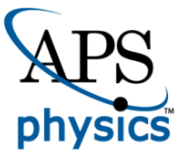

This is the accepted manuscript made available via CHORUS. The article has been published as:

Dynamic behavior analysis of an internet flow interaction model under cascading failures

Xiaoyu Wu, Rentao Gu, Yuefeng Ji, and H. Eugene Stanley

Phys. Rev. E **100**, 022309 — Published 16 August 2019

DOI: 10.1103/PhysRevE.100.022309

Dynamic behavior analysis of an Internet flow interaction model under cascading failures

Xiaoyu Wu[1,2], Rentao Gu[1],* Yuefeng Ji[3], and H.Eugene Stanley[2]
[1] *Beijing Laboratory of Advanced Information Networks, School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[2] *Center for Polymer Studies and Department of Physics, Boston University, Boston 02215, Massachusetts, USA and*
[3] *State key lab of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications,Beijing 100876, China*
(Dated: August 1, 2019)

Cascading failures in the Internet have attracted recent attention due to its unpredictability and destructive consequences. Exploring the failure behavior patterns is necessary because it can provide effective intervention approaches to prevent huge network disasters. To analyze Internet flow behaviors during cascading failures (chain reactions in router and link failures), we characterize the Internet as two coupled networks, the router network and the flow network. Here, flow network is an abstract representation of data correlations obtained from the router network. We use this coupled network to build a cascading failure model for studying flow transmission and competition, which reflects in bandwidth competition given by limited link capacity. We first study the dependency between routers and flows to explore the flow transmission efficiency when a failure event occurs. What's more, we find that rerouting enables flow competition area (the number of flows that one flow has competitive relationship with) to initially remain stable during a failure episode, but that it then quickly drops due to poor physical network connectivity. Additionally, in the early stage after the failure event, the degree of flow competition sharply increases because of the growing number of the flows and congestion. Subsequently, the flow competition decreases due to the failure of flow transmission.

PACS numbers: 89.20. Hh, 89.70. Hj, 89.75. Fb.

I. INTRODUCTION

Cascading failures in complex systems have attracted much attention in recent years [1–12] due to its destructive consequences.Failure propagations are hard to predict because system components are highly interdependent. But small random attacks [13] can destroy such systems as power grids [14–17], communication networks [18–20], and transportation systems [21–26]. Because the Internet is highly interdependent and an essential part of the social infrastructure, it is particularly vulnerable to network failure. A small initial shock, such as a flow burst or the breakdown of an Internet router, can trigger cascading failure. Understanding the response of Internet flow to the occurance of failure is essential, because it directly affects the quality of Internet service [27, 28]. The number of Internet flows is huge, and its relationship with network components (routers and links) is complicated; thus, analyzing flow behavior is extremely difficult.

Failure will happens in routers and links if they are heavily overloaded, which means that the routers or links are no longer able to forward upcoming data flows. Therefore, cascading failures will bring devastating influence by destroying network structures and functions. We describe these consequences as macroscopic behaviors, because they are happening on real physical entities. Learning macro-level behavior during a failure is an efficient and direct approach to trace the reason behind, and many researchers did a lot of work on this topic recent years. Crucitti et al.[29] propose a cascading failure model based on dynamic flow redistribution. They find that, if a single node is carrying a load above a certain high threshold, its failure can cause system collapse. The resiliance of the Internet has been described as "robust yet fragile (RYF) [30–32]. Guo et al.[31] propose a load-capacity model based on network dynamic protocols and flow load patterns to analyze the RYF phase transformation of network damage during failure. Simulation results show that the RYF behavior in the Internet is similar to an abnormal network load pattern. Liu et al. [33] discover that the router failure can increase the flow load pressure of related routers and cause cascading failure in the router network. Note that all of these research findings focus on how failure affects Internet macro-level behaviors, e.g., network efficiency and network phase transition [34]. An adequate analysis of micro-level behaviors, such as flow behaviors, has not yet been carried out.

In this paper we model the Internet as two coupled networks, the physical network of routers and links and the flow network of individual Internet flows. We use this model to analyze the flow dynamic behavior in cascading failure, taking flow rerouting capacity and dynamic network resource allocation into consideration. As

* rentaogu@bupt.edu.cn

to network resource allocation, bandwidth is one of the most concerned network resources in the Internet, flows with different priorities take up different bandwidth resource following specific rules, and this is called network resource allocation.

Based on the cascading failure model established, we study the dynamic dependency between routers and the flows during failure. We also examine flow competition behaviors, including flow competition areas and competition degrees during the failure process. Flow competition usually reflects in bandwidth competition due to the limited link capacity, and flow competition area refers to the number of flows that one flow has competitive relationships with. The behaviors mentioned above indicate how cascading failure affects Internet flow patterns, and enable us to increase Internet robustness.

