Physica A 458 (2016) 194–203

Contents lists available at ScienceDirect

Physica A

journal homepage: www.elsevier.com/locate/physa

Fuzzy-information-based robustness of interconnected networks against attacks and failures

Qian Zhu[a,b,*], Zhiliang Zhu[a], Yifan Wang[a], Hai Yu[a]

[a] *Software College, Northeastern University, Shenyang 110819, China*

[b] *School of Information Science & Engineering, Northeastern University, Shenyang 110819, China*

HIGHLIGHTS

- We establish a cascading failure model for interconnected networks.
- The associated data-packet transport problem of the network is discussed.
- We use fuzzy information in resisting uncertain failures and malicious attacks.
- The coupling probability reaches a critical value for disassortative coupling.
- A critical phenomenon that information accuracy affects the network robustness is observed.

ARTICLE INFO

Article history:
Received 2 December 2015
Received in revised form 5 April 2016
Available online 19 April 2016

Keywords:
Robustness
Cascading failure
Attack
Interconnected network
Fuzzy information

ABSTRACT

Cascading failure is fatal in applications and its investigation is essential and therefore became a focal topic in the field of complex networks in the last decade. In this paper, a cascading failure model is established for interconnected networks and the associated data-packet transport problem is discussed. A distinguished feature of the new model is its utilization of fuzzy information in resisting uncertain failures and malicious attacks. We numerically find that the giant component of the network after failures increases with tolerance parameter for any coupling preference and attacking ambiguity. Moreover, considering the effect of the coupling probability on the robustness of the networks, we find that the robustness of the assortative coupling and random coupling of the network model increases with the coupling probability. However, for disassortative coupling, there exists a critical phenomenon for coupling probability. In addition, a critical value that attacking information accuracy affects the network robustness is observed. Finally, as a practical example, the interconnected AS-level Internet in South Korea and Japan is analyzed. The actual data validates the theoretical model and analytic results. This paper thus provides some guidelines for preventing cascading failures in the design of architecture and optimization of real-world interconnected networks.

[*] Corresponding author at: Software College, Northeastern University, Shenyang 110819, China.
E-mail address: zhuq@mail.neu.edu.cn (Q. Zhu).

http://dx.doi.org/10.1016/j.physa.2016.04.007
0378-4371/© 2016 Elsevier B.V. All rights reserved.

1. Introduction

In the modern society, as the high-technology continues to develop, more and more critical network infrastructures will be revolutionized. For example, the Internet, power grids, wireless communication networks, airline networks, and so on, are all continuously evolving and revolutionizing. A lot of research efforts have been devoted to evaluating network robustness, indeed quite intensively in the past decade [1–20]. Researchers have focused on cascading failures models [1–5], cascade control and defense strategies [6–14], different attack strategies [15–20], and so on. However, these approaches focus on single networks, neglecting interdependence among different coupled networks. Modern infrastructures are actually coupled together and significantly interact with each other. The interdependencies of information systems are drastically increased. Recently, some coupled network models have drawn increasing attention from scientific communities [21–31]. A typical example in point is that communication networks control and manage power stations, while the power grids provide electricity supply for the operation of communication networks [21]. As a matter of fact, such interdependencies severely impact the vulnerability of both of these two different types of networks. In a communication network, data-packets are transported among the nodes. If some nodes failed or are being attacked, the traffic loads of these nodes will be redistributed to other nodes in the network. These failing nodes can cause the interdependent nodes in other network to fail. As this process continues, the impact will spread out to the whole systems and eventually lead to a large-scale disaster. This initiative work stimulates some deeper studies to focus on coupling patterns [22,23], coupling strengths [21,24], and network structures [25–29] with respect to the robustness of such networks. In coupled networks, individual networks are connected together depending on certain interdependent relationships. The failures of some nodes in one network will cause failures in other coupled networks thereby causing the entire network to collapse as a consequence.

In addition to interdependent networks, many independent networks which are originally disconnected have the needs to connect with each other for some specific purposes or requirements [30–36], forming a new interconnected network. Differing from the interdependent links between each network, the interconnected links across two networks play the same role as the connectivity within each network. For example, different power networks need new transmission lines to transmit electricity between any pair of them. Zhao et al. [30] explored an interconnected network model considering cascading failures based on the dynamic redistribution of flow in the networks, they found enhancing the heterogeneity will make networks more susceptible. The coupling preference makes no differences for the effects of various coupling preferences. However, most studies on the interconnected networks assume that networks are same in size. Zhang et al. [31] studied the different network size and the number of interconnected links affects the robustness of coupled networks. They found that when two networks with similar sizes are coupled, the interconnected networks are the most fragile for sparse coupling while they are the most robust for dense coupling. Liu et al. [32] explored the spread of epidemics in interconnected small-world networks with spatial constraints. In modern society, the traffic of the network systems is an important issue. Tan et al. [33] analyzed the traffic congestion of interconnected networks, and found that assortative coupling can alleviate traffic congestion better than other two coupling preferences. The literatures above view the intra-links and inter-links as the same when defining the loads, which is not in accordance with the reality. Peng et al. [34] investigated the proportion of contribution of the intra-links and inter-links to the network's loads, and found that if inter-links contribute more to the loads, the interconnected networks will be more robust. Tan et al. [35] have studied cascading failures in interconnected scale-free networks under intentional attack. They found that enhancing the coupling probability can mitigate cascading failures for sparse coupling, but intensify the cascades for dense coupling.

Noticeably, previous research works were carried out mainly against pure random attacks or pure intentional attacks onto the networks. These are two particular situations in real-life scenarios. When an attacker has accurate information of the whole network structure, he will be more inclined to attack key nodes in the network (e.g., the nodes with highest degrees). Otherwise, the attacker may simply attack the network randomly, which corresponds also to random failures in general. In real-world applications, one may only know partial information of the network in question. Therefore, the available information is imprecise and incomplete, referred to as fuzzy information below. In recent studies, some attack strategies have been based on such fuzzy information [19,20]. Wu et al. [20] studied the robustness of a single scale-free network under fuzzy-information-based attacks and found interestingly that the robustness of a scale-free network can be intensified by decreasing the precision of the attack information. The cascading-failure model therein was built from the perspective of network static properties, which does not take traffic overloads into consideration. Brummitt et al. [36] studied a sandpile model for interconnected networks, where traffic loads are redistributed from an overloaded node to its neighbors. However, it only considers the local dynamic process. Different from the models used in Refs. [20,36], this paper considers cascading failures in a double-layer network due to traffic overloading, taking into account the global dynamic characteristics of the interconnected network.

