# Tolerance of Intentional Attacks in Complex Communication Networks

Shi Xiao, Gaoxi Xiao and Tee Hiang Cheng
Division of Communication Engineering
School of Electrical and Electronic Engineering
Nanyang Technological University, Singapore 639798
Email: shixiao@pmail.ntu.edu.sg, egxxiao@ntu.edu.sg, ethcheng@ntu.edu.sg

***Abstract*—**Motivated by recent developments in the theory of complex networks, we examine the tolerance of communication networks to intentional attacks that aim to crash network by taking down network hubs. In addition to providing a brief survey of key existing results, we investigate two different effects that have been largely ignored in past studies: (i) Many communication networks, like Internet, are too large for anyone to have global information of their topologies, which makes accurate intentional attack virtually impossible; and (ii) most attacks in communication networks have to propagate from nodes to their adjacent nodes, utilizing local network-topology information only. We show that incomplete global information has different impacts to intentional attacks in different circumstances, and local information-based attacks can actually be highly efficient. Such insights will be helpful for the future developments of efficient network attack and protection schemes.

***Index Terms* —** Complex network, scale-free network, network robustness, intentional attack, distributed attack.

## I. Introduction

Recently there is increased interest in studying large-scale real-world systems by formulating them into various network models. It is found that different systems, which include Internet, world-wide web (WWW), airline transportation systems, food web, protein-protein reactions, co-authorship, and terrorist activities, when formulated into network models, share some stunning common features. The above observations have spawned a new research topic called *complex networks* [1].

The most important complex network model is probably the *scale-free network* [1]. In such networks, the nodal degrees follow a *power-law* distribution which means that the number of nodes

This work was supported in part by Microsoft Research Asia (MSRA).

with a nodal degree $k$ is basically proportional to $k^{-\alpha}$, where $\alpha$ is the exponent. Different from the very well-known Erdős-Rényi random graph [1], the most visible feature of the scale-free networks is the relatively large number of hub nodes they have, as shown in Fig. 1. It is claimed (though not without arguments, which we will discuss in more details later) that all the systems we mentioned above can be formulated as scale-free networks [1].

There have been debates on whether the communication systems, especially the Internet, are indeed scale-free networks [2]. While most statistical results are showing scale-free nodal-degree distributions in communication systems, the contentious point is that the traceroute method (the method of sending packets to record the addresses of all the network nodes they have passed through) used to sample the Internet topology may have led to the biased statistics [2]. The debates may not be resolved until a better sampling method is devised though it is widely agreed that the tracerouted part of the Internet indeed forms a scale-free network. For many applications, it is the tracerouted part that matters most since it is the part that can be steadily reached by the packets from the starting nodes.

Theory of complex networks sheds new light which helps to understand complex communication systems and networks. One of the most important results is that while a scale-free network is highly robust to random failures, it is fragile under *intentional attacks* that aim at bringing down network nodes in decreasing order of nodal degrees [1, 3]. In the Internet research domain, again there are hot debates on whether the fragileness indeed exists. Doyle and his colleagues argued that, as a result of careful design for maximizing network throughput, the hub nodes at the router level are typically the edge nodes with a large number of low-capacity connections. The removal of these hub nodes, though disastrous to the large number of low-capacity users connected to them, will not really bring down the Internet [4]. Meanwhile, it is widely believed that the self-emergent scale-free network models that are discussed in [3] may be adequate in modeling the Internet at the autonomous system (AS) level with plausible accuracy [5].

Other important existing results related to network robustness under intentional attacks include

- A modest alteration of link connections or link insertions between low-degree nodes can enhance the robustness of complex networks under intentional attacks [6]. Without changing its nodal-degree distribution, a scale-free network can still have enhanced robustness under intentional attack if (i) high-degree nodes tend to connect more densely with high-degree nodes; or (ii) medium-degree nodes mainly connect with lower-degree nodes [7]. However, it is not

clear how to encourage the alternation of link connections in self-organized, extra-large systems like Internet. And as long as the power-law nodal-degree distribution persists, intentional attack, by removing hub nodes together with the large number of links connected to them, remains as a serious challenge to network survivability.

- While under the intentional attack, a scale-free network can restore its connectivity by reconstructing a limited number of connections between the some affected nodes [8].

Still another closely related topic is the effect of malicious attacks causing cascading failures [9] as well as the countermeasures. Such studies have many applications in power grid safety, congestion control of communication and transportation networks, etc. A comprehensive survey of the existing results and their applications, however, requires a separate report.