We organize the paper as follows. Sections II and III describe the coupled network and cascading failure models, respectively. Section IV explains the transmission and competition behaviors of the Internet flows during failure. Section V is a summary and provides some conclusions.

II. COUPLED NETWORK MODEL

To start with, we define what flow is. The Internet flow is not a single data packet. It is a continuous packet flow where packets have the same source and destination address, belonging to the same service request.

Since flows compete for the finite network resources, such as bandwidth resource, we construct a flow network to characterize the competitive relationships among flows (see Fig.1(b)). In the flow network $G_f = (V_f, E_f)$, node set V_f represents the flows in the Internet and edge set E_f competitive relationships between flows. $W_f = \{w_f\}$ is the node weight matrix of $G_f = (V_f, E_f)$ that quantifies the degree of flow congestion. $w_f = (d_f - b_f)/d_f$, where d_f and b_f represent the flow bandwidth demand and the actual transmission bandwidth, respectively.

When two flows share links in the Internet, there is potential competition between them, and we connect them in the flow network. For example, fig.1(a) shows a small mesh network with six routers. Packet flows, numbered 1-5, are transmitted in this network. Flow 3 and flow 4 share two links in fig.1(a), so there is an edge between node/flow 3 and node/flow 4 in fig.1(b). However, there is no connection between flow 2 and flow 4 because they do not share links. The flow network reflects the competitive relationships between Internet flows, and also we could better observe the competition degree and its trends during cascading failures by applying this flow network.

Furthermore, to clearly show how flows and routers interact with each other, we model the Internet as two coupled networks (see fig.2), the top layer is the flow network, the bottom layer is the router network. We use $G_r = (V_r, E_r)$ to describe the router network, where

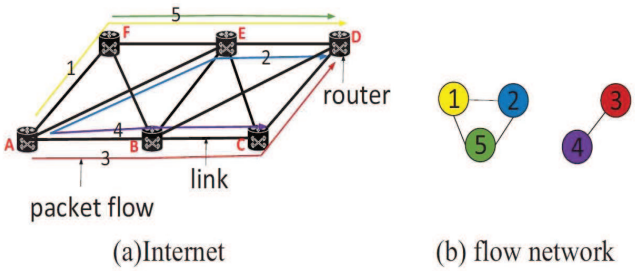

FIG. 1. (Colour online) An example of the Internet and the corresponding flow network. Fig.1 (a) shows an example of the Internet. Nodes represent routers, edges represent links. Flows numbered 1-5 are transmitted in this network; flow paths are showed with different colors. Fig.1 (b) shows the corresponding flow network. In the flow network, each node represents a packet flow, node number in fig. 1(b) are in accord with the flow number in fig.1 (a). Connections between flows represent the competitive relationships.

V_r represents routers and E_r represents links between routers. $W_r = \{w_r\}$ is the edge weight matrix of $G_r = (V_r, E_r)$ that quantifies the transmission capacity l of links, $w_r = l$. The dependencies between the flow network and the router network are established by the following rule. When a flow passes through a router, there is a connection between flow and router. For example, flow 3 passes through routers A, B, C and D (see Fig.1 (a)), so we connect flow 3 with routers A-D (see dotted lines in Fig.2). In return, we could locate one of the possible transmission paths of a flow by tracing the dependent connections in the coupled networks.

Cascading failure process is usually described by the chain reaction in node and link failure. During this failure process, flow interactions and the dependencies between flows and routers change because of the re-routing rule, thus the coupled network established above is also dynamic.

III. CASCADING FAILURE MODEL

In previous work, the cascading failure is usually modeled by the chain reaction in node failure, where an overload condition destroys a node as a whole[21–26]. However, this may not match the real Internet. In fact, routers have multiple ports working in parallel, and link capacity determines the maximum forwarding packets in each port. If more packets arrive at router port than the port capability, the overload packets will have to wait in a buffer, resulting in link congestions. When the congestion reaches a certain level, the port stops working normally, resulting in the functional failure in the attached links. Therefore, in the real Internet congestions will cause failures of the corresponding links, not directly in the whole router.

