International Journal of Control and Automation
Vol. 9, No. 11 (2016), pp.1-14
http//dx.doi.org/10.14257/ijca.2016.9.11.01

Cascading Failure on Complex Networks Based on Routing Strategy

Feng Zhou[1], Jianeng Tang [*, 2], Kai Wang[3] and Li Zhao[3]

[1]College of information Engineering, Yancheng Institute of Technology, No.9 Xiwang Avenue, Yancheng 224051, China
[2]College of Engineering, Huaqiao University, No.269, Chenghua North Road, Fengze District, Quanzhou, Fujian 362021, PR China
[3]Key Laboratory of Underwater Acoustic Signal Processing of Ministry of Education, Southeast University, No.2 Sipailou, Nanjing 210096, China
[*]Corresponding author's email:tangjianeng@sina.com

Abstract

It has shown that the betweenness distribution of shortest path (SP) routing strategy on scale-free networks is exponential. Some nodes with great degree have higher flow. It is very easy to cause cascading failure when the node's flow exceeds its processing capacity. As a result, the service quality will fall. Utilizing the BA scale-free networks, we study the cascading failure between the minimum information path (MIP) routing strategy and the shortest path (SP) routing strategy. Then the tolerance parameters with upper and lower threshold are obtained by theory. The conclusion displays that the performance of SP routing strategy is slightly better than the MIP routing strategy when the network has little processing capacity. However, the value G of MIP rapidly growths and is close to 1, but the value of SP growths slowly with the process capacity increasing. In a word, the performance of MIP routing strategy is obviously better than the SP routing strategy. Therefore the robustness can be improved greatly by increasing the process capacity of some nodes under MIP routing policy.

***Keywords**: Cascading failure; tolerance parameters; MIP routing strategy; robustness*

1. Introduction

Studies have shown that the performance of network has great relation to the network usage and network load. If the network traffic is too heavy or the network load is too concentrated on certain nodes or areas of the network, causing the network resources are insufficient to deal with the corresponding network load, the performance of network will degrade. Therefore, the quality of network shouldn't be evaluated only when it is stable. Whether it can maintain the original performance under destruction, called the robustness, should also be considered as the evaluation index. Cascading failure is a dynamic network robustness evaluation criterion. Assumed that a node is removed due to a fault, and then the changes in the routing table will redistribute the load of each node in the network. And the redistribution may lead to overloading of other nodes, causing more nodes to be removed. The situation is called cascading failure. It may bring serious consequences such as massive power grid failure, severe obstruction of Internet and even the collapse of the entire network. Therefore the study of cascading failure is critical for transport system. Currently the research work of cascading failure includes 3 aspects. Firstly, the study of various cascading failure models and their performance. For example, Motter first proposed the concept of cascading failure, and the linear load-handling capacity model (ML model), besides he analyzed the impact of network integrity caused by cascading failure and presents two situations that will cause global cascading failure [1]. Crucitti has

ISSN: 2005-4297 IJCA

proposed another model of cascading failure, in which the impact is measured by the reduced efficiency of network [2]. And Lai studied the impact of cascading failure caused by edges of network attraction [3]. While Simonsen studied the situation of cascading failure considering the dynamic nature of stream, and compared it with the static model [4]. Dou proposed a load-handing capability nonlinear model of cascading failure and analyzed it by simulation [5]. And Lehmann studied a new load redistribution mechanism of cascading failure--random probability model [6]. Xia studied the cascading failure in the WS small world model with both homogeneous distribution of degrees and heterogeneous distribution of betweenness [7]. Hackett studied the cascading failure in a kind of complex group of networks, and analyzed the effection of clustering degree to the range of cascading. Secondly, study how to resist and control cascading failure, thereby improving robustness of network [8]. Motter tried to remove some nodes and edges to defend the cascading failure in the scale-free networks [9]. Based on the ML model, Zhao found out the phase shift of key parameters of cascading failure in scale-free network, and if the parameter is less than the phase shift points, cascading failures would result in the collapse of the entire network [10]. Lee proposed that in scale-free network, the avalanche size distribution of cascading failure meet power-law distribution at the critical point, and then analyzed the robustness [11]. Zhao *et al* proposed a method based on the upper boundary of the calculating capability, networks that higher than the upper boundary can be immunized against cascading failure [12]. Wang *et al* studied the cascading failure caused by attacking edges in weighted complex networks, and proposed the relation between weighted parameters and universal robustness[13]. Huang *et al* studied cascading breakdown in complex clustered networks and proposed an effective strategy to prevent it[14]. Yang *et al* proposed that by selecting the appropriate weighting parameter, we can resist cascading failure and improve the robustness of networks to the highest level [15]. Thirdly, is about the cascading failure in two or more interdependent networks. For example, Buldyrev *et al* first proposed the model of interdependent networks. He studied the phenomenon of cascading failure in two networks that depends on each other, and found out a characteristic different from in a single network, that is the fragility when facing random attacks [16]. Huang *et al* studied the cascading failure in interdependent networks under deliberate attacks and compared it to the situation in single network, and came to a conclusion that it's harder for interdependent networks to defend deliberate attacks [17]. Zhao *et al* studied the cascading failure in two coupled network system with multiple dependencies [18].