Inspired by the investigations of fuzzy-information-based attacks considered in single networks [19,20], and by the newly-proposed concept of interconnected networks [30–36] in the field of complex networks, this paper studies the robustness of interconnected networks, using the familiar Barabasi–Albert (BA) network [37] as a platform, for fuzzy-information-based attacks in terms of cascading failures due to traffic overloading. For this purpose, the traffic flow transport model [1] will be adopted. If one node fails, it may likely change the traffic flow paths between itself and other remote nodes thereby causing global failures. In this paper, the critical threshold of removing nodes is found, over which the networks will breakdown. Moreover, the robustness of a network with different coupled preferences and different coupling probabilities is examined in detail. Finally, an application to the interconnected AS-level Internet of South Korea and Japan is demonstrated.

2. The model

2.1. Network structure

In this model, as mentioned above, only the case of two BA networks is considered here because it can represent the heterogeneity of many real-world networks [37]. Label the two networks as A and B. Without loss of generality, the number of nodes in the coupled networks A and B is assumed to be the same, $N_A = N_B = N$, with the same degree distribution. The two BA networks are interconnected by some links. These links provide paths for the traffic flow between the two coupled networks. Data packets can be delivered along the links between the two networks. A coupling probability p $(0 \leq p \leq 1)$ is used. It can be described as 'the number of interconnected links divided by the network size N'. Assume that each node has at most one interconnected link to the other network.

In the interconnected network, if some nodes of one network fail, then the nodes of the other network may also fail, due to cascading reactions and failure propagation from one network to another, thus leading to catastrophic failures eventually. To study these cascading failures caused by traffic overload dynamics, we assume that the load on one node can be redistributed to anywhere in the whole interconnected network through connecting links.

To describe the new model, we introduce three coupling preferences based on load distribution in a BA scale-free network [23].

- ***Assortative coupling pattern***. The nodes of network A are sorted in the descending order according to their loads, labeled as $x_1, x_2, \ldots, x_n$, where if some nodes have the same load, then randomly arrange them; nodes in network B are sorted in the same way, labeled as $y_1, y_2, \ldots, y_n$. Connect x_1 with y_1, connect x_2 with y_2, and so on. Finally, randomly connect $N \times p$ links between networks A and B.
- ***Disassortative coupling pattern***. The nodes of network A are sorted in the descending order according to their loads, labeled as $x_1, x_2, \ldots, x_n$. On the contrary, nodes in network B are sorted in the ascending order, labeled as $y_1, y_2, \ldots, y_n$. Connect x_1 with y_1, connect x_2 with y_2, and so on. Finally, randomly connect $N \times p$ links between the networks A and B.
- ***Random coupling pattern***. In each of the two networks, randomly select one node respectively. If neither of them has an interconnected link, then connect them. Thus, a total of $N \times p$ links will be connected randomly between the networks A and B.

2.2. Cascading dynamics

In this paper, assume that data-packets are transmitted according to the shortest-path routing rule as in most real-world information networks [1]. The amount of flows that one node needs to transmit is considered to depend on the total number of shortest paths passing through it. So the betweenness of node i is used to evaluate its load in the whole networks, which is defined as

$$B_i = \sum_{j \neq l \neq i} \frac{n_{jl}(i)}{g_{jl}} \tag{1}$$

where g_{jl} is the number of shortest topological paths from node v_j to v_l, and $n_{jl}(i)$ denotes the number of such paths from node v_j to v_l through node i, i.e. the load of node i equals the betweenness centrality. The capacity of node i is denoted by C_i. When the load of a node exceeds its capacity, it will fail. Furthermore, assume that [1] the capacity C_i of node i is proportional to its initial load L_i as follows:

$$C_i = (1 + \beta)L_i. \tag{2}$$

Here, constant $\beta \geq 0$ is the tolerance (or redundancy) parameter and L_i is the initial load of node i. The network operates in a stable state when $\beta \geq 0$. The role of the tolerance parameter in cascading failure dynamics has been studied [23], where the cascading failing process occurs locally to impact only its neighbor nodes. However, here the traffic load is distributed based on the shortest-path routing rule, i.e. the betweenness of the nodes. Therefore, the removal of any one node may affect all nodes in the network.

The dynamical process of the cascading failure can be described as follows: when one node is removed, this can change the shortest paths between other nodes. The data-packets through these nodes have to change their paths to arrive to the destination nodes, consequently the loads of other nodes will be changed (increased). Those nodes that loads exceed these capacities will fail, it can trigger load redistribution over and over again through the whole network, until the network reaches a final stable state.

When the cascading failure stops, the survived nodes may not be connected. The relative size of the remaining giant component G in network is usually used to measure the functional integrity and robustness of a network:

$$G = \frac{N'}{N} \tag{3}$$

where N and N' respectively represent the size (number of nodes) of the original network and the size of the giant component of the network after failures. When $G \approx 1$, it means that the network is well maintained. However, when $G \approx 0$, it indicates that the network is fully breakdown. For the same fraction of initial nodes removal, the network with the larger remaining G is more robust. In the past, it was found that the giant component G after cascading failure is largely associated with the tolerance parameter β with different coupling probabilities p, for interconnected or interdependent networks [23,36]. It was also found that G increases with β. These conform to one's intuition that the more redundant capacities a network has, the higher robust the network becomes. As a consequence, in the present paper, we first investigate G as a function of β with different attacking ambiguity parameter α. Then the focus will be on the attacking strategy, because it is easier to control the attack information than to transform the network structure and performance in real situations.