We are motivated to study the robustness of communication systems under intentional attacks from a complex network point of view. Specifically, after perusing the existing results, we recognize that two different effects have largely been ignored. First, complex communication systems such as Internet and WWW are too large for anyone to get hold of their global topology information, which means an accurate intentional attack is hardly feasible. Second, for any real-world intentional attacks to take place, they have to "propagate" through the network by attacking the neighborhood nodes adjacent to those "crashed" nodes step by step. And such attacks typically are based on local information of network topology only. In this paper, we call such attacks *distributed attacks*.

We examine the above two effects by means of extensive simulations. It is shown that (i) different missed knowledge of network topology has different impacts on the efficiency of intentional attacks; hence hiding network-topology information (e.g., by keeping detailed network interconnections strictly confidential and/or hiding IP addresses of network hubs, etc.) may help strengthen network robustness under certain circumstances; (ii) on the other hand, distributed attacks with no global network-topology information can actually be highly efficient; in some cases it is almost as efficient as an accurate, global information-based intentional attack. Therefore more effective methods have to be developed to protect against such attacks.

The rest parts of this paper are organized as follows. In Section II, we study the efficiency of the intentional attack based on incomplete/inaccurate network-topology information. A few distributed attack schemes are proposed and evaluated in Section III. Finally, Section IV concludes the paper.

## II. INTENTIONAL ATTACKS BASED ON INCOMPLETE NETWORK-TOPOLOGY INFORMATION

The robustness of a network is typically measured by its *biggest cluster size* (i.e., the number of nodes in the biggest *connected* node set versus the number of nodes in the whole network) and the *cluster diameter* (i.e., the average length of the shortest paths between all the node pairs in the biggest connected node set) under attacks [1, 3, 6-10]. If a node has been attacked, we call it *crashed*; otherwise, we call it a *live* node.

As mentioned above, the classic intentional attack is defined as the attack that brings down network nodes in a decreasing order of their nodal degrees in the original network [1, 3]. In other words, the biggest hub node in the network is the no. 1 target of the attack, then the second biggest hub, etc. It has been shown by extensive simulations [3] and theoretical analysis [10] that scale-free networks are fragile under intentional attacks. To provide some examples, we simulate the classic intentional attacks using the following models:

- The well-known Barabási-Albert (BA) model that generates scale-free networks by "growth" and "preferential attachment" [1, 3]. Specifically, network nodes are sequentially added, where each of the newly-added nodes is connected to a fixed number of existing nodes. The probability that a newly-added node is connected to an existing node is proportional to the nodal degree of the existing node. In our simulations, we test the BA model with 10,000 nodes and 20,000 links.
- A real-world Internet model on the AS-level as measured by the Applied Network Research (NLANR) Project on January 2, 2000 [11], which contains 6470 inter-connected nodes and 12,566 links. We have verified that it is indeed a scale-free network.

The simulations have been conducted by using C programs developed by ourselves. We define the *threshold of crash* as the percentage of network nodes crashed when the biggest cluster size is reduced to no more than 5% of the original network size. It is shown in Fig. 2 that the BA model crashed when roughly about 14% of all the network nodes are taken down, while the Internet model has an even lower threshold of crash at about 2.7%. On the other hand, both networks are highly robust under *random failures* which randomly take down network node one after another [1, 3], with the thresholds of crash at 72% and 80%, respectively.

The threshold of crash under classic intentional attack in fact can be further lowered. Specifically, some hub nodes are mostly connected to other hub nodes, and a network can be crashed without

touching them: these nodes will become largely isolated once their neighborhood nodes, which are hub nodes by themselves, are taken down. By avoiding taking down such "non-critical" hub nodes (which obviously needs highly accurate global information), the thresholds of crash in the two example networks can be further lowered to 11% and 2.1% respectively. It remains as an open problem, however, to figure out the most efficient attacking method that minimizes a scale-free network's threshold of crash.

To study the efficiency of intentional attacks when accurate global information of network topology is *not* available, we consider two different cases as follows:

- Due to incomplete knowledge of network nodal-degree distribution, a big hub is missed in the intentional attack. As an example, we test the special case that only the biggest hub is missed while all the other hubs are accurately taken down;
- The big hubs are all taken down, yet some medium-sized hubs are missed in the attack. Specifically, in the BA model, we test the cases where the top 1% of biggest hubs are all taken down and after that, 10% and 50% of the next top 3% hub nodes (with nodal degrees varying from 12 to 23) are missed respectively. The same percentages apply to the simulations in the Internet model, where the degrees of missed medium-sized nodes vary from 10 to 40.