Based on the failure principles of ports and links men-

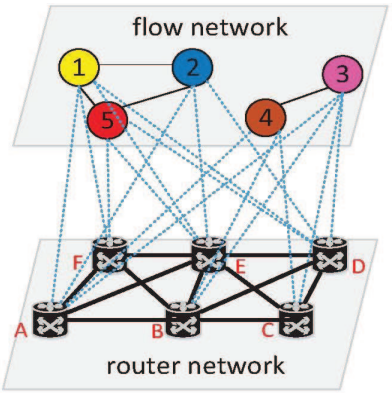

FIG. 2. (Colour online) The coupled networks of the Internet. The top layer is the flow network. The bottom layer is the router network. Connections between the two networks reveal the dependencies between flows and routers.

tioned above, we abstract the cascading failure process as follows: in our model of cascading failure, overloaded ports cause failures in the attached links by losing their ability to transfer flows, and subsequent flows bypass these failed links and choose alternate paths. This causes a redistribution of flows, which can cause overloads and failures in other links. As this process continues, cascading failures occur. Recovery is possible during an overload failure, but it is often slowed by such complex congestion relief mechanisms, such as buffer management and queue scheduling [35, 36]. Thus, we do not consider device recovery in our model.

Bandwidth allocation algorithm is introduced to understand how flow load distributes and overload failure occurs. In the router network, $L = \{l\}$ is the transmission capacity of the link. In the flow network, $D = \{d\}$ is the flow bandwidth demand. The $B = \{b\}$ value is the actual flow transmission bandwidth. $(d - b)$ is the number of packets waiting in the buffer per unit time. Obviously, the transmission bandwidth is no more than the bandwidth demand, i.e., $b \leq d$. The $\Phi = \{\phi\}$denotes the flow priority. Higher priority services can be transmitted preferentially. In general, the flow transmission bandwidth is in proportion to its priority [37, 38].

For each flow, once its source and destination are determined, a path from the source to the destination is chosen based on a specific routing algorithm. If there are multiple paths, we choose one randomly. Suppose the path of flow f_o is represented by link set $\{e_{r,1}, e_{r,2}, ..., e_{r,i}, ...e_{r,N}\}$. Using the proportional allocation algorithm [37, 38], the transmission bandwidth of flow f_o allowed by link $e_{r,i}$ is

$$b_{f_o,e_{r,i}} = min\{l_{e_{r,i}} \frac{\phi_{f_o}}{\sum_{f_o \in F_{e_{r,i}}} \phi_{f_o}}, d_{f_o}\}, \quad (1)$$

here $l_{e_{r,i}}$ is the transmission capacity of link $e_{r,i}$, ϕ_{f_o} and d_{f_o} are the priority and the bandwidth demand of flow f_o, respectively, and $F_{e_{r,i}}$ is the set of flows that pass through link $e_{r,i}$.

The transmission bandwidth of flow f_o is also affected by the other links that support its transmission. Since the bandwidth is continuous on the whole path, the final transmission bandwidth of flow f_o on every link of its path is decided by the minimum bandwidth.

$$b_{f_o} = min\{b_{f_o,e_{r,1}}, b_{f_o,e_{r,2}}, ...b_{f_o,e_{r,i}}, ...b_{f_o,e_{r,N}}\}. \quad (2)$$

For link $e_{r,i}$, the transmission load is

$$l'_{e_{r,i}} = \sum_{f_o \in F_{e_{r,i}}} b_{f_o}, \quad (3)$$

In the same way, we can calculate the transmission bandwidths of all flows and transmission loads of all links.

Thus far we have obtained the initial flow load distribution in the network, and we can use this quantity to further study link overload failures.

In the Internet, if more packets arrive at router ports than they are able to process per unit time, the extra packets wait in buffer and build up queues. According to TCP/IP protocol [39], the buffer size is determined by the link capacity and the Round-Trip Time (RTT) of packets. We use parameter β to reflect the Round-Trip time, then the buffer size is described as

$$Q_{e_{r,i}} = \beta l_{e_{r,i}}. \quad (4)$$

If the congested packets in link $e_{r,i}$ are larger than the buffer size $Q_{e_{r,i}}$, i.e., when

$$\sum_{f_o \in F_{e_{r,i}}} d_{f_o} - l'_{e_{r,i}} > Q_{e_{r,i}}, \quad (5)$$

an overload failure occurs in link $e_{r,i}$. Otherwise, link $e_{r,i}$ works normally.

Using the initial flow load distributions of Eq. (1) and the link failure criterion of Eq. (5),we found the failed links and temporarily removed them from the network. Flows will then reroute and find alternate paths based on the new network structure. Through flow rerouting, flow loads are redistributed according to the proportional bandwidth allocation algorithm provided by Eq. (1) and (2), and can cause failures in other links. As this process continues, cascading failures occur.

Based on the failure model established, we further model the flow behaviors during a failure process.