2.3. Fuzzy information attacks and failures

With the increasing scale of a network, one knows more information about the network, but the information may be imprecise (more does not mean clearer). Let α be the ambiguity of the information. Then, the interest is on the relationship between the giant component G and the ambiguity α based on the three coupling preferences. Specifically, consider the critical removed fraction f_0 of nodes after an attack or failure. To analyze it, some more notations are needed. Denote the degree of node v_i as d_i and the minimum degree and the maximum degree of nodes in the network by l and L, respectively. Moreover, let $\tilde{d}_i$ be the observed degree of node v_i. Suppose that the attacker attacks the nodes of highest degree $\tilde{d}$, then the second highest, and so on. If $\tilde{d}_i = d_i$, then the attack is an intentional attack; if $\tilde{d}_i$ is not related to d_i, then it is a random attack. The name of "fuzzy-information-based attack" refers to the situations between these two extreme cases. This attack pattern represents all attacks between random attack and intentional attack.

Now, assume [19] that $\tilde{d}_i$ is a random variable on the interval $[d_i - (d_i - l)(1-\alpha), d_i + (L - d_i)(1-\alpha)]$. So, one can write $\tilde{d}_i$ as

$$\begin{aligned}\tilde{d}_i &= d_i - (d_i - l)(1-\alpha) + (L-l)(1-\alpha)\rho \\ &= d_i\alpha + l(1-\alpha) + (L-l)(1-\alpha)\rho \end{aligned} \tag{4}$$

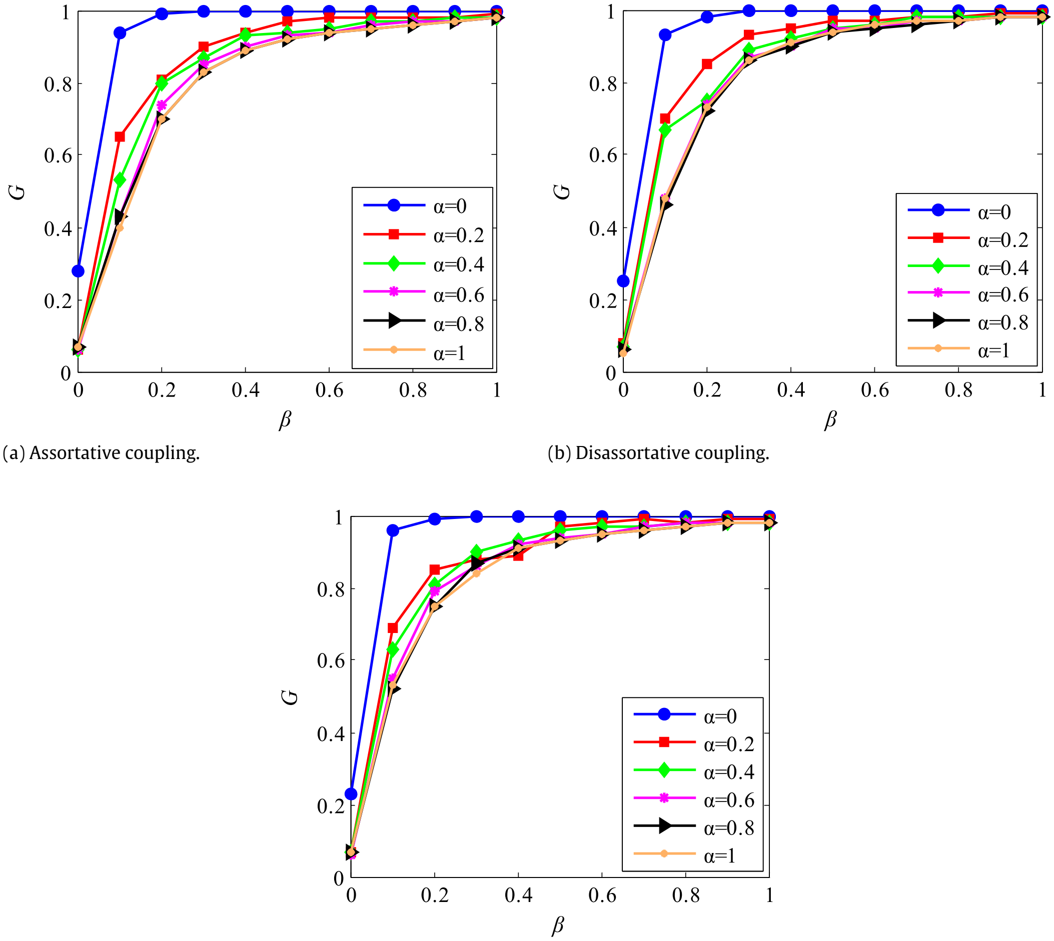
where ρ is a random variable with a uniform distribution on the unit interval $[0, 1]$, and the ambiguous parameter $\alpha \in [0, 1]$ represents the attack precision: when $\alpha = 1$, the attack is an intentional attack; when $\alpha = 0$, $\tilde{d}_i$ is a random variable with a uniform distribution in the subinterval $[l, L]$, therefore the corresponding attack is a random attack (or random failure).

Clearly, the cascading failing process of an interconnected network and that of a single network are different. When one node fails, the betweenness of the other nodes in the interconnected network will change consequently. Once the loads of some nodes exceed their capacities, these nodes will fail, and their loads will be redistributed all over the entire network through connections. This will trigger a series of changes until the remaining nodes have loads less than their capacities; or otherwise the network will crash into pieces of subnetworks. Noticeably, the cascading failure of one network can propagate to the other network through interconnections, thus causing more severe cascading failures. This cascading failing process will be simulated and analyzed in the next section.

3. Simulation results

Through extensive numerical simulations on the robustness of two interconnected BA networks subject to fuzzy information, the method in Ref. [38] is used. More precisely, choose the network size $N_A = N_B = 2000$, with average degree $\langle k_A \rangle = 6$, $\langle k_B \rangle = 6$. In the cascading failing process, the coupling preferences and coupling probability are all considered with respect to the traffic dynamics. As mentioned above, when we remove an initial node, the relative size of G in network after failures is used to quantify the network robustness. First, the relationship between the giant component G and the tolerance parameter β is investigated for a fixed coupling probability $p = 0.02$ under ambiguous information attack. Fig. 1 shows that G increases with β for any ambiguous parameter α. The results are approximately same for assortative, disassortative and random couplings, respectively. This is in agreement with our intuition, the more redundancy the network has, the higher the robustness is. Additionally, when $\beta = 0.2$, the robustness of the coupled network is very strong for any coupled preference. As a consequence, we set $\beta = 0.2$ for subsequent experiments.