The simulation results are presented in Fig. 2. We observe that missing the single biggest hub makes the intentional attack drastically less efficient. In the BA model, 20% of all the nodes have to be removed before the network crashed, representing a 6% increase in the threshold of crash. In the Internet model, the effect is even more significant. The threshold of crash jumps from a very low 2.7% to a rather high 28.7%. The fragileness of the Internet model under the classic intentional attack and this significant increase in the threshold of crash are strongly related to the same reason: the Internet hubs are of very high degrees (The biggest hub's nodal degree is 1,458, while in the BA model it is only 386.). Therefore the survival of a single hub may drastically enhance network robustness. The lesson we can learn from such observations is obvious: it is worth all the efforts for the offending (defending) side to take down (protect) the big hubs.

Missing a certain portion of the medium-sized nodes also degrades the efficiency of intentional attacks, as we can observe in Fig. 2. Considering the fact that it is difficult to identify *all* the medium-sized nodes in extra-large communication networks, we argue that (i) the high possibility of missing some medium-sized nodes may severely degrade the efficiency of intentional attacks, and (ii)

for the defending side, in certain circumstances it may be more practical and more effective to protect or hide some medium-size nodes rather than the very obvious big hubs.

Another interesting observation is that in the BA model, missing 50% medium-sized nodes leads to a higher threshold of crash (26%) than that of missing the biggest hub (Fig. 2(a)), which is obviously not the case in the Internet model (Fig. 2(b)). This again can be explained by the relatively much lower degree of the biggest hub in the BA model: the impact of missing a degree-386 node, significant as it is, is surpassed by that of missing 150 medium-sized nodes with degrees between 12 and 23. The impact of missing the degree-1458 hub in the Internet model, on the other hand, overweighs that of missing 97 nodes with degrees between 10 and 40.

Finally, the cluster diameters of the two models under various types of intentional attacks are shown in Fig. 3. We see that in most cases, the cluster diameters are significantly increased long time before the network crashed, making the network highly inefficient in supporting data communications though it is still connected to a large extent. Such impacts can also be degraded when complete knowledge of network topology is not available, especially when a big hub is missed in the attack. As we can see in Fig. 3, when the biggest hub is not taken down, the cluster diameter actually never becomes too large during the whole process of attack until the network crashed. Once again, we see that the BA model maintains a relatively short diameter throughout the whole procedure when 50% medium-sized nodes are missed in the attack.

## III. DISTRIBUTED ATTACKS BASED ON LOCAL INFORMATION

As mentioned earlier, the distributed attack can only "propagate" through the network step-by-step, attacking the neighborhood of some nodes that had crashed before. Furthermore, the target(s) of the next-step attack is selected solely based on local information.

We evaluate several different distributed attack schemes as follows:

- **Greedy sequential attack:** the attack that chooses the largest-degree live node adjacent to the node crashed in the *last* step as its next-step target. If no neighborhood live node exists, it randomly selects a live node as its target.
- **Coordinated attack:** the attack that searches through *all* the live nodes adjacent to *any* crashed node and selects among them the largest-degree one as its next-step target. If no such node exists, it randomly selects a live node to continue the attack.

- **Lower-bounded parallel attack:** instead of taking down only a single node in each step, an attack is executed from *each* crashed node to take down its largest-degree neighborhood node *iff* that neighborhood node's degree is higher than a preset threshold. If no such neighborhood node exists, the attack stops.

Fig. 4 compares the efficiencies of the greedy sequential attack and the coordinated attack, respectively. It is shown that the greedy sequential attack is not quite effective in bringing down the whole network, whereas the coordinated attack, though based on local information only, achieves almost the same threshold of crash as that of an accurate intentional attack. This observation can be understood as follows: we have to take down a lot of low-degree nodes in a greedy sequential attack since, in many steps, there are no big hubs adjacent to the just-crashed node. In a coordinated attack, we can choose in each step the next-step target from a much larger number of nodes. Consequently we seldom need to attack a low-degree node. The main drawback of the coordinated attack, however, is the rather complicated collaborations between all the attacking frontiers in order to find the best next-step target.

To eliminate the complicated collaborations and information exchanges between all the attacking frontiers, we have proposed the lower-bounded parallel attack, which arguably may better resemble a real-world attack. To avoid the burden of taking down a large number of low-degree nodes, we set up nodal-degree lower bounds at 4 and 10 respectively. A live node adjacent to a crashed node will not be taken down unless its degree is strictly higher than the threshold.

The simulation results are reported in Fig. 5. For the Internet model, setting the nodal-degree lower bound at 10 makes the distributed attack almost as effective as the accurate intentional attack. In fact, the threshold of crash is only slightly increased from 2.7% to 2.9%. If we set the lower bound at 4, more nodes have to be taken down before the network crashed: the threshold of crash becomes 4.8%. On the other hand, fewer steps of attacks are needed since more nodes are taken down in each step. In the BA model, the observations are different: when we set the nodal-degree lower bound at 4, the threshold of crash is close to that of the accurate intentional attack (15% vs. 14%). When the threshold is set at 10, however, the attack will be terminated after 17 steps when the degrees of all the live nodes adjacent to the attacking frontiers are lower than the threshold. At that moment, the network is still largely connected.