The root cause of cascading failure is that network resources cannot meet the network load. In the research of complex network, by optimizing network topology, improving the performance of key nodes or edges and designing optimal routing strategy can improve the network transmission capacity and reduce the possibility of cascading failures. Among the three aspects, key nodes and edges are determined by network topology and corresponding routing strategy, and the change of topology cost much, so more research focus on finding portable routing strategy. Currently shortest path (SP) routing strategy is the most widely used global routing strategy, and has become the main routing method in Internet. The local information routing strategy in which we choose routes based on local information probability of neighbor nodes can distribute network load evenly. Based on principles of node degree and minimization, effective routing strategy can ensure that the average path length is in line with small world network features, while the network transmission capacity is 10 times more than SP strategy. Recently we found that, the time a single particle gets through a particular path is proportional to the continued products of all the nodes degree in the path. Accordingly, we proposed routing policy based on minimum information path (MIP) [19]. Different from SP and effective routing strategy, the principle of MIP is minimum continued product of node degree. Studies have shown that in MIP, the load of network is proportional to the degree of nodes. Further, still take continued product of node degree as principle; we can build generalized MIP when node processing capabilities is distributed evenly by adjusting the variable parameters. By analyzing routes' average betweeness centrality, we compared the MIP and generalized one with SP and effective routing strategy. And we found out that both in the situation where process capacity is related to degree or not, the routing efficiency of MIP is much higher than SP and effective routing strategy.

The main routing strategy in Internet is based on shortest path first principle, but SP strategy has some defects. Researches have shown that, in scale-free networks the distribution of nodes betweeness is SP strategy showed strong heterogeneous and some nodes of greater degree bear high traffic load. It's easy to cause cascading failure and seriously affecting the quality of service when the load exceeds the processing capacity. In real networks the cascading failure caused by uneven network traffic can't be solved by simply increasing resources, so innovation is necessary in the design of best routing strategy. In this paper, we concentrate on studying the robustness of networks in SP and MIP routing strategy under the evaluation criteria of cascading failure. In MIP routing strategy the choose of routes is based on minimizing the continued product of nodes in the path, which avoid abuse of nodes with large degrees and reduce the traffic on the core nodes and reduce the possibility of network congestion. Using BA scale-free network model, we analyzed the cascading failure situation of MIP and SP routing strategy theoretically. We get the tolerate parameters and threshold of processing capabilities of both routing strategies and verify the theoretical analysis by simulation experiments. Theoretical analysis and experimental results show that when the node processing capability is small, performance of SP routing strategy is slightly better than the performance of the MIP routing strategy. But with the increasing processing power, the G value of MIP increase rapidly and is close to 1, while the G value of SP grows slowly. Overall, the performance of MIP is obviously better than the performance of SP. In MIP routing strategy, the robustness of network can be increased by adding a small number of processing nodes.

2. Model Introduction

2.1. Cascading Failure

Cascading failure is about the network load reallocation after failure of a certain node. For example, in the Internet network, the load represents transmitted data packets of a node (route) per unit time, and overload means block up. The reallocation of a data package from a blocked router to another router will spread the blocking in the network. For a given network, we can use the concept of betweenness to describe the load distribution in a certain routing strategy. Make the load of a node is all the total number of paths through the node, then the processing capacity of a node is the maximum load the node can handle. Assuming the processing capacity C_i of node i is proportional to its initial load L_i, namely

$$C_i = (1+\alpha)L_i, \quad i = 1, 2, ..., N \tag{1}$$

In the function, α is tolerance parameter and N is the initial number of nodes. When all the nodes are enabled, the network will be in a free-flowing state as long as $\alpha \geq 0$. When a node fails, the change of the path will change the load of remaining nodes. And if the load exceeds the processing capacity of the node after changing, it will fail. Any failure will lead to a new load redistribution, which led to further failures. Effect caused by cascading failure can be measured by the relative size G of the maximum connecting portion.

$$G = \frac{N'}{N} \tag{2}$$

where N and N' is the total number of nodes of the largest part before and after the cascading failure respectively. If $G \approx 1$, then the network is almost unbroken, while if $G \approx 0$, the network is broken.

2.2. Routing Strategy based on MIP [19]

Recently, we found that the time a single particle gets through a particular path is proportional to the connected product of all the nodes on the path in the study of random walk process. This means, when given a particular path $C(l) = c_0 \ldots c_l$ in the network, the average time for a node to find the path is:

$$< T > = \Re'(1) = 2m\prod_{i=1}^{l-1} k_i + \Phi \tag{3}$$

In which, k_i is the degree of node i, m is the number of edges of the network, and parameter Φ is only related to the network topology structure.

Based on this, we proposed the minimum information path (MIP) routing strategy: assuming $i \equiv v_0, v_1, \ldots, v_{n-2}, v_{n-1} \equiv j$ is a random path from node i to node j, the optimized path P_{mip} can be calculated by the following formula:

$$p_{\min}(l : i \to j) = \min \prod\nolimits_{m=i}^{j} k_m \tag{4}$$

with $\ln(k_m)$ instead of k_m, formula (4) can be transformed into:

$$p(i \to j) = \min \sum_{n=0}^{l} \ln(k_n) \tag{5}$$

Figure 1 shows the corresponding relationship between average nodes betweenness and node degree in SP and MIP routing strategy. BA scale-free network is selected, in which number of nodes is 1000, degree distribution $\gamma \approx 3$ and $< k > = 4$. X-axis represents node degrees and Y-axis represents node betweeness, SP is short for shortest path routing strategy and MIP is short for minimum information path routing strategy. As is shown in Figure 1, average node betweeness have an exponential relationship with node degree in SP routing strategy, while in MIP strategy, the relationship is proportional. And the largest betweeness of MIP routing strategy is much less than that of SP routing strategy.