In the coupled networks of Internet (see Fig.2), cross-layer connections between flows and routers reflect the transmission paths of flows. So we quantify the dependency connections to reflect the flow transmission efficiency. ρ is the dependency intensity, which is described as

$$\rho(t) = \frac{\mu(t)}{N_{Router} N_{Flow}}, \quad (6)$$

where t is the flow load redistribution time, revealing the failure process. N_{Router} is the number of routers,

N_{Flow} is the number of flows. $N_{Router}N_{Flow}$ denotes all the possible dependency connections. μ is the actually existing interconnections, which may change during the cascading failure. For each flow, the connections with routers is one more than its path length. Thus,

$$\mu(t) = \sum_{f_i \in N_{Flow}} (len(f_i, t) + 1), \tag{7}$$

$len(f_i, t)$ is the path length of flow f_i. ρ then equals

$$\rho(t) = \frac{\sum_{f_i \in N_{Flow}} (len(f_i, t) + 1)}{N_{Router} N_{Flow}}. \tag{8}$$

When the flow number is large enough, we can use average path length $\bar{s}$ to further obtain the theoretical value of ρ .

$$\rho^*(t) = \frac{(\bar{s}(t) + 1) N_{FLow}}{N_{Router} N_{Flow}} = \frac{\bar{s}(t) + 1}{N_{Router}}, \tag{9}$$

here $\bar{s}(t)$ is the average path length of flows. Usually, a lower value of ρ^* means a shorter average path length of flows, implying a higher flow transmission efficiency.

In addition to flow transmission behaviors, we also model flow competition behaviors. The giant component in a network is often used to measure the effect of cascading failures [40–43]. In a flow network, g_F reflects the maximum competition area.

$$g_F = \frac{N^{'}_{Flow}}{N_{Flow}}, \tag{10}$$

$N^{'}_{Flow}$ is the number of flows in the giant component of flow network.

Further, the flow competition degree γ is described as

$$\gamma = \frac{1}{N_{Flow}} \sum_{i=1}^{N_{Flow}} \frac{k_i(t)}{k_{max}} w_{f_i}(t), \tag{11}$$

where k_i is the degree of flow f_i, k_{max} is the initial maximum degree of flows. k_i/k_{max} quantifies the competition density of f_i . w_{f_i} is the congestion degree of f_i that quantifies the competitive strength. According to the definition of w_{f_i} ,

$$\gamma = \frac{1}{N_{Flow} k_{max}} \sum_{i=1}^{N_{Flow}} k_i(t)(1 - \frac{b_{f_i}(t)}{d_{f_i}}). \tag{12}$$

The maximum value of γ equals

$$\begin{aligned} \gamma_{max} &= \frac{1}{N_{Flow} k_{max}} (1 - \frac{b_{min}(t)}{d_{max}}) \sum_{i=1}^{N_{Flow}} k_i(t) \\ &= \frac{\bar{k}(t)}{k_{max}} (1 - \frac{b_{min}(t)}{d_{max}}), \end{aligned} \tag{13}$$

where $\bar{k}(t)$ is the average degree of flows, $b_{min}(t)$ is the minimum transmission bandwidth of flows, d_{max} is the maximum bandwidth demand of flows.

Now, we have modeled flow behaviors from perspectives of flow transmissions and flow competitions. In the next section, simulations are conducted by utilizing our model.

IV. SIMULATION AND ANALYSIS

To generate the router network, Barabási-Albert (BA) network and the Erdős-Rényi (ER) random network are taken into consideration. For BA scale-free networks, the network size is $N_{BA} = 2000$ with exponent $\lambda = 2.6$. For ER random networks, $N_{ER} = 2000$ and the average degree is $\bar{k} = 10$. α is to adjust the link transmission capacity.

$$l = \alpha l_0, \tag{14}$$

where $l_0 = 10$(Gps) is the basic capacity. $\beta = 0.1$(s) to measure the average Round-Trip Time of packets.

To initially trigger cascading failures, we randomly and intentionally select 5% routers for attack respectively, induce a redistribution of flow load, and create a congested network environment. Both attacked routers and attached links are removed. When the attacks are random, the routers are removed indiscriminately. When they are intentional, the higher degree routers are removed. 100,000 flows are randomly distributed in the router network, which means the source-destination pairs are randomly chosen. The paths are assigned through Dijkstra shortest path algorithm. Flows are endowed with random priorities $\Phi \in \{1, 2, 3, 4, 5\}$, and flow bandwidth demands obey a normal distribution $d \sim N(0.2, 0.4)$.

Fig.3 shows the dependency intensity ρ in several coupled networks under different attacks when $\alpha = 1$. The x-axis (t) is the flow load redistribution time, revealing the failure process. In the rest of the paper, for simplicity, the coupled networks derived from the BA scale-free Internet is called a BA coupled network, and the coupled networks derived from ER random Internet is called ER coupled network. From fig.3 we can see ρ and ρ^* have almost the same trendency, which means ρ does have a positive correlation with the average path length of flows $\bar{s}$. Utilizing this, we can measure the flow transmission efficiency by ρ . For example, BA networks are more efficient in packets delivery than ER networks because of lower values of ρ when $t = 0$ (no attack).