Next, to obtain what coupling strength and which link pattern can effectively improve the robustness of the interconnected network against cascading failure, we research the relationship between the giant component G and the ambiguous parameter α for different coupling probabilities p. The tolerance parameter is $\beta = 0.2$. Fig. 2 shows such a relationship in the two interconnected BA networks, with assortative, disassortative and random couplings, respectively. It is obvious that the ambiguous parameter α affects G significantly. In the three cases considered, G decreases with α, so the conclusion is in accordance with that for a single network [19]. Comparing the first three Fig. 1(a), (b), (c), one can see that the robustness of the network with assortative coupling and random coupling increases with the coupling probability p. It means that increasing the number of interconnected links can enhance the network robustness. When the coupled network has very few interconnected links, all the loads will be located on a few nodes having these interconnected links.



(a) Assortative coupling.

(b) Disassortative coupling.

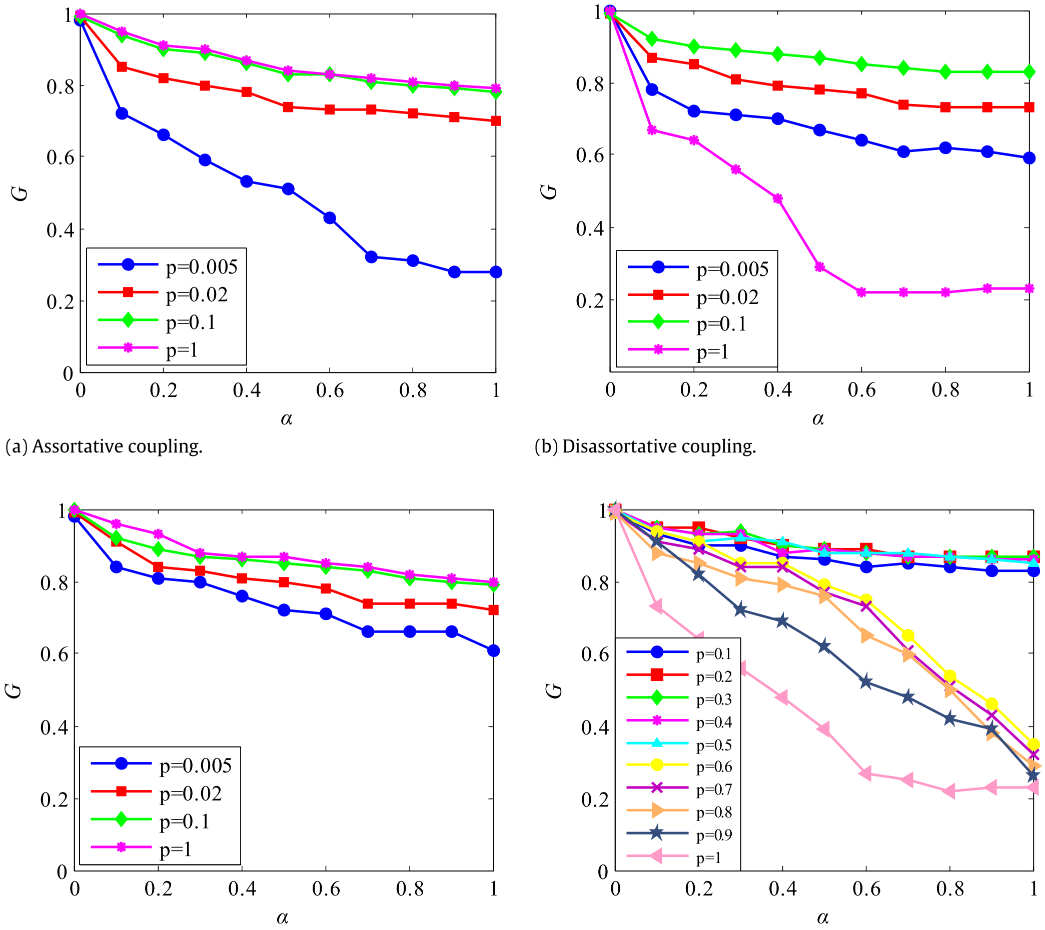
(c) Random coupling.

Fig. 1. Correlation between the relative size of the giant component G and tolerance parameter β with a fixed coupling probability $p = 0.02$, for assortative coupling (a), disassortative coupling (b) and random coupling (c), respectively. Every point is the average value over 50 realizations.

Consequently, the loads of these nodes are quite large. As soon as one of such nodes fails, its high load will be redistributed through a cascading process. This can cause many other nodes to be overloaded, thus fail as well. As more interconnected links are added, obviously this phenomenon can be relieved.

Another finding is that, for the disassortative coupling, only when $p \leq 0.1$, G increases with the coupling probability p. Moreover, as shown in Fig. 2(b), when $p = 1$, for the disassortative coupling, the node with the lightest load is prone to arrive at the destination node via shortest paths through interconnected links for data traffic. This increases the flows between the two networks, thus the robustness of the interconnected network decreases instead, when $p = 1$. This implies that if the interconnectivity is too high, it will lead to a severer detriment on the contrary. Furthermore, for the disassortative coupling, when $p = 0.1$ to 1, with step size 0.1, the results are as shown in Fig. 2(d). One can observe that when the coupling probability p reaches 0.6, the robustness of the coupling network abruptly decreases. Consequently, the coupling probability of $p = 0.6$ is the critical value for the disassortative coupling. It means that when the interconnected links become dense, the robustness of the network becomes worse on the contrary. There are two reasons. First, interconnective links open up pathways for the coupled networks to induce more severe cascading. Second, as in real networks, new interconnections increase the capacity and the total load, which can cause even larger cascading effects. The impact of defunctionalizing one node can easily spread out to the whole network due to the domino effect. One reason is overloading inside one network, and another reason is the loss of connectivity between the two networks.