From the simulation we can see, when the node processing capacity is proportional to its node degree, the transmission capacity is efficiently improved by MIP routing strategy. Compared to SP routing strategy, finding the shortest path is not the only goal of MIP routing strategy, the node degree of network also has been taken into consideration. So it avoids the degree nodes, reducing the flow of core nodes and the possibility of congestion, and improving the network transmission capacity. MIP routing strategy chooses routers based on minimizing the continued product of node degree and avoid the excessive use of node with large degree, while limit the length of paths at the same time. In which way, nodes of different degree are used more reasonable and the transmission capacity is well improved.

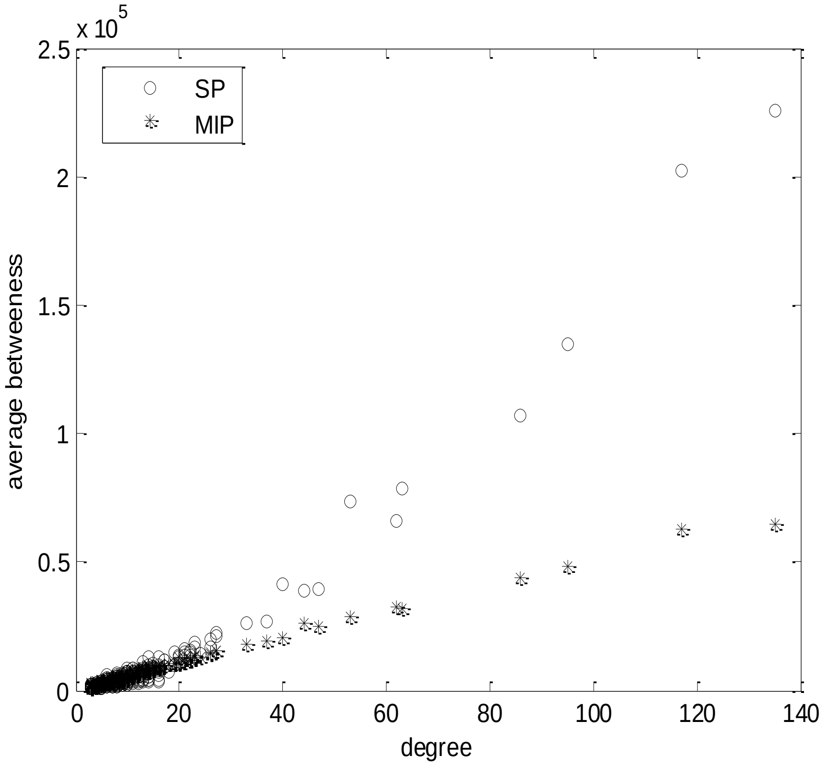


Figure 1. (Color Online) The Relationship between Average Node Betweeness and Node Degree

3. Tolerance Parameters

The main title (on the first page) should begin 1 3/16 inches (7 picas) from the top edge of the page, centered, and in Times New Roman 14-point, boldface type. Capitalize the first letter of nouns, pronouns, verbs, adjectives, and adverbs; do not capitalize articles, coordinate conjunctions, or prepositions (unless the title begins with such a word). Please initially capitalize only the first word in other titles, including section titles and first, second, and third-order headings (for example, "Titles and headings" — as in these guidelines). Leave two blank lines after the title.

Make network node degree distribution is $P(k) = ak^{-\gamma}$, load distribution is $L(k) = bk^{\eta}$, where a and b are positive constants [1]. We can know:

$$\int_1^{k_{\max}} P(k)dk = N \tag{6a}$$

$$\int_1^{k_{\max}} P(k)L(k)dk = S \tag{6b}$$

where S is the total network load, $k_{\max}$ is the maximum degree of the network. By the formula (6) we can obtain:

$$a = \frac{(1-\gamma)N}{[k_{\max}^{1-\gamma} - 1]} \tag{7a}$$

$$b = \frac{\beta S}{a(1 - k_{\max}^{-\beta})} \tag{7b}$$

where $\beta \equiv \gamma - \eta - 1 > 0$. Assume that a node of $\hat{k}$ degree is attacked in the network, then the network load will redistribute for the first time, and the distribution of degree and betweenness become $P'(k) = a'k^{-\gamma'}$ and $L'(k) = b'k^{\eta'}$. Because only one node is removed from the network, the changes of distribution scaling index can be ignored. We can get $P'(k) = a'k^{-\gamma}$ and $L'(k) = b'k^{\eta}$, a' and b' are counted the same way as a and b . Thereby obtaining

$$a' = (1-\gamma)(N-1)/[k_{\max'}^{1-\gamma} - 1] \quad (8a)$$

$$b' = \beta S'/a'[1-k_{\max'}^{-\beta}] \quad (8b)$$

where S' is the total load of the network after the attack, and $k_{\max'}$ is the largest degree of the network after removing the attracted node.

We calculate the lower threshold α_d and upper threshold α_u of tolerance parameter α to measure the effect on routing performance caused by distribution. When $\alpha \le \alpha_d$, after the attack and redistribution, the rest nodes are almost overloaded, and G is close to 0; when $\alpha \ge \alpha_u$, after the attack and redistribution, the rest nodes are almost not overloaded, and G is close to 1.

3.1. Lower Threshold of Tolerance Parameter

In the section, based on the nonlinear control theory, an effective method for designing synchronization methods in the fractional order Chen chaotic systems with time delays has proposed to realize synchronization.