When a failure occurs, some links will fail and be removed from the network, the affected flows will choose other paths. Since the network is now less dense, the alternative paths are usually longer. Thus ρ increases at the beginning of the failure, and the flow transmission efficiency becomes progressively lower. The length of the rising period of ρ also reflects the network resilience. During this period, the router network is able to carry the flow load, although the flow transmission efficiency declines. The longer the rising period, the better the network resilience. In BA coupled networks the rising period is shorter than in ER coupled networks, which means that when there is a cascading failure, the resilience of the BA scale-free Internet is poorer.

As the failure progresses, ρ and ρ^* decreases. To explain this phenomenon, we further calculate the proportion of flows that are failed to be transmitted during the failure process (see subfigures $p(len = 0)$ in Fig.3). The

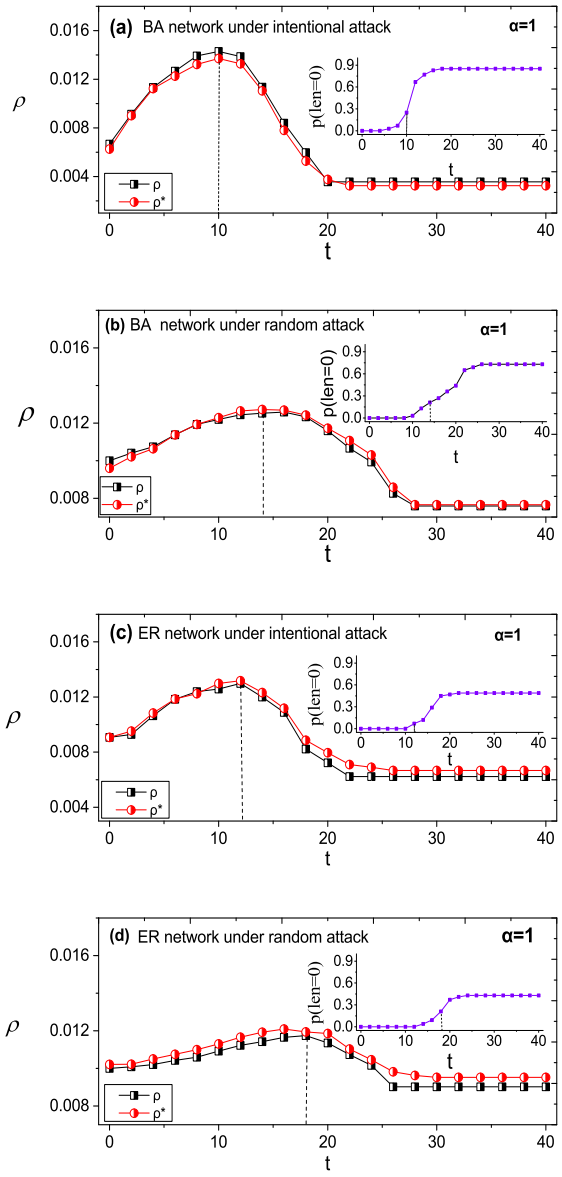

FIG. 3. (Colour online) Dependency intensity when ρ when $\alpha = 1$. t is the load redistribution time, revealing the failure process. For BA coupled network and ER coupled network, the router number is $N_{Router} = N_{BA} = N_{ER} = 2000$. 5% routers are initially attacked. $\beta = 0.1$ to measure the average RTT of packets. 100,000 flows are randomly distributed with random priorities $\Phi \in \{1, 2, 3, 4, 5\}$. The paths are assigned through Dijkstra shortest path algorithm. The flow bandwidth demands obey a normal distribution $d \sim N(0.2, 0.4)$. Simulation settings are the same below.