In Fig. 3, one can also observe that the relationship between the ambiguous parameter value α and the giant component size G. For the same fraction of initial nodes removal, the simulation results are in general consistent among assortative coupling, disassortative coupling and random coupling cases, no matter which coupling preference is considered. The larger the α is, the worse the robustness is. For example, if the ambiguous parameter value is increased to $\alpha = 0.6$, then removing only 4% of nodes can cause a nearly complete disintegration of the interconnected network. In fact, the larger



(a) Assortative coupling.

(b) Disassortative coupling.

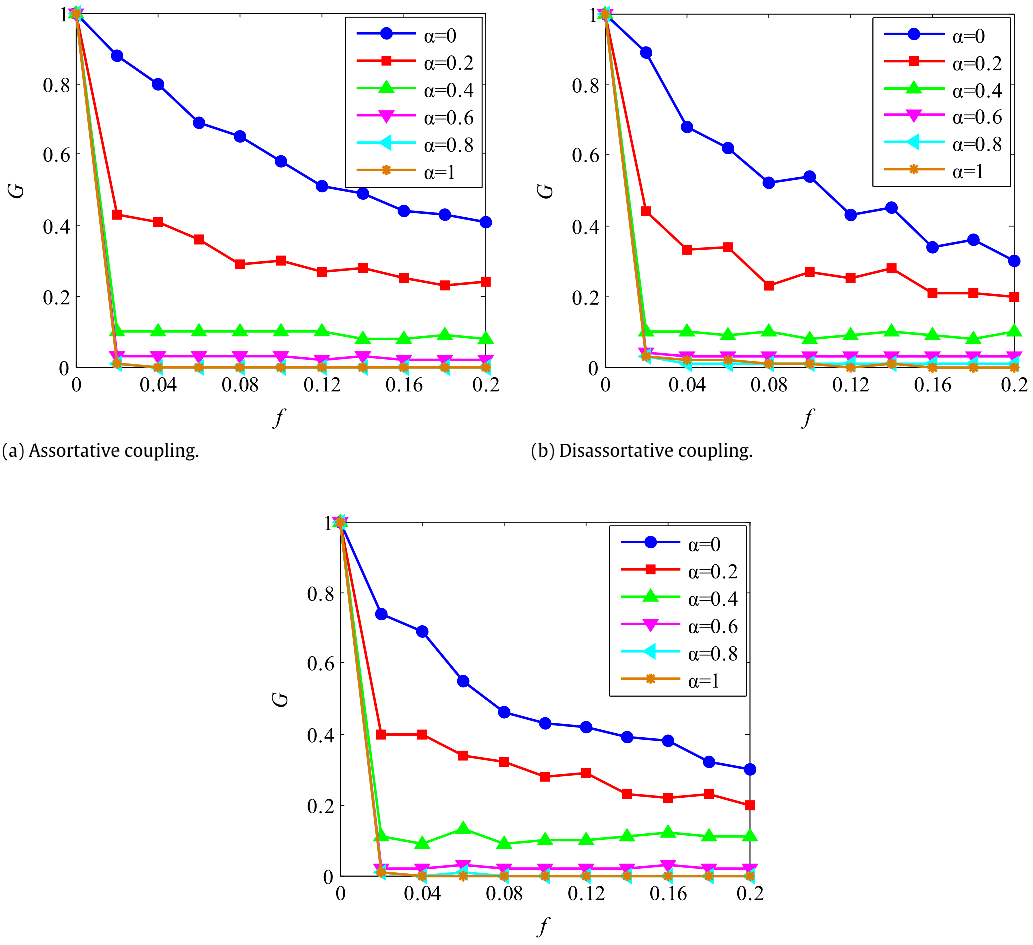
(c) Random coupling.

(d) Assortative coupling.

Fig. 2. Demonstration of cascading failures in two interconnected BA networks under fuzzy-information-based attacks. Three different types of coupling preferences are considered: (a) assortative coupling, (b) disassortative coupling, (c) random coupling. (d) All parameters are the same as in (b), except for $p = 0.1$ to 1, with step size 0.1. Every point is the average value over 50 realizations.

the α is, the more close to an intentional attack the real attack will be. Intentional attack aims at the most significant node (with the highest degree). Thus, after an attack, the shortest-paths going through this node between node-pairs will be changed. Consequently, it causes more severe traffic overloading and thus does more damage to the network. In other words, decreasing the ambiguous level of the fuzzy information can improve the robustness of the network.

For every fixed ambiguous parameter value α, there exists a corresponding critical removal fraction. In the study of the robustness of networks, a non-zero G means the network is functioning and $G = 0$ means that the whole network completely collapsed. In order to be more realistic in line with actual situations, a new performance indicator f_0 is introduced. It represents the minimum fraction of nodes to be removed from the network which cause the whole network to collapse, i.e. $G = 0$. Fig. 4 shows the critical removal fraction f_0 as a function of the fixed ambiguous parameter value α. For a network with any coupling preference, parameter α has an important effect on the robustness of the interconnected network. Regardless of the coupling probability p, when the value of α is low, f_0 decreases sharply as α increases. As shown in Fig. 4, there exists a critical value of $\alpha_c \approx 0.8$. When $\alpha > 0.8$, f_0 is almost same as that when α increases with different coupling probabilities, regardless of the coupling preference. Therefore, the efficiency of attacking a network based on fuzzy information at a time is almost the same as that of the intentional attack at this time. The result can be interpreted as that the central nodes which caused all nodes to fail can be accurately identified at this time. Consequently, the effect of cascading failures is the same as the situation with $\alpha = 1$. After the central nodes of a network are being attacked, cascading failures can happen due to traffic overloading, thus it can lead the network to collapse quickly. So, the accuracy of the information on other nodes besides the central nodes can hardly affect the robustness of the network. It is remarkable to see that this result is different from the findings of Li et al. [19]. When $\alpha > 0.8$, the critical removal fraction in Ref. [19] apparently decreases as α increases. This is mainly because the cascading failure of a network is considered here, while the static robustness of a network is discussed there. Also, an interconnected network is considered here, but only a single network is studied there. According to some previous research results [1], the robustness of a coupled network is generally worse than that of a single network.



