Fig.2(b). As shown in Fig.3(c), one can also find that, for random networks, Num approaches zero for the tolerance parameter $\alpha > \alpha_c$, where $\alpha_c \approx 0.2$ larger than 0.1 obtained in Fig.2(c). For scale-free networks, Num surprisingly has a sharp drop when tolerance parameter $\alpha < 0.1$, while it may decrease linearly with tolerance parameter for the case without considering the effect of the feedback, as shown in Fig.2(c). Note that, compared with Fig.2, after introducing the feedback mechanism, it shows that the robustness of random networks is decreased. Actually, when α is close to zero, any attack may lead to congestion which may affect the self-organized trip distribution due to the effect of the feedback. Then the load distribution can also be affected, which may lead to new congestions. As a result, the performance of the network (e.g., FC and Num) may become much more sensitive to the tolerance parameter, except for E. The reason may be due to the fact that, according to Eqs.(10) and (12), E and the behaviour of the self-organized trip distribution are correlated.

As mentioned above, we can infer that, after introducing a feedback procedure, the discrepancy of cascading failures between random and scale-free networks, can be effectively reduced. Actually, when tolerance parameter $\alpha < 0.1$, most edges are congested, as shown in Fig.2(c) and Fig.3(c). Then, the minimum travel time between every origin and destination can be increased, leading to traffic demand dynamics (see Eq.(12)).

4. Summaries and conclusions

Cascading failure, triggered by small initial perturbation, is one of the intriguing problems in physics. In this paper, we aim to study the effect of a feedback procedure on traffic dynamics in complex networks. Interestingly, the feedback procedure can be described by user equilibrium with variable demand. Under the attack, we numerically investigate three quantities to evaluate the performance of complex networks, and obtain some interesting results.

For the case without considering a feedback procedure, the fragile property of scale-free networks and the robust feature of random networks to intentional attacks are recovered. However, for the case considering the effect of the feedback, the discrepancy of instability between random and scale-free networks to intentional attacks is largely reduced. Congestion in scale-free networks can be effectively improved. Moreover, when $\alpha < 0.1$, scale-free networks become less sensitive to tolerance parameter α as compared with random networks. These results should be useful for further studies in the important area of network security.

References

[1] Barabási A L and Albert R 1999 *Science* **286** 509

[2] Albert R and Barabási A L 2002 *Rev. Mod. Phys.* **74** 47

[3] Newman M E J 2003 *SIAM Rev.* **45** 167

[4] Albert R, Jeong H and Barabási A L 2000 *Nature* **406** 378

[5] Cohen R, Erez K, Ben-Avraham D and Havlin S 2000 *Phys. Rev. Lett.* **85** 4626
Callaway D S, Newman M E J, Strogatz S H and Watts D J 2000 *Phys. Rev. Lett.* **85** 5468

[6] Motter A E and Lai Y C 2002 *Phys. Rev.* E **66** 065102(R)

[7] Crucitti P, Latora V and Marchiori M 2004 *Phys. Rev.* E **69** 045104(R)

[8] Holme P and Kim B J 2002 *Phys. Rev.* E **65** 066109
Holme P 2002 *Phys. Rev.* E **66** 036119

[9] Zhao L, Park K, Lai Y C and Ye N 2005 *Phys. Rev.* E **72** 025104(R)

[10] Wu J J, Gao Z Y and Sun H J 2006 *Phys. Rev.* E **74** 066111

[11] Wang B and Kim B J 2007 *Europhys. Lett.* **78** 48001

[12] Zheng J F, Gao Z Y and Zhao X M 2007 *Europhys. Lett.* **79** 58002
Zheng J F, Gao Z Y and Zhao X M 2007 *Phys.* A **385** 700
Zheng J F, Gao Z Y, Zhao X M and Fu B B 2008 *Int. J. Mod. Phys.* C **19** 1727

[13] Di C, Gao Z Y and Zheng J F 2009 *Chin. Phys.* B **18** 992

[14] Brandes U 2001 *J. Mathematical Sociology* **25** 163

[15] Sheffi Y 1985 *Urban Transportation Networks: Equilibrium Analysis with Mathematical Programming Methods* (New Jersey, USA: Prentice-Hall, Englewood Cliffs)

[16] Kim T J 1990 *Advanced Transport and Spatial Systems Models* (New York, USA: Springer-Verlag)

[17] Latora V and Marchiori M 2001 *Phys. Rev. Lett.* **87** 198701

[18] Motter A E 2004 *Phys. Rev. Lett.* **93** 098701

[19] Gallos L K, Cohen R, Argyrakis P, Bunde A and Havlin S 2005 *Phys. Rev. Lett.* **94** 188701