For the nodes with degree of k , the change of betweenness before and after the attack can be expressed as $\Delta L(k) \approx (b'-b)k^{\eta} = [(b'/b)-1]L(k)$. Given processing capacity $C(k)$, the maximum load increment a node can handle is $C(k) - L(k) = \alpha L(k)$. So when $\alpha > [(b'/b)-1]$, nodes work properly, and when $\alpha < [(b'/b)-1]$, failure accrues. Whereby the low-threshold of tolerance parameter can be expressed as

$$\begin{aligned}\alpha_d &= \frac{b'}{b} - 1 \approx \left(\frac{k_{\max'}{}^{1-\gamma}-1}{k_{\max}{}^{1-\gamma}-1}\right)\left(\frac{1-k_{\max}{}^{-\beta}}{1-k_{\max'}{}^{-\beta}}\right)\left(\frac{S'}{S}\right) - 1 \approx \left(\frac{1-k_{\max}{}^{-\beta}}{1-k_{\max'}{}^{-\beta}}\right)\left(\frac{S'}{S}\right) - 1 \\ &\approx \left\{1-(k_{\max}{}^{-\beta} - k_{\max'}{}^{-\beta})\right\}\left(\frac{S'}{S}\right) - 1 = \left\{1 - k_{\max'}{}^{-\beta}\left[-1+\left(\frac{k_{\max}}{k_{\max'}}\right)^{-\beta}\right]\right\}\left(\frac{S'}{S}\right) - 1\end{aligned} \quad (9)$$

when $N \to \infty$ and $\gamma > 1$, $k_{\max'}{}^{1-\gamma}$ and $k_{\max}{}^{1-\gamma}$ are close to 0, so $(k_{\max'}{}^{1-\gamma}-1)/(k_{\max}{}^{1-\gamma}-1) \approx 1$. And when $N \to \infty$, $k_{\max'}^{-\beta} \to 0$, $k_{\max}/k_{\max'} \to$ constant and $S'/S \to 1$, so we can get that $\alpha_d \approx 0$,which means as long as $\alpha > 0$, infinitely large scale-free network will not collapse because of one time attack. On the other hand, for a finite network, $k_{\max'}^{-\beta} > 0$ and $\alpha_d > 0$, which means when $\alpha < \alpha_d$, the network will collapse.

We can see from formula (9) that, when the network is constant, $k_{\max}$ and $k_{\max'}$ will be constant, and because $S'/S \to 1$, the lower threshold of tolerance parameter is determined by parameter β . Suppose there is a BA free-scale network with 2000 nodes, in which $\gamma \approx 3$, $<k>=4$, $k_{\max} = 127$, $k_{\max'} = 118$, .Consider the lower threshold of tolerance parameter in SP routing strategy and MIP strategy separately. In SP routing strategy, we can statistically know that the load of network $S \approx 1.45\times10^7$ and $S' \approx 1.473\times10^7$ after change, $\beta = \gamma - \eta - 1 = 3 - 1.6 - 1 = 0.4$, and according to formula (9) we can obtain $\alpha_d \approx 0.02$. While in the MIP routing strategy, the load of network $S \approx 1.62\times10^7$ and $S' \approx 1.65\times10^7$ after change, $\beta = \gamma - \eta - 1 = 3 - 1 - 1 = 1$, and $\alpha_d \approx 0.01$.

3.2. Upper Threshold of Tolerance Parameter

The chaos synchronization consists in the tracking of the master system trajectories by the slave system. However, this problem can be restated as the stabilization of the orbits of a dynamical system which represents the discrepancy between two systems. In order to observe the synchronization behavior in two identical fractional-order Chen systems with time delays, we build a drive-response configuration with a drive system given by the fractional-order Chen system with time delays (with three state variables denoted by the subscript m) and with a response system (with three variables denoted by subscript s). The drive and response systems are described by the following differential equations, respectively:

Further, we consider the upper threshold α_u. To make the G value close to 1 after deliberate attract means to make sure that all the nodes won't be overloaded after redistribution. Which also means that, for a random node i, the load of network before and after the redistribution L_i', L_i and the processing capacity C_i should meet the equation $L_i' \le C_i = (1+\alpha)L_i$. Since all nodes are required to meet the equation above, we can see:

$$\begin{aligned} & L'(k) \le C(k) = (1+\alpha)L(k) \Rightarrow \alpha \ge \frac{L'(k)-L(k)}{L(k)} \\ & \quad \Rightarrow \alpha_u = \max\left\{\frac{L'(k)-L(k)}{L(k)}\right\} \end{aligned} \tag{10}$$

For a node with k degree, the change of betweenness after the attack can be expressed as $\Delta L(k) \approx (b'-b)k^{\eta} = [(b'/b)-1]L(k)$. Thus the lower threshold of tolerance parameter α_d can be expressed as:

$$\begin{aligned} \alpha_u &= \max\left\{\frac{L'(k)-L(k)}{L(k)}\right\} = \max\left\{\frac{b'}{b}\right\} - 1 \approx \max\left\{\left[1-(k_{\max}{}^{-\beta} - k_{\max'}{}^{-\beta})\right]\left(\frac{S'}{S}\right)\right\} - 1 \\ &= \max\left\{\left\{1 - k_{\max'}{}^{-\beta}\left[-1+\left(\frac{k_{\max}}{k_{\max'}}\right)^{-\beta}\right]\right\}\left(\frac{S'}{S}\right)\right\} - 1 \end{aligned} \tag{11}$$

Based on formula (11) we can know that, when the network is constant, $k_{\max}$ and $k_{\max'}$ will be constant, and because $S'/S \to 1$, the upper threshold of tolerance parameter is related to parameter β too. In the same BA free-scale network with 2000 nodes, in which $\gamma \approx 3$, $<k>=4$, $k_{\max} = 127$, $k_{\max'} = 118$. What should be noted is that, the formula (11) shows the relationship between the upper threshold of tolerance parameter and the parameters of the network statistically. But in particular route, because of the randomness of the source and destination nodes, the node with maximum load variation after redistribution is not fixed. By repeatedly compare the initial load distribution table (between's table) after redistribution, the maximum average value of load change rate can be calculated: in SP routing strategy $\alpha_u \approx 1.3$, and in MIP routing strategy $\alpha_u \approx 0.3$.