(a) Assortative coupling.

(b) Disassortative coupling.

(c) Random coupling.

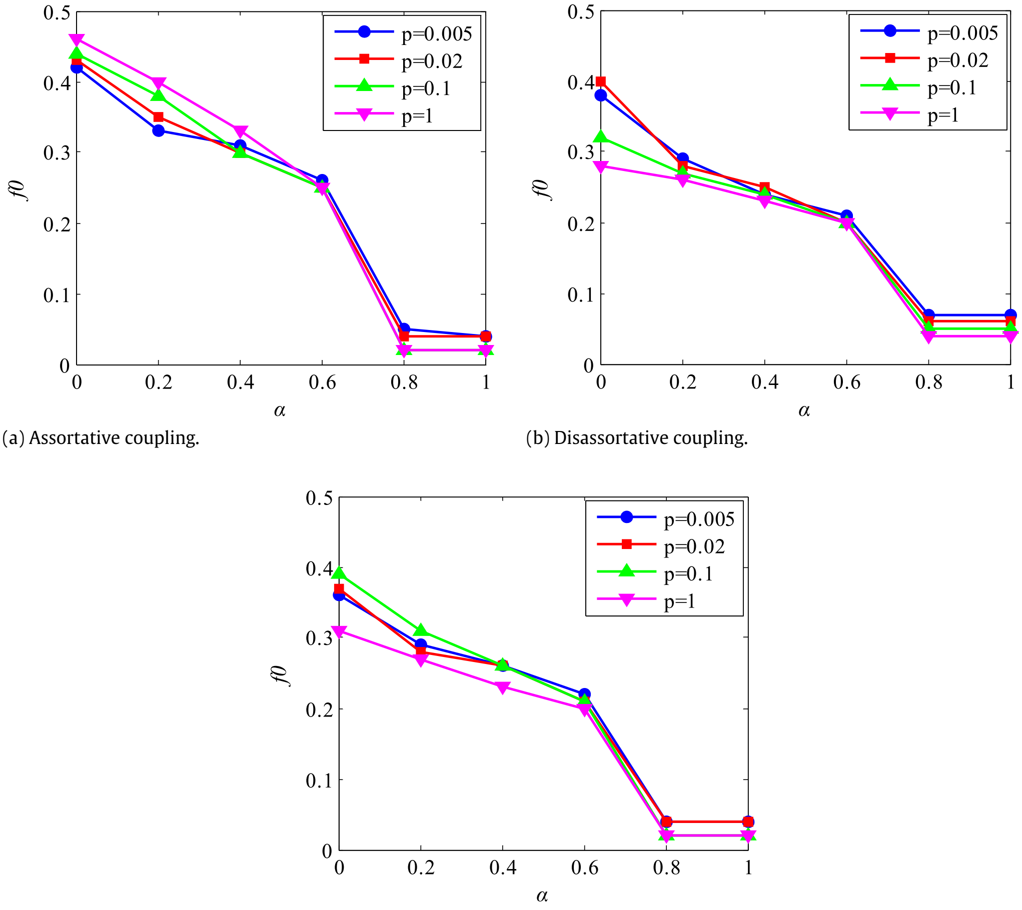
Fig. 3. Correlation between the relative size of the giant component G and the removal fraction f with different ambiguous parameter values α, for assortative coupling (a), disassortative coupling (b) and random coupling (c), respectively. The coupling probability is $p = 0.02$. Every point is the average value over 50 realizations.

4. Application example

Many real-world networks are evolving through interconnections of single subsystems. Consider two interconnected components of the Internet at the autonomous system (AS) level in South Korea and Japan [33]. These two networks are also connected to networks of other countries or regions, which are ignored for simplicity in this discussion. Network SK and JP are of sizes $N_{SK} = 677$ and $N_{JP} = 509$, respectively. They both have a power-law degree distribution as shown in Fig. 5. It is found that these two networks are sparsely interconnected by just 14 links, which is close to the model in this paper with $p = 0.02$. These 14 links follow the random coupling preference discussed above. The role of the connectivity between the two networks provides paths for transmitting data packets between the two countries, to work together properly.

First, when we remove an initial node, the relationship between the relative size of the giant component G after failures and the ambiguous parameter value α for the interconnected Internet AS-level topologies of South Korea and Japan is shown in Fig. 6. As can be seen in Fig. 6, G decreases with α. This is in agreement with the above analysis on the idealized model.

Second, the robustness of the interconnected SK and JP networks is also explored through studying the relative size of the giant component G for the same fraction of the initial nodes removal f with different values of α, as shown in Fig. 7. Obviously, decreasing the information precision can improve the robustness of the networks. When $\alpha = 0$, the corresponding attack is a random failure; but when $\alpha = 1$, the corresponding attack is intentional attack. When $\alpha > 0.6$, even if 4% of the nodes fail, G remains almost not changed. To be specific, this is because the precision of information becomes higher, the central nodes are easier to be attacked. After that, the accuracy of attacking other nodes besides the central nodes can hardly affect the robustness of the networks. This is in agreement with the above analysis on the model. Fig. 8 also verifies this observation. More precisely, when α is low, f_0 (the critical removal fraction at which $G = 0$) decreases sharply as α increases; when



(a) Assortative coupling.

(b) Disassortative coupling.

(c) Random coupling.

Fig. 4. Correlation between the critical removal fraction f_0 and a fixed ambiguous parameter value α for different coupling probabilities p, with assortative coupling (a), disassortative coupling (b), random coupling (c), respectively. Every point is the average value over 50 realizations.