The above observations can be explained as follows: the large-degree nodes in most complex

networks form a *connected* sub-network. Therefore we could attack and take down this sub-network virtually without going through any low-degree nodes. More significantly, to take down these large-degree nodes, we actually do not need any global information of network topology at all: local information-based attacks can easily penetrate through the connected sub-network. To protect a communication system from being crashed by such kind of distributed attacks, it is crucial to identify and stop the attack at the early stage. As we can see in Fig. 5, the networks' decomposition is slow at the early stage and then sped up tremendously after a certain number of steps into the attack. In addition, we observe that it is important for the offending side to select proper threshold values in such attacks: a low threshold causes the attack to take down a large number of low-degreed nodes unnecessarily, thus slowing down the attack and giving the defending side a better chance to react. On the other hand, a high threshold renders the attack to be ineffective in crashing the network, as shown in Fig. 5(a).

Lastly, we examine the cluster diameters of the Internet model under distributed attacks. We observe in Fig. 6(a) that the coordinated attack quickly extends the cluster diameter, and shortly after that, the network is totally crashed. The greedy sequential attack, though not quite effective in crashing the whole network, quickly makes the cluster diameter quite large and hence renders the network inefficient in supporting data communications. Another interesting observation is that, under the greedy sequential attack, even after the network has been largely crashed after 8% of network nodes are removed, the cluster diameter remains to be larger than 7, suggesting the existence of some sparsely-connected clusters (which are of small sizes but have large diameters). In the lower-bounded parallel attacks, as we can see from Fig. 6(b), the cluster diameter increases slowly at the beginning and then speeds up quickly. We also observe that, when we set the lower bound at 10, the cluster diameter remains a constant value of 12 after 19 steps of attacks. This large diameter belongs to a sparsely-connected 217-node cluster in which there is no node with a nodal degree higher than 10.

## IV. Conclusion

In this paper, we examined the robustness of communication networks under intentional attacks from a complex-network point of view. In addition to providing a brief survey of existing results, we considered different cases, in which the attacks are based on incomplete/inaccurate network-topology information and local information respectively. We found that incomplete information may degrade the efficiency of intentional attack significantly, especially if a big hub is missed. On the other hand, local-information based distributed attacks can be highly effective, sometimes almost as efficient as

an accurate global information-based attack. Such insights, as we believe, will be helpful for developing effective attacking/protecting strategies for future complex communication systems.

## REFERENCES


[1] S. Bornholdt, H. G. Schuster (Eds.), *Handbook of Graphs and Networks: From the Genome to the Internet*, Wiley-VCH, 2003.

[2] D. Achlioptas, A. Clauset, D. Kempe, and C. Moore, "On the bias of traceroute sampling," *Proc. ACM STOC'05*, Feb. 2005.

[3] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, pp. 378-382, July 2000.

[4] J. C. Doyle, *et al.*, "The 'robust yet fragile' nature of the Internet," *Proc. Nation. Acad. Science*, vol. 102, no. 41, pp. 14497-14502, Oct. 11, 2005.

[5] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On Power-Law Relationship of the Internet Topology," *Proc. of ACM SIGCOMM'99*, pp. 251-262, 1999.

[6] A. Beygelzimer, G. M. Grinstein, R. Linsker, and I. Rish, "Improving network robustness by edge modification," *Physica A*, vol. 357, no. 3-4, pp. 593-612, Apr. 2005.