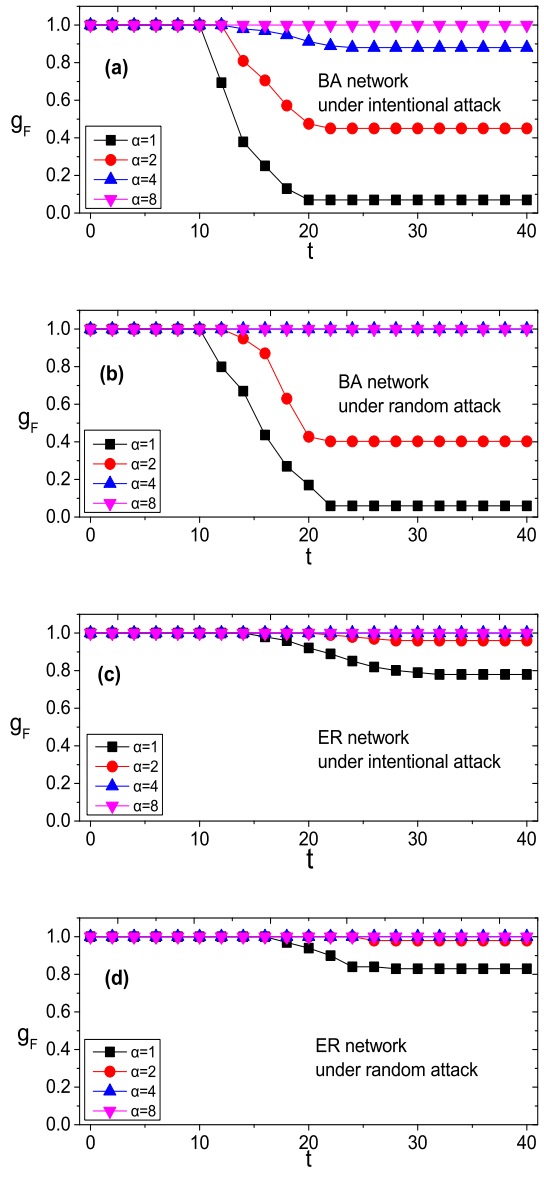

FIG. 4. (Colour online) Competition area g_F of flows. g_F reflects the maximal flow competition area. The decreasing trend of during failures in BA flow networks is much more obvious than that in ER flow networks. $\alpha = 1, 2, 4, 8$ separately to adjust the link transmission capacity (l). $l_0 = 10$(Gps). Simulation settings are the same as Fig.3.

turning point of ρ from increase to decrease is where there is a fair amount of untransmitted flows. The path lengths of untransmitted flows equal zero, leading to the decrease of ρ and ρ^* . Also, the decreasing trend indicates that there is a deteriorative connectivity of router network. For example, in BA coupled networks under intentional attacks (see Fig.3 (a)), the value ρ drops approximately 80%, and nearly 90% flows failed to be transmitted. The failure effect on network structure and connectivity is clearly serious. Furthermore, the vertical amplitude of ρ differs in different coupled networks. In BA coupled networks, the range of the amplitude is wider, indicating that more flows are affected by the failure and resulting in a clear effect on flow rerouting paths, especially when attacks are intentional.

Figure 4 shows the fluctuations of flow maximum competition area g_F during the failure process. When the

flow redistributes, the connections between flows are rebuilt, and we recalculate. For simplicity, the flow networks derived from the BA Internet is called BA flow network, and the flow networks derived from the ER Internet is called ER flow network. Figure 4 shows that BA flow networks are vulnerable to both intentional and random attacks. The maximum competition area is initially $g_F = 1$, then quickly drops as the cascading failure progresses. Initially, most flows interrupted by the failure can reroute, find alternate paths, and maintain their competitive relationship with other flows. As the failure continues, the connectivity of the router network deteriorates, many flows become isolated (see subfigures $p(len = 0)$ in Fig.3), and are no long able to compete for network resources. Thus, the size of the flow competition area drops quickly. In ER flow networks, however, the g_F values decrease very little under both random and intentional attacks, and most flows maintain their ability to compete for network resources. The competition area g_F in ER flow networks can be as much as 4 times the size of the competition area in BA flow networks. Furthermore, by increasing link capacity, the flow network can obviously improve its robustness, much more flows stay in the giant component and success in transmission.

Figure 5 shows the flow competition degree γ under different attacks. Note that γ increases at the beginning of the failure. This is because most of the flows affected by failure links reroute successfully at the beginning of the collapse. However, as the number of links and network resources decrease, the degree k_i of flow increases and the transmission bandwidth b_{f_i} declines, jointly leading to an increasing trend in γ . As the failure continues, γ decreases. Since router network connectivity deteriorates, an increasing number of flows become isolated. For these flows, the flow degree $k = 0$, leading to a decreasing trend in γ . All in all, the flow competition degree is affected by two factors, flow degree k_i and flow transmission bandwidth b_{f_i} . By ignoring the influence of b_{f_i} , we obtain the maximum value γ_{max} (Eq.13). From figure 5, γ and γ_{max} have the same trend, and as the failure continues, the difference gets smaller (see subfigures $\gamma_{max} - \gamma$ in fig.5). Since the calculation complexity of γ_{max} is much smaller, we could use γ_{max} to roughly evaluate the scale of flow competition degree. At last, due to the heterogeneous structure of BA network, flows in BA network are more concentrated. Under this circumstance, network attacks will influence more flows compared with ER network. Thus, γ varies much more obviously in BA flow network.