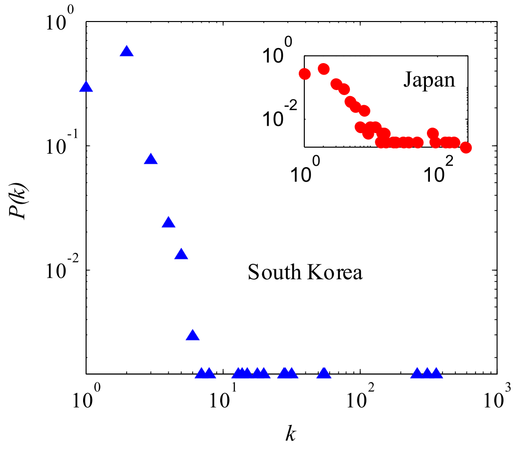


Fig. 5. The degree distributions of networks SK and JP. Internet AS-level topologies of the South Korea, with $N_{SK} = 677$ nodes and the averaged internal connectivity degree $\langle k_{SK} \rangle \approx 3.65$. Internet AS-level topology of Japan, with $N_{JP} = 509$ nodes and $\langle k_{JP} \rangle \approx 4.40$.

$\alpha > 0.8, f_0$ remains almost not changed even if α increases, i.e. the robustness of the networks is no longer changed. The SK and JP network data firmly verify the above analysis and conclusions.

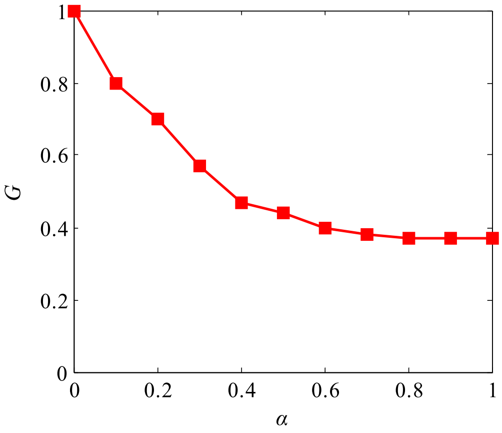


Fig. 6. Demonstration of cascading failures in the interconnected Internet AS-level topologies of South Korea and Japan under fuzzy-information-based attacks. The figure shows the relationship between the giant component G and the ambiguous parameter value α. Every point is the average value over 50 realizations.

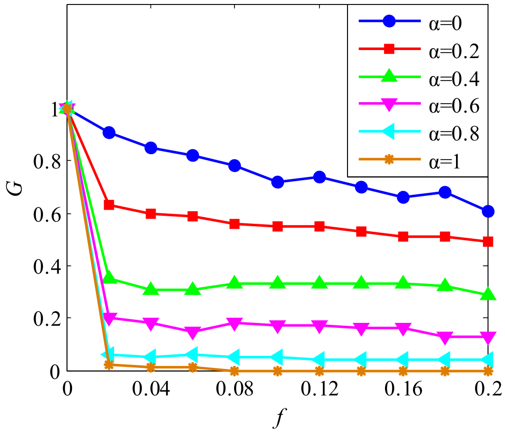


Fig. 7. Correlation between the relative size of the giant component G and the removal fraction f for different ambiguous parameter values of α on the cascading failures of the interconnected Internet AS-level topologies of South Korea and Japan under fuzzy-information-based attacks. Every point is the average value over 50 realizations.

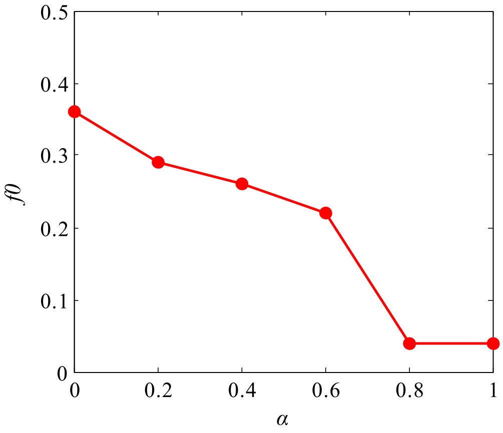


Fig. 8. Correlation between f_0 and the ambiguous parameter values of α for the real interconnected Internet AS-level topologies of South Korea and Japan. Every point is the average value over 50 realizations.

5. Conclusions

In this paper, we have studied cascading failures of interconnected networks based on fuzzy-information-attacks in terms of traffic loads. Our results demonstrate that the remaining giant component of the network after the same fraction of initial nodes removal increases with tolerance parameter for any ambiguous attacking parameter value. Assortative, disassortative and random couplings share a similar robustness. We find that the robustness of the network with assortative coupling and random coupling increases with the coupling probability. Nevertheless, for the disassortative coupling, when the coupling probability reaches 0.6, the robustness of the coupling network abruptly declines, it is an interesting and enlightening phenomenon. In addition, we find that the larger the ambiguous attacking parameter value is, the worse the robustness of the network is, no matter which coupling preference is considered. Furthermore, we used a critical removal fraction f_0 of nodes for disintegration of networks to measure the robustness of the network. We find that there exists a critical value of $\alpha_c = 0.8$. When $\alpha > 0.8$, f_0 is almost constant as ambiguous attacking parameter increases with different coupling probability, regardless of the coupling preference. Finally, the new model has been applied to study the interconnected Internet at the AS-level between South Korea and Japan. The results on the realistic data are consistent with the previous theory model. Our research results could provide guidelines and help for improving the robustness of interconnected network. In terms of future work, we are planning to explore the failure spreading within a layer and across layers, by considering the intra-links in either one of the two networks and the inter-links between the two networks.

Acknowledgment

We would like to thank Tanfei for supplying real Internet data for our simulation.

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61473073, 61374178, 61202085, 61402092, 61440014), the Fundamental Research Funds for the Central Universities (Grant Nos. 130417004, 130317001, 130317003), and the National Natural Science Foundation of Liaoning Province, China (Grant No. 201202076).