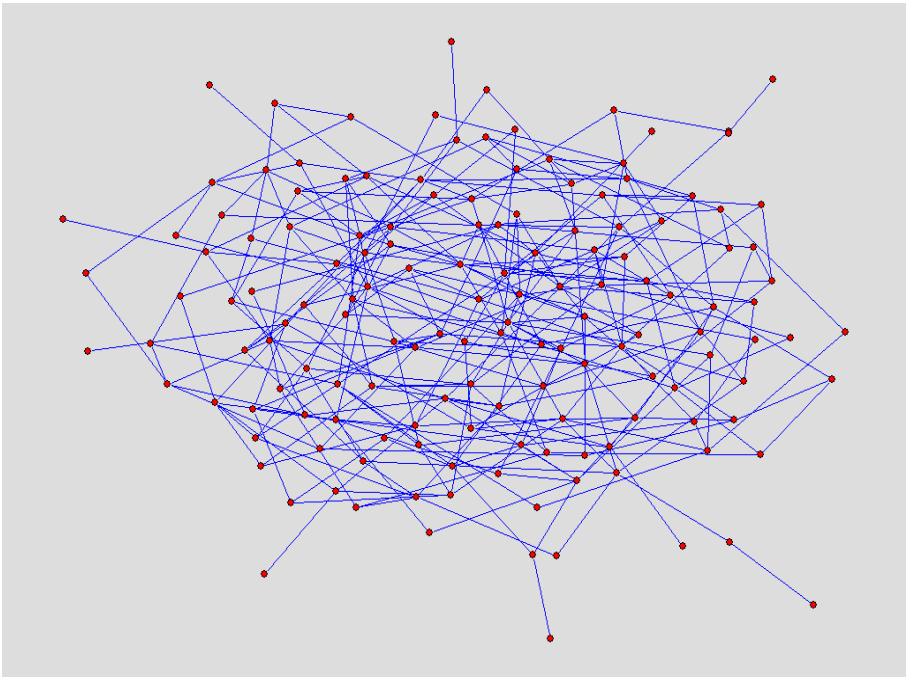
[7] S. Xiao, G. Xiao, and T. H. Cheng, "Robustness of Complex Communication Networks under Rewiring Operations," *Proc. IEEE ICCS 2006*, Oct. 2006.

[8] B. A. Rezaei, N. Sarshar, V. P. Roychowdhury, and P. O. Boykin, "Disaster management in scale-free networks: recovery from and protection against intentional attacks," http://arxiv.org/abs/cond-mat/0504185, Apr. 2005.

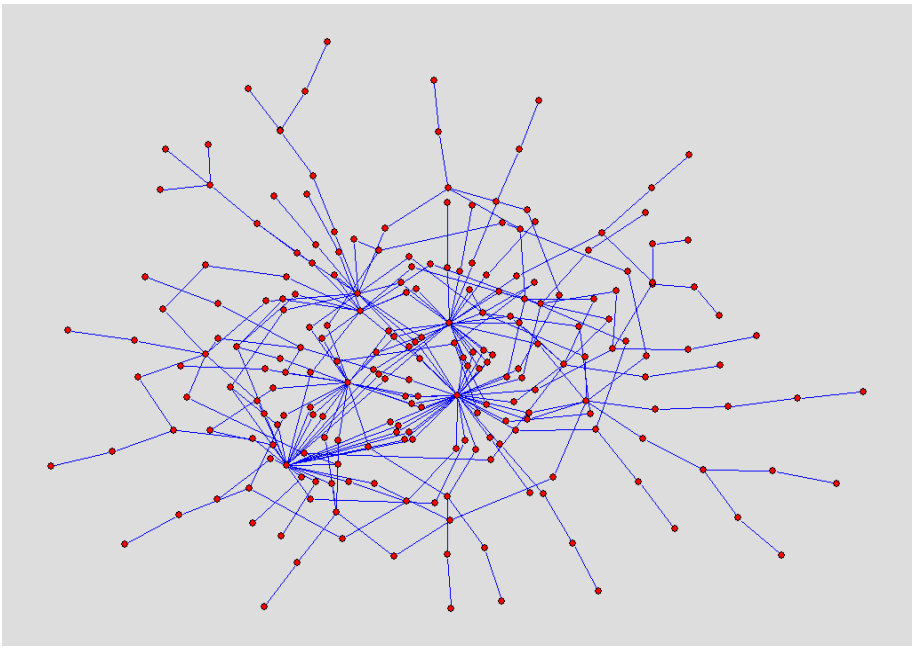
[9] L. Zhao, K. Park, and Y.-C. Lai, "Attack vulnerability of scale-free networks due to cascading breakdown," *Phy. Rev. E*, vol. 70, 035101, 2004.

[10] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, "Breakdown of the Internet under intentional attack," *Phy. Review Lett.*, vol. 86, no. 16, pp. 3682-3685, Apr. 2001.