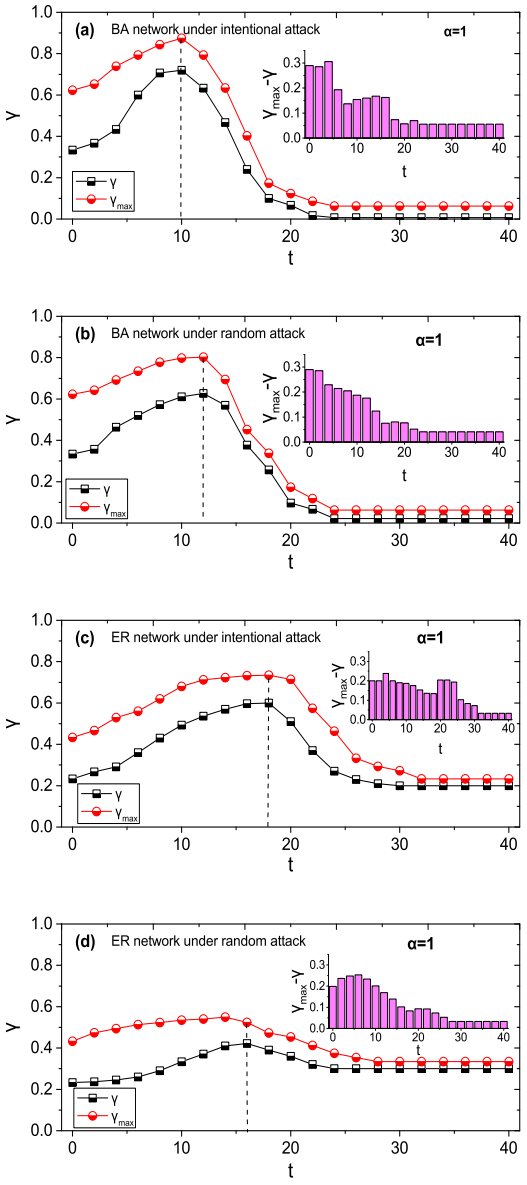

FIG. 5. (Colour online)Competition degree γ of flows. The flow competition degree in BA flow networks is more intense and concentrated. The difference of γ and γ_{max} gets smaller as the failure continues. Simulation settings are the same as Fig.3.

V. CONCLUSION

We have modeled the Internet as two coupled networks. We examine the cascading failure process and analyze flow dynamic behaviors, including flow transmission and competition. The way in which flow depends on routers indicates the flow transmission efficiency and network performance. The intensity of this dependence increases at the beginning of a failure event because flows are seeking alternative paths, which are invariably longer. As the failure intensifies and continues to spread, an increasing number of flows stop transmitting, and the transmission dependency thus rapidly decreases. Because flows are able to reroute, initially the flow competition area remains stable, but as the router network connectivity continues to deteriorate, the competition area sharply drops. We also have studied the flow competition degrees during the failure process. Ini-

tially the competition degree increases because degree of flow clustering and congestion both increase. As the failure progresses, the competition degree decreases due to the failure transmission of flows.

The cascading failure model and the flow behavior findings supplied in this paper will assist those who developing ways of improving Internet robustness when it responds to failure events.

ACKNOWLEDGMENTS

This work was jointly supported by Beijing Natural Science Foundation under Grant No. 4182040, National Natural Science Foundation of China under Grant No.61871051. The Boston University work was supported by NSF Grants PHY-1505000, CMMI-1125290, and CHE-1213217, and by DTRA Grant HDTRA1-14-1-0017 and DOE Contract DE-AC07-05Id14517.