References

[1] A.E. Motter, Y.C. Lai, Cascade-based attacks on complex networks, Phys. Rev. E 66 (2002) 065102.
[2] P. Crucitti, V. Latora, M. Marchiori, Model for cascading failures in complex networks, Phys. Rev. E 69 (2004) 045104.
[3] R. Albert, H. Jeong, A.L. Barabasi, Error and attack tolerance of complex networks, Nature 406 (2000) 378–382.
[4] J.W. Wang, L.L. Rong, Cascade-based attack vulnerability on the US power grid, Saf. Sci. 47 (2009) 1332–1336.
[5] W.X. Jin, P. Song, G.Z. Liu, H.E. Stanley, The cascading vulnerability of directed and weighted network, Physica A 427 (2015) 302–325.
[6] W.X. Wang, G.R. Chen, Universal robustness characteristic of weighted networks against cascading failure, Phys. Rev. E 77 (2008) 026101.
[7] A.E. Motter, Cascade control and defense in complex networks, Phys. Rev. Lett. 93 (2004) 098701.
[8] J. Ash, D. Newth, Optimizing complex networks for resilience against cascading failure, Physica A 380 (2007) 673–683.
[9] J.W. Wang, L.L. Rong, A model for cascading failures in scale-free networks with a breakdown probability, Physica A 388 (2009) 1289–1298.
[10] X.B. Cao, C. Hong, W.B. Du, J. Zhang, Improving the network robustness against cascading failures by adding links, Chaos Solitons Fractals 57 (2013) 35–40.
[11] R. Yang, W.X. Wang, Y.C. Lai, G.R. Chen, Optimal weighting scheme for suppressing cascades and traffic congestion in complex networks, Phys. Rev. E 79 (2009) 026112.
[12] J.W. Wang, Mitigation strategies on scale-free networks against cascading failure, Physica A 392 (2013) 2257–2264.
[13] T. Tanizawa, G. Paul, R. Cohen, S. Havin, H.E. Stanley, Optimization of network robustness to waves of targeted and random attack, Phys. Rev. E 71 (2005) 047101.
[14] A. Majdandzic, B. Podobnik, S.V. Buldyrev, D.Y. Kenett, Spontaneous recovery in dynamical networks, Nat. Phys. 10 (2014) 34–38.
[15] L. Zhao, K. Park, Y.C. Lai, Attack vulnerability of scale-free networks due to cascading breakdown, Phys. Rev. E 70 (2004) 035101.
[16] L. Zhao, K. Park, Y.C. Lai, N. Ye, Tolerance of scale-free networks against attack-induced cascades, Phys. Rev. E 72 (2005) 025104.
[17] J.W. Wang, L.L. Rong, Edge-based-attack induced cascading failures on scale-free networks, Physica A 388 (2009) 1731.
[18] P. Holme, B.J. Kim, C.N. Yoon, S.K. Han, Attack vulnerability of complex network, Phys. Rev. E 65 (2002) 056109.
[19] J. Li, J. Wu, Y. Li, H.Z. Deng, Y.J. Tan, Attack robustness of scale-free networks based on grey information, Chin. Phys. Lett. 28 (2011) 058904.
[20] J. Wu, H.Z. Deng, Y.J. Tan, D.Z. Zhu, Vulnerability of complex networks under intentional attack with incomplete information, J. Phys. A 40 (2007) 2665–2671.
[21] S.V. Buldyrev, R. Parshani, G. Paul, H.E. Stanley, S. Havlin, Catastrophic cascade of failures in interdependent networks, Nature 464 (2010) 1025–1028.
[22] R. Parshani, C. Rozenblat, D. Ietri, C. Ducruet, S. Havlin, Inter-similarity between coupled networks, Europhys. Lett. 92 (2010) 68002.
[23] F. Tan, Y.X. Xia, Robust-yet-fragile nature of interdependent networks, Phys. Rev. E 91 (2015) 052809.
[24] J.W. Wang, Y. Li, Q.F. Zheng, Cascading load model in interdependent networks with coupled strength, Physica A 430 (2015) 242–253.
[25] J.X. Gao, S.V. Buldyrev, H.E. Stanley, S. Havlin, Networks formed from interdependent networks, Nat. Phys. 8 (2011) 40–48.
[26] G.G. Dong, J.X. Gao, L.X. Tian, R.J. Du, Y.H. He, Percolation of partially interdependent networks under targeted attack, Phys. Rev. E 85 (2012) 016112.
[27] M. Li, R.R. Liu, C.X. Jia, B.H. Wang, Critical effects of overlapping of connectivity and dependence links on percolation of networks, New J. Phys. 15 (2013) 093013.
[28] M. Li, R.R. Liu, C.X. Jia, B.H. Wang, Cascading failures on networks with asymmetric dependence, Europhys. Lett. 108 (2014) 56002.
[29] R.R. Liu, W.X. Wang, Y.C. Lai, B.H. Wang, Cascading dynamics on random networks: Crossover in phase transition, Phys. Rev. E 85 (2012) 026110.
[30] Z. Zhang, P. Zhang, H.J. Yang, Cascading failures in interconnected networks with dynamical redistribution of loads, Physica A 433 (2015) 204–210.
[31] W.P. Zhang, Y.X. Xia, B.Y. Ou, L.R. Jiang, Effect of network size on robustness of interconnected networks under targeted attack, Physica A 435 (2015) 80–88.
[32] M. Liu, D. Li, P. Qin, H. Wang, F. Wang, Epidemics in interconnected small-world networks, PLoS One 10 (2015) 0120701.
[33] F. Tan, J.J. Wu, Y.X. Xia, C.K. Tse, Traffic congestion in interconnected complex networks, Phys. Rev. E 89 (2014) 062813.
[34] X.Z. Peng, H. Yao, J. Du, Z. Wang, C. Ding, Load-induced cascading failures in interconnected networks, Nonlinear Dynam. 82 (2015) 97–105.
[35] F. Tan, Y. Xia, W. Zhang, X. Jin, Cascading failures of loads in interconnected networks under intentional attack, Europhys. Lett. 102 (2013) 28009.
[36] C.D. Brummitt, R.M.D. Souza, E.A. Leicht, Suppressing cascades of loads in interdependent networks, Proc. Natl. Acad. Sci. 109 (2011) 680–689.
[37] A.L. Barabasi, R. Albert, Emergence of scaling in random networks, Science 286 (1999) 509–512.
[38] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, D.U. Hwang, Complex networks structure and dynamics, Phys. Rep. 424 (2006) 175–308.