[11] http://moat.nlanr.net/Routing/rawdata

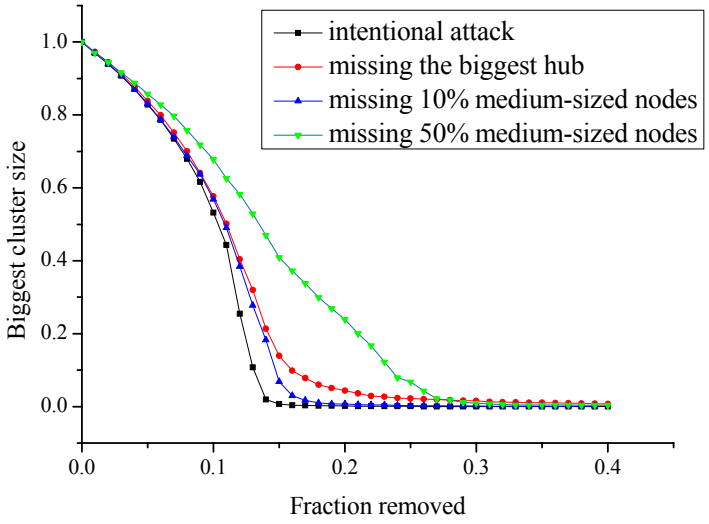


(a) A 200-node Erdős-Rényi random network.

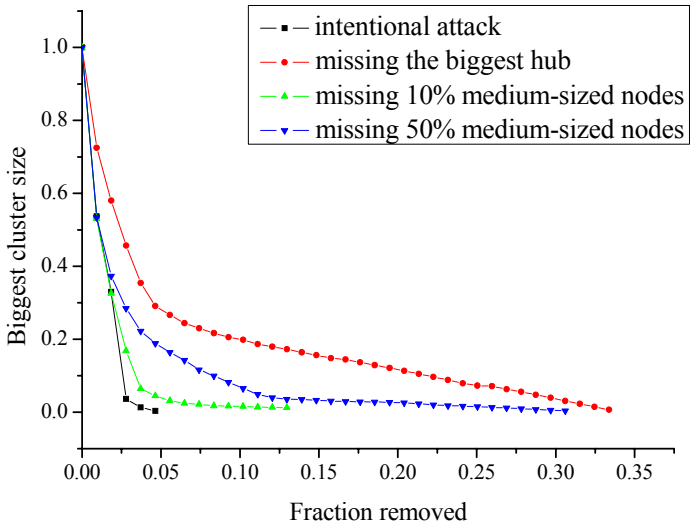


(b) A 200-node scale-free network.

Fig. 1. Examples showing the differences between a random network and a scale-free network.

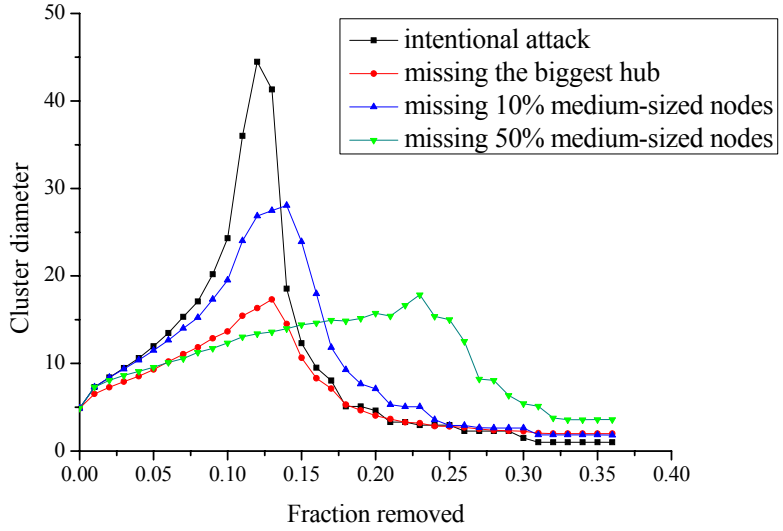



(a) BA model

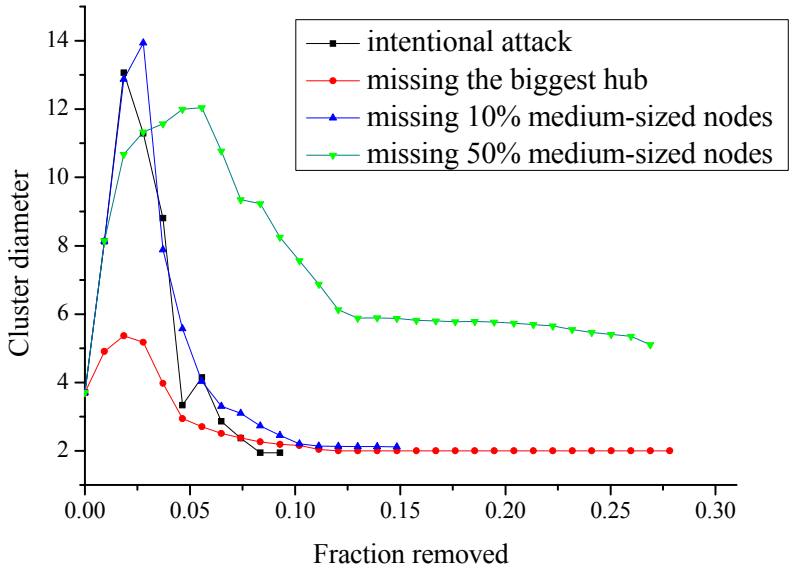



(b) 6470-node Internet model

Fig. 2. Robustness of the scale-free networks under intentional attacks that miss (i) the biggest hub, and (ii) 10% and 50% of medium-sized nodes, respectively.