3.3. The Conversation between Tolerance Threshold and Processing Capacity

Calculating the tolerance parameter threshold is to distribute initial processing capacity better, so as to avoid the damages cascading failure caused. From formula (1) we can know that, the processing capacity is not only related to control parameter but also related to network load. The load of nodes are different under different routing circumstances, so it is necessary to convert the thresholds of tolerance parameters to corresponding node processing capacity, then we can evaluate the performance of different routing strategies under the same criteria. As described above, in the SP routing strategy, $S_{sp} \approx 1.45 \times 10^7$, can get $\alpha_{d,sp} \approx 0.02$, and from formula (1) we can know $C_{d,sp} = (1+\alpha_{d,sp})S_{sp} \approx 14.79$ million. While in MIP routing strategy, $S_{mip} \approx 1.62 \times 10^7$, $\alpha_{d,mip} \approx 0.01$, and from formula (1) we can know $C_{d,mip} = (1+\alpha_{d,mip})S_{mip} \approx 16.40$ million. Thus, to ensure the whole network not collapse, the processing capacity SP is smaller than processing capacity MIP. The reason is that in SP routing strategy, the total network is less than in MIP strategy.

On the other hand, by calculating we can get the up-threshold of tolerance parameter $\alpha_{u,sp} \approx 1.3$ of SP routing strategy and $\alpha_{u,mip} \approx 0.3$ of MIP routing strategy. Based on formula (1) we can get $C_{u,SP} = (1+\alpha_u)S \approx 33.35$ million, $C_{u,mip} = (1+\alpha_u)S \approx 21$ million. Thus, to maintain the network integrity after attack, the processing capacity we need in MIP routing strategy is much less than SP routing strategy. The reason is that, the network load in MIP routing strategy is more evenly distributed, so there won't be too many nodes crashing after redistribution. While the SP routing strategy, the load distribution is proportional to node degree, so the change of network load after redistribution can be really huge, causing further collapse. Thus, with increase of initial processing capacity, *G* value in MIP routing strategy gets close to 1 faster.

In addition, we can analyze from another point of view: removing a node in the network can be regarded as the loss of processing capacity. Assume to remove the node with biggest degree, since C_i is proportional to L_i, L_i and in SP routing strategy, L_i is proportional to $k_i^{1.6}$, the proportion of processing capacity lost is

$$\delta = \frac{C_i}{\sum_j C_j} = \frac{L_i}{\sum_j L_j} = \frac{k_i^{1.6}}{\sum_j k_j^{1.6}} \tag{12a}$$

$$\delta' = \frac{C_i}{\sum_j C_j} = \frac{L_i}{\sum_j L_j} = \frac{k_i}{\sum_j k_j} \tag{12b}$$

Before removing the node with biggest degree, we can get $\delta \approx 0.04$, and in MIP routing strategy, L_i is proportional to k_i, after removing $\delta' \approx 0.01$. This means, the loss of processing capacity after removing node of biggest degree in MIP routing strategy is much less than in SP routing strategy. Thus, with the initial processing capacity increasing, *G* value in MIP routing strategy gets close to 1 faster.

The analysis above shows that: the low-threshold of tolerance parameter α, $[\alpha_d]_{MIP} < [\alpha_d]_{SP}$, and the upper threshold $[\alpha_u]_{MIP} < [\alpha_u]_{SP}$. From the view of processing capacity, when the initial processing capacity is small, the SP routing strategy can provide better insurance to keep the network working well. However, with increasing processing capacity, the MIP routing strategy can avoid cascading failure faster and thus enhance the network robustness. Overall, the MIP routing strategy can better withstand the cascading failure.

4. System Simulation

Select a BA free-scale network with 2000 nodes, in which $\gamma \approx 3$, $<k>=4$. According to the simulation statistics based on SP and MIP routing process, we can know the initial network load is 14.5 million and 16.2 million. The initial total load of SP routing strategy is smaller. Further, increase the initial load gradually, simulate the process of cascading failure in SP strategy and MIP strategy respectively and calculate the *G* value under the same processing capacity. The data in the figures are average results of 30 times repeat simulations.