[1] R. Albert, H. Jeong, and A.-L. Barabási, Nature **406**, 387 (2000).
[2] S. M. Chen, Y. F. Xu, and S. Nie, Physica A: Stat. Mech. Appl. **471**, 536 (2017).
[3] D. W. Zhao, Z. Wang, G. X. Xiao, B. Gao, and L. H. Wang, EPL **115**, 58004 (2016).
[4] S. Hong, C. Lv, T. D. Zhao, B. Q. Wang, J. H. Wang, and J. X. Zhu, J. Phys. A: Math. Theor. **49**, 195101 (2016).
[5] D. Q. Li, Y. N. Jiang, R. Kang, and H. Shlomo, Scientific Reports **4**, 5381 (2014).
[6] J. X. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, Phys. Rev. Lett. **107**, 195701 (2011).
[7] A. E. Motter and Y. C. Lai, Phys. Rev. E **66**, 065102 (2002).
[8] P. Dey, R. Mehra, F. Kazi, S. Wagh, and N. M. Singh, IEEE Transactions on Smart Grid **7**, 1970 (2016).
[9] M. A. DiMuro, S. V. Buldyrev, H. E. Stanley, and L. A. Braunstein, Phys. Rev. E **94**, 042304 (2016).
[10] M. Rohden, D. Jung, S. Tamrakar, and S. Kettemann, Phys. Rev. E **94**, 032209 (2016).
[11] I. Simonsen, L. Buzna, K. Peters, S. Bornholdt, and D. Helbing, Phys. Rev. Lett. **100**, 218701 (2008).
[12] Y. Yang, T. Nishikawa, and A.E. Motter, Phys. Rev. Lett **118(4)**, 048301 (2017).
[13] A. Moussawi, N. Derzsy, X. Lin, and B. K. Szymanski, Scientific Reports **7**, 11729 (2012).
[14] Y. Yang, T. Nishikawa, and A.E. Motter, Science **358**, 3184 (2017).
[15] D. P. Nedica, I. Dobsonb, D. S. Kirschena, B. A. Carrerasc, and V. E. Lynchc, International Journal of Electrical Power & Energy Systems **28**, 627 (2006).
[16] R. V. Sole, M. Rosas-Casals, B. Corominas-Murtra, and S. Valverde, Phys. Rev. E **77**, 026102 (2008).
[17] I. Dobson, and P. Rezaei, IEEE Transactions on Power Systems **32**, 958 (2017).
[18] S. Sreenivasan, R. Cohen, E. Lopez, Z. Toroczkai, and H. E. Stanley, Phys. Rev. E **75**, 036105 (2007).
[19] Y. Cai, Y. J. Cao, Y. Li, T. Huang, and B. Zhou, IEEE Transactions on Smart Grid **7**, 530 (2016).
[20] E. J. Lee, K.-I. Goh, B. Kahng, and D. Kim, Phys. Rev. E **71**, 056108 (2005).
[21] P. Zhang, B. S. Cheng, Z. Zhao, D. Q. Li, G. Q. Lu, Y. P. Wang, , and J. H. Xiao, EPL **103**, 68005 (2013).
[22] F. Tan, Y. X. Xia, W. P. Zhang, and X. Y. Jin, EPL **102**, 28009 (2013).
[23] S. Hong, B. Q. Wang, X. M. Ma, J. G. Wang, and T. D. Zhao, J. Phys. A: Math. Theor. **48**, 485101 (2015).
[24] Z. Su, L. X. Li, H. P. Peng, J. Kurths, J. H. Xiao, and Y. X. Yang, Scientific Reports **4**, 5413 (2014).
[25] J. Lehmann and J. Bernasconi, Phys. Rev. E **81**, 031129 (2010).
[26] S. Mizutaka and K. Yakubo, Phys. Rev. E **92**, 012814 (2015).
[27] X. Y. Wu, R. T. Gu, and Y. F. Ji, Physica A: Stat. Mech. Appl. **462**, 341 (2016).
[28] X. Y. Wu, R. T. Gu, and Y. F. Ji, EPL **116**, 18005 (2016).
[29] P. Crucitti, V. Latora, and M. Marchiori, Phys. Rev. E **69**, 045104 (2004).
[30] J. C. Doyle, D. Alderson, L. Lun, S. Low, M. Roughan, S. Shalunov, R. Tanaka, and W. Willinger, Proceedings of National Academy of Sciences of the United states of America **102**, 14497 (2005).
[31] C. Guo, L. N. Wang, F. R. Zhou, L. N. Huang, and Z. Peng, the 9th International Conference for Young Computer Scientists (ICYCS, Zhangjiajie 2008) , pp. 2149.
[32] F. Tan, Y. X. Xia, and Z. Wei, Phys. Rev. E **91**, 052809 (2015).
[33] X. H. Liu and Y. F. Ji, the 1st International Conference on Communications and Networking in China (IEEE, Beijing,2006) , pp. 1.
[34] Y. Yang, and A.E. Motter, Phys. Rev. Lett **119(4)**, 248302 (2017).
[35] K. M. Kobayashia, S. Miyazakib, and Y. Okabeb, Theoretical computer science **675**, 27 (2017).
[36] W. Choi, R. Sekhon, and W. Seok, Science China Information Sciences **59**, 069301 (2016).
[37] E. C. Park and C. H. Choi, Proceedings of 23rd IEEE International Conference on Computer Communications (INFOCOM) **3**, 2038 (2004).
[38] X. B. Zhou and C. Z. Xu, IEEE transactions on parallel and distributed systems **15**, 835 (2004).
[39] C. Villanmizar and C. Song, Acm Sigcomm Computer Communication Review **24**, 45 (1994).
[40] S. V. Buldyrev, N. W. Shere, and G. A. Cwilich, Phys. Rev. E **83**, 016112 (2011).
[41] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, Nature **464**, 08932 (2010).
[42] J. X. Gao, S. V. Buldyrev, H. E. Stanley, X. M. Xu, and S. Havlin, Phys. Rev. E **88**, 062816 (2013).
[43] J. X. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, Phys. Rev. E **85**, 066134 (2012).