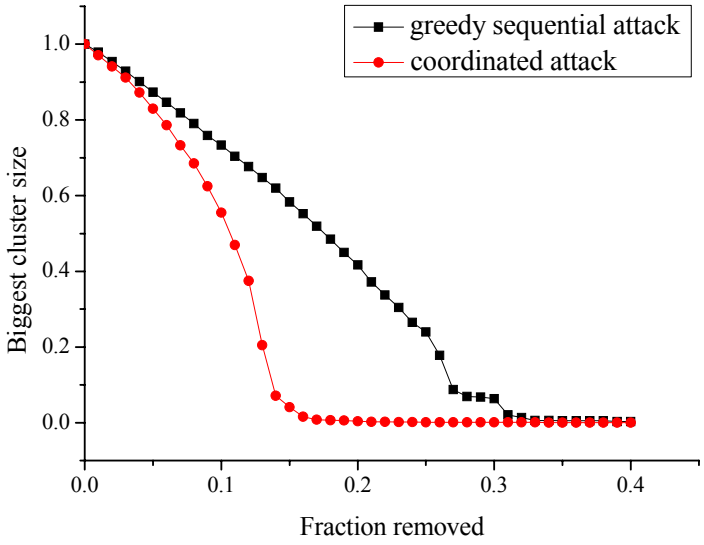



(a) BA model

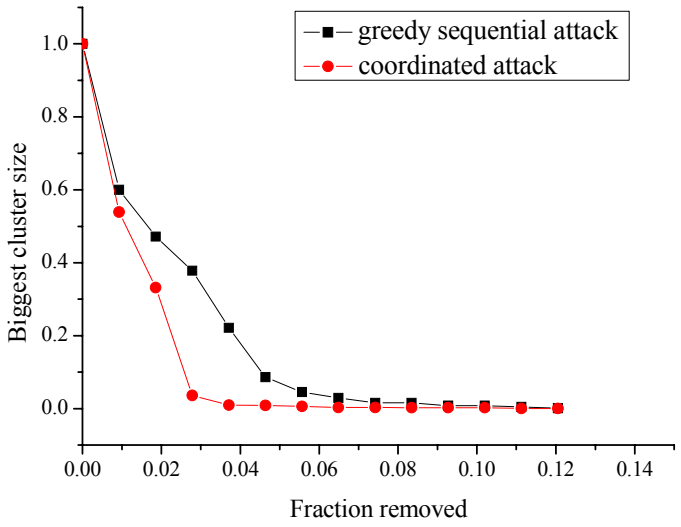



(b) 6470-node Internet model

Fig. 3. The cluster diameters of the scale-free network models under intentional attacks.