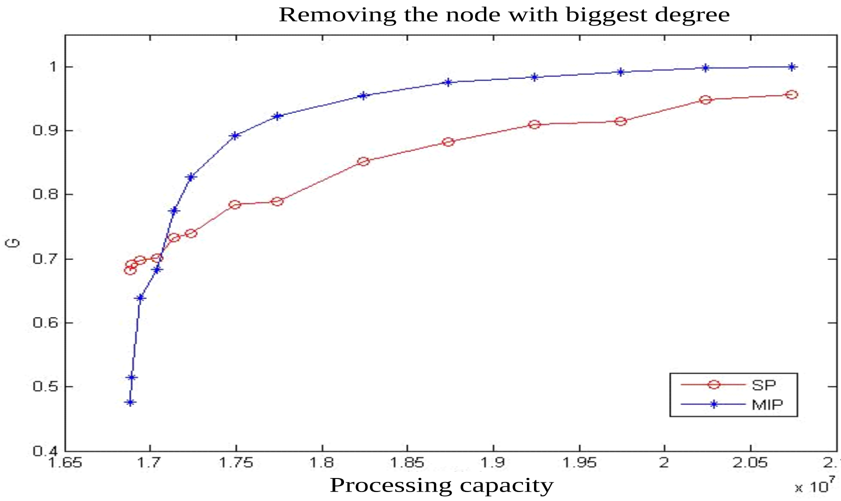


Figure 2. (Color Online) Cascading Failure in BA Free-Scale Network, $\gamma = 3, < k >= 4, N = 2000$, the Node Been Attacked has Biggest Degree. *X*-axis Represents Processing Capacity and *Y*-Axis Represent *G* Value. Start is the Result of MIP Strategy and Circle is the Result of SP Strategy

In Figure 2, we compare the relationship between value *G* and the processing capacity in SP routing strategy and MIP routing strategy respectively after removing the node with biggest degree and cascading failure happening. As is shown in the figure, when the processing capacity is small, *G* of SP routing strategy is smaller than *G* of MIP strategy, but with the processing capacity increasing, *G* of MIP routing strategy grows quickly and exceeds *G* of SP routing strategy. After that, *G* value of MIP routing strategy keeps leading. For example, when processing capacity is 18 million, the *G* value in SP routing strategy is about 0.8, while *G* value under MIP routing strategy has reached 0.95. When the *G* value of MIP routing strategy is close to 1, which means the network is substantially unaffected, there are still 5% nodes in faults under SP routing policy. Accordingly, in the network with 2000 nodes we used in simulation, it means about 100 nodes are disconnected. Therefore, if the processing capacity allocated is sufficient, MIP routing strategy can resist cascading failure more efficiently.

Figure 3 shows the *G* value under both routing strategy when the processing capacity is small. The parameters in Figure 3 are same as in Figure 2 We can see that, the lower threshold of processing capacity under SP routing strategy is 14.8 million, namely, when processing capacity is bigger than 14.8 million, the network won't collapse entirely after deliberate attack., while the lower threshold of processing capacity under MIP routing strategy is about 16.3 million. It can be seen that, the initial total network load is smaller under SP routing strategy, therefore, when the processing capacity can be allocated is small, the SP routing policy better.

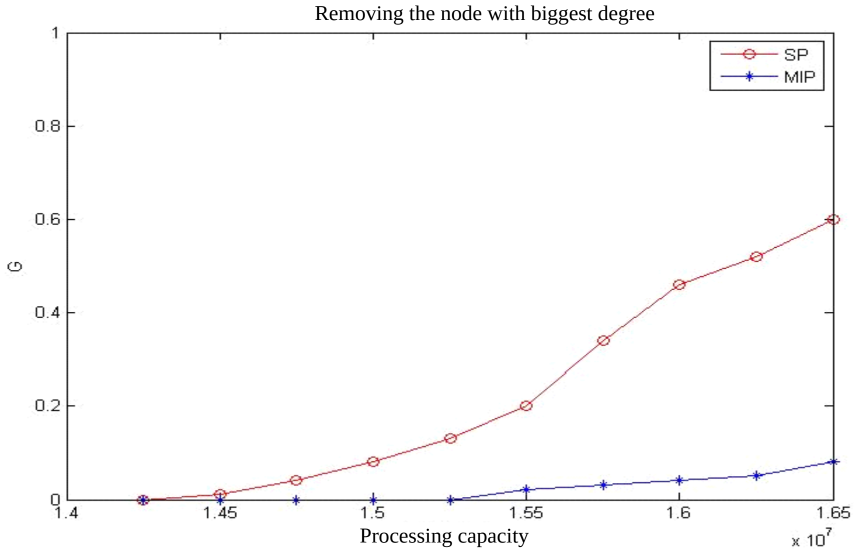


Figure 3. (Color Online) Cascading Failure in BA Free-Scale Network, the Lower Threshold of Processing Capacity in both SP and MIP Routing Strategy

Figure 4 shows the G value under both routing strategy when the processing capacity is big. The parameters in Figure 4 are same as in Figure 2. The upper threshold of processing capacity under SP routing strategy is 33.4million, namely, when processing capacity is bigger than 33.4 million, the network won't collapse entirely after deliberate attack, while the upper threshold of processing capacity under MIP routing strategy is about 21 million, which is much smaller than in SP routing strategy. Therefore, with the processing capacity increasing, MIP routing strategy can resist cascading failure faster.