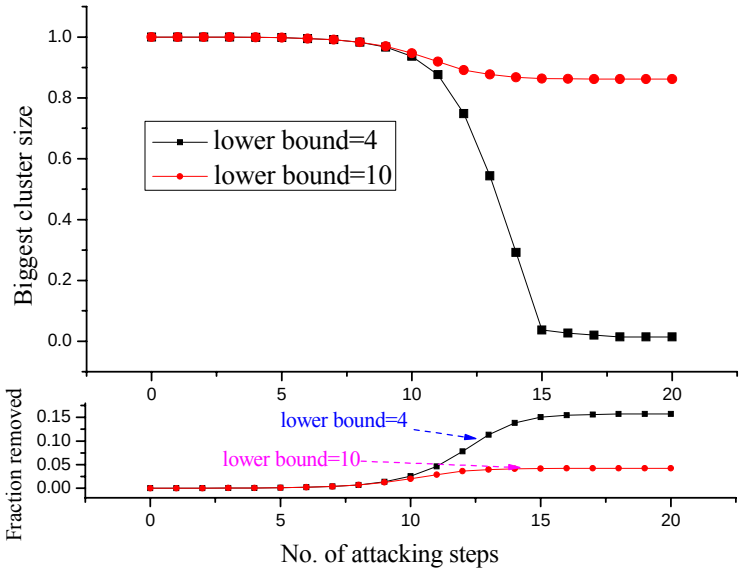



(a) BA model

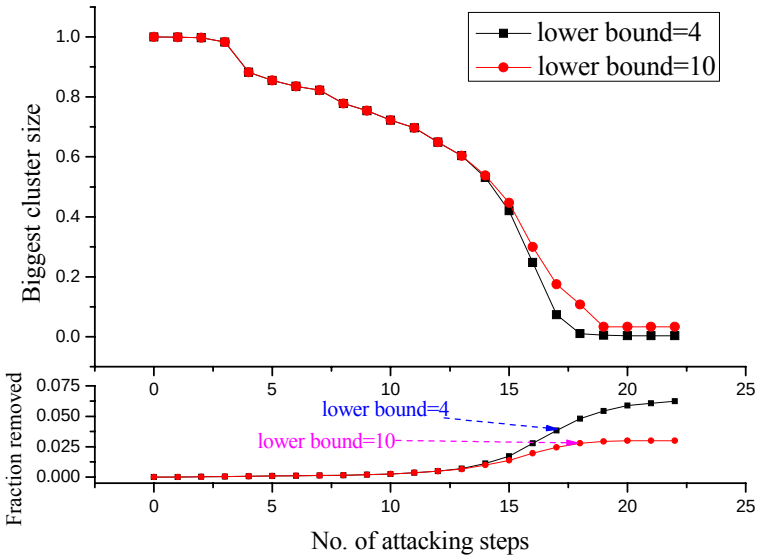



(b) 6470-node Internet model

Fig. 4. The efficiencies of the greedy sequential attack and the coordinated attack, respectively.

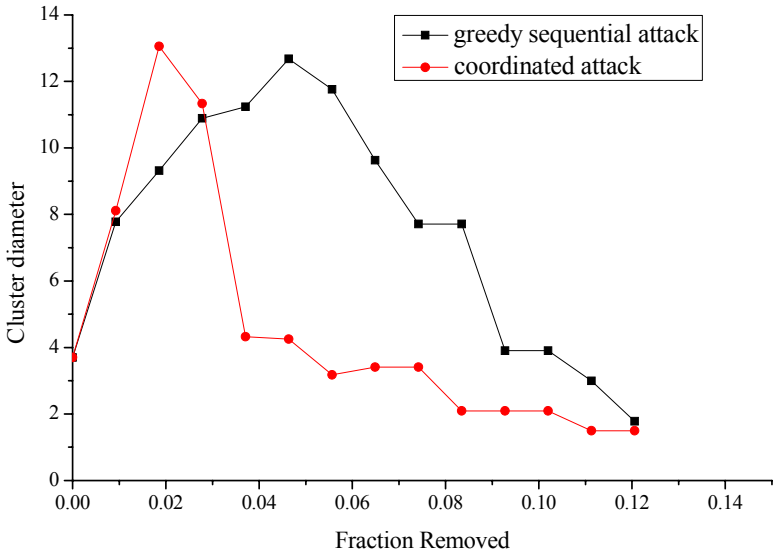



(a) BA model

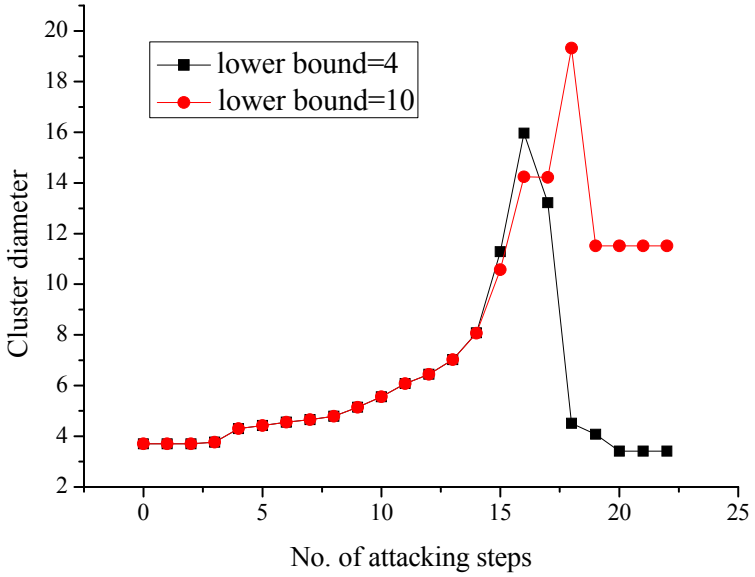



(b) 6470-node Internet model

Fig. 5. The efficiencies of the lower-bounded parallel attack with nodal-degree lower bounds set at 4 and 10, respectively.




(a) Greedy sequential attack and coordinated attack




(c) Lower-bounded parallel attack

Fig. 6. The cluster diameters of the 6470-node Internet model under different distributed attacks.