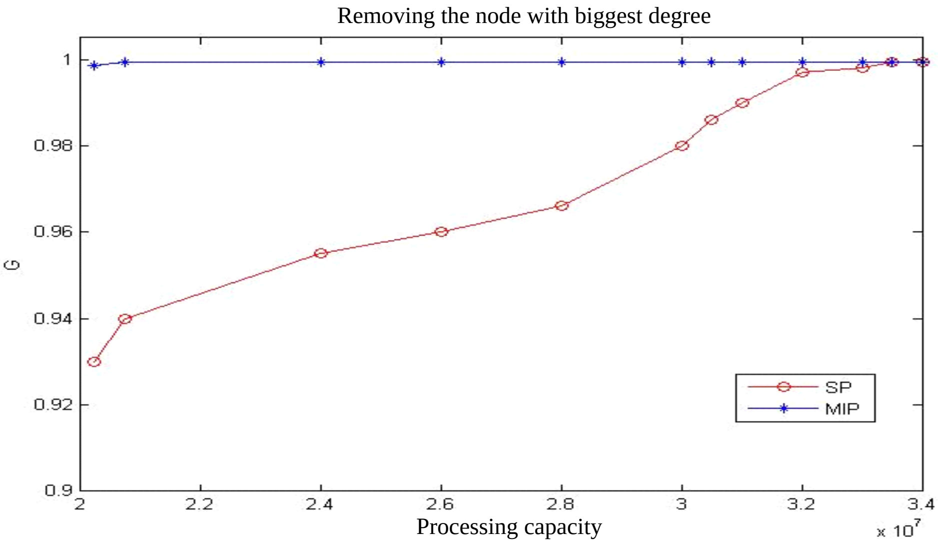


Figure 4. (Color Online) Cascading Failure in BA Free-Scale Network. The Up-Threshold of Processing Capacity of both SP and MIP Routing Strategy

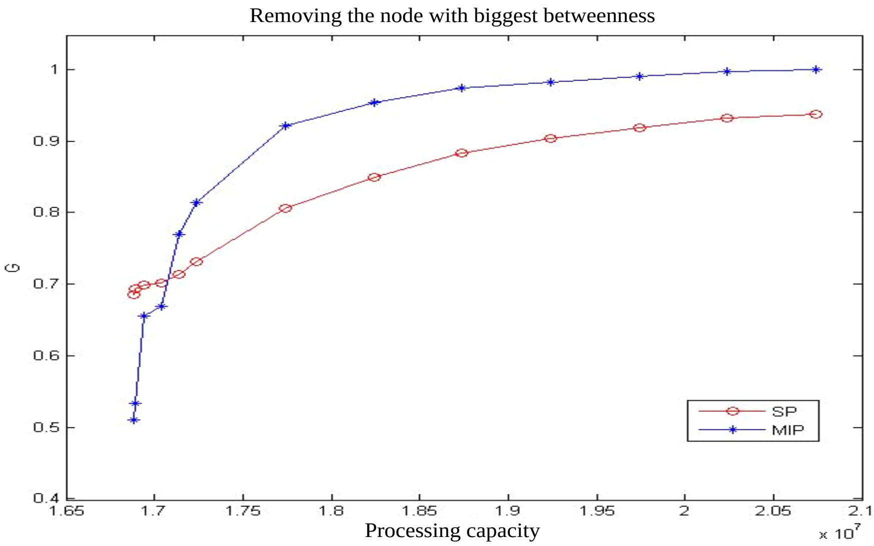


Figure 5. (Color Online) Cascading Failure in BA Free-Scale Network, the Node Been Attacked Has Biggest Betweenness

Figure 5 shows that in a BA free-scale network, the situation of cascading failure when the node with biggest betweenness is attacked under both SP and MIP routing strategy. The parameters in Figure 5 are the same as in Figure 2. Betweenness of a node means the number of the shortest paths through the nodes, which is an important network property. As can be seen from the figure, the relationship between G value and processing capacity under both routing strategies is almost same as the situation when the node with biggest degree is attacked. For example, when the processing capacity is 17 million, after attacking the node with biggest betweenness, the G value of MIP routing strategy is about 0.66, and the G value of SP routing strategy is about 0.7. And when after attacking the node with the biggest degree, the G value of MIP routing strategy is about 0.64, and the G value of SP routing strategy is about 0.7. The results are almost same. When the processing capacity is small, the G value under SP routing strategy is bigger than under MIP routing strategy, however, with processing capacity increasing, G value under MIP routing strategy grows quickly to 1, while the G value under SP routing strategy grows slowly.

5. Conclusions

Since MIP routing strategy is based on minimum continued product of node degree, it can improve the network's load capacity to the uttermost. In this paper, we studied the robustness of MIP and SP routing strategy, taking cascading failure as the evaluation criteria. We build a BA free-scale network model, not only theoretically analyzed the cascading failure situation of MIP and SP routing strategy rigorously, getting the tolerance parameter and the threshold of processing capacity, but also verify the analysis by simulation experiments. Two methods of attack are used in this paper, which are attacking the node with biggest degree and attacking the node with biggest betweenness, the results are basically the same. Then we come to the conclusion that the performance of SP routing strategy is slightly better than the MIP routing strategy when the network has little processing capacity. However, the value G of MIP rapid growths and is close to 1, but the value of SP growths slowly with the process capacity increasing. In a word, the performance of MIP routing strategy is obviously better than the SP routing strategy. The conclusion can be used to improve the robustness of network, and has a certain value in network security field.

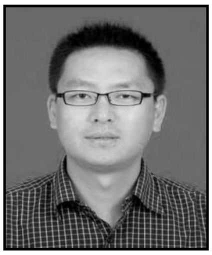
Acknowledgments

This work was supported by the Natural Science Foundation of China under Grant No. 61201173, by China Postdoctoral Science Foundation under Grant No. 2015M571637, by the Fundamental Research Funds for the Central Universities (No.v2242013K30010), by the Foundation of the Fujian Education Department under Grant No. JA15035, by Forward looking research projects in Jiangsu Province under Grant No. BY2015057-39, by the Foundation of Quanzhou Grant No. 2014Z103 and No. 2015Z114.

References

[1] A. E. Motter and Y. C. Lai, "Cascade-based Attacks on Complex Networks", Physical Review E, vol. 66, no. 6, **(2002)**, pp.065102.
[2] P. Crucitti, V. Latora and M. Massimo, "Model for Cascading Failures in Complex Networks", Physical Review E, vol. 69, no. 4, **(2004)**, pp. 045104(R).
[3] Y. C. Lai, A. E. Motter and T. Nishikawa, "Attacks and Cascades in Complex Networks", Lecture Notes in Physics, vol. 650, **(2004)**, pp.299-310.
[4] I. Simonsen, L. Buzna, K. Peters, S. Bornholdt and D. Helbing, "Transient Dynamics Increasing Network Vulnerability to Cascading Failures", Physical Review Letters, vol. 100, no. 21, **(2008)**, pp.218701.
[5] B. L. Dou, X. G. Wang and S. Y. Zhang, "Robustness of Networks Against Cascading Failures", vol. 389, no. 11, **(2010)**, pp. 2310–2317.
[6] J. Lehmann and J. Bernasconi, "Stochastic Load-Redistribution Model for Cascading Failure Propagation", Physical Review E, vol. 81, no. 3, **(2010)**, pp. 031129.
[7] Y. X. Xia, J. Fan and D. Hill, "Cascading Failure in Watts-Strogatz Small-world Networks", Physica A: Statistical Mechanics and its Applications, vol. 389, no. 6, **(2010)**, pp. 1281-1285.
[8] A. Hackett, S. Melnik and P. G. James, "Cascades on a Class of Clustered Random Networks", Physical Review E, vol. 83, no.5, **(2011)**, pp. 056107.
[9] A. E. Motter, "Cascade Control and Defense in Complex Networks", Phys. Rev. Lett., vol. 93, no. 9, **(2004)**, pp.098701.
[10] L. Zhao, K. Park and Y. C. Lai, "Attack Vulnerability of Scale-free Networks Due to Cascading Breakdow", Physical Review E, vol. 70, no. 3, **(2004)**, pp.035101(R).
[11] E. J. Lee, K. I. Goh, B. Kahng and D. Kim, "Robustness of the Avalanche Dynamics in Data Packet Transport on Scale-free Networks", Physical Review E, vol. 71, no. 5, **(2005)**, pp. 056108.
[12] L. Zhao, K. Park, Y. C. Lai and N. Ye, "Tolerance of Scale-free Networks Against Attack-induced Cascades", Physical Review E, vol. 72, no.2, **(2005)**, pp. 025104(1–4).
[13] W. X. Wang and G. R. Chen, "Universal Robustness Characteristic of Weighted Networks Against Cascading Failure", Physical Review E, vol. 77, no.2, **(2008)**, pp. 026101.
[14] L. Huang, Y. C. Lai and G. R. Chen, "Understanding and Preventing Cascading Breakdown in Complex Clustered Networks", Physical Review E, vol. 78, no.3, **(2008)**, pp.036116.
[15] R. Yang, W. X. Wang, Y. C. Lai and G. R. Chen, "Optimal weighting scheme for suppressing cascades and traffic congestion in complex networks", vol. 79, no.2, **(2009)**, pp.026112.
[16] S. Havlin, N. A. M. Araújo, S. V. Buldyrev, C. S. Dias, R. Parshani, G. Paul and H. E. Stanley, "Catastrophic Cascade of Failures in Interdependent Networks", Proceedings of the International School of Physics "Enrico Fermi", vol. 176, **(2012)**, pp. 311-324.
[17] X. Huang, J. Gao, S. V. Buldyrev, S. Havlin and H. E. Stanley, "Robustness of Interdependent Networks Under Targeted Attack" Physical Review E, vol. 83, no.6, **(2011)**, pp.065101(R).
[18] J. Shao, S. V. Buldyrev, S. Havlin and H. E. Stanley, "Cascade of Failures in Coupled Network Systems with Multiple Support-Dependence Relations", Physical Review E, vol. 83, no.3, **(2011)**, pp.036116.
[19] K. Wang, Y. F. Zhang, S.Y. Zhou, W. J. Pei, S. P. Wang and T. Li, "Optimal routing strategy based on the minimum information path", Physica A, vol. 390, **(2011)**, pp. 2593-2600.

Authors



Feng Zhou, he received the B.S. and M.S. degrees from Southeast University, Nanjing, China, in 2004 and 2012, respectively.Currently, he is a lecturer inSchool of Information Engineering, Yancheng Institute of Technology,Yancheng, China. Her research topics include complex networks, signal and information processing, image and voice signal processing.

Jianeng Tang, he was born in 1983. He received the Ph. D. degree in Information and Communication Engineering from Southeast University in 2012. Currently, he is with College of Engineering, Huaqiao University, Quanzhou, Fujian, China. His main research interests include nonlinear systems, chaos synchronization and control, complex networks, acoustic emission technology and speech signal processing.

Kai Wang, he received his Ph.D. degree in Signal Processing from the School of Information and En-gineering, Southeast University, Nanjing, China, in 2009, where he is an Associate Professor in Signal Processing.His research interests include signal processing,chaotic cryptosystems and complex network.

Li Zhao, he received the B.E. degree from Nanjing University of Aeronautics and Astronautics (China) in 1982, the M.S. degree from Suzhou University (China) in 1988, and the Ph.D. degree from Kyoto Institute of Technology (Japan) in 1998. He is currently a Professor in Southeast University, Nanjing, Jiangsu, China. His major interests include pattern recognition, speech signal processing and nonlinear systems.