Tolerance of Local Information-Based Intentional Attacks in Complex Networks

Shi Xiao, Gaoxi Xiao, 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*—** We study the tolerance of complex networks against intentional attack which takes down network nodes in a decreasing order of their degrees. Specifically, we evaluate an effect which has been largely ignored in existing studies: in many real-life systems such as communication networks, attacks typically propagate throughout the networks from compromised nodes to their adjacent nodes, utilizing at most local network-topology information. By theoretical analysis and numerical simulations, we show that though different local information-based attacks have different performances, generally speaking they can be highly efficient. Such insight shall 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

Research on complex systems recently has been booming up. It is found that different systems, including the Internet, world-wide web (WWW), airline transportation systems, food web, protein-protein reactions, co-authorship, even terrorist activities, when formulated into network models, share some stunning common features. Such observations have spawned a new research area called *complex networks* [1-2].

One of the most important complex network models is the *scale-free network* [1-2]. In such networks, the fraction of nodes with a nodal degree k is proportional to $k^{-\alpha}$, where α is the exponent. In other words, the nodal degrees in such networks follow the *power-law* distribution. Different from the well-known Erdős-Rényi random graph [1], a visible feature of a scale-free network is the existence of a relatively large number of high-degree hub nodes.

Theory of complex networks sheds new light which helps better understand real-life systems. One of the most important results is that while a scale-free network is highly tolerant against random failures, it is fragile under *intentional attack* which takes down network nodes in a decreasing order of their degrees [3]. Such kind of attack, by removing hub nodes together with the large number of links connected to them, imposes a serious challenge to network survivability.

Extensive research efforts have been made to study the robustness of scale-free networks [3-12]. Theoretical analyses on the robustness of scale-free networks under random failures and intentional attack were developed in [4] and [5], respectively. The applicable ranges of these theories were studied in detail in [6]. It is shown in [7] that, for either random failure or intentional attack, there exists a phase transition in the fraction of node loss, below which the network basically continues to function well. Gallos *et al.* evaluated the case where the probability that a node is removed by hostile attack is a function of its own degree [8]. To enhance network robustness against intentional attack, the proposed methods include link insertion [9-10], link rewiring [11] and link recovery [12], etc.

In this paper, we evaluate network robustness against hostile attack by considering an effect which has been largely ignored in existing studies: In many real-life systems such as communication networks, hostile attacks typically have to "propagate" throughout the network, taking down those nodes adjacent to the already compromised nodes. Since such attacks typically use at most the local network-topology information, we term them *distributed attacks*. Theoretical analysis and numerical simulations show that though different distributed attacks perform differently in different networks, overall speaking they can be highly efficient. In some cases, they are almost as damaging as the global information-based intentional attack. Effective methods have to be designed to protect systems against such attacks.

The rest of this paper is organized as follows. In Section II, A few distributed attack schemes are proposed. Theoretical analysis and simulation results for evaluating these schemes on *random* scale-free networks (to be defined later) are proposed in Sections III and IV, respectively. Numerical evaluations on a few real-life network models are presented in Section V. Finally Section VI concludes the paper.

II. DISTRIBUTED ATTACK SCHEMES

We define a node that has already been taken down as a *crashed* node; and otherwise a *live* node. As mentioned earlier, distributed attacks basically target on some or all of the live nodes adjacent to

the crashed nodes in each step; and the selections of the targets depend on only the local network-topology information.

We study a few different distributed attack schemes as follows:

- **Greedy sequential attack:** the largest-degree node adjacent to the node crashed in the *last* step is selected as the next-step target. If no adjacent node exists, a live node is randomly selected as the target.
- **Coordinated attack:** the largest-degree live node adjacent to any crashed node is selected as the next-step target. If no adjacent node exists at all, a live node is randomly selected as the target.
- **Lower-bounded parallel attack:** instead of taking down only a single node in each step, the attack starts from *every* crashed node to randomly take down one of its adjacent live nodes as long as the live node's degree is no less than a certain threshold. If no such adjacent node exists, the attack stops.
- **Lower-bounded flooding attack:** the attack starts from every crashed node to take down *all* the adjacent live nodes as long as the live node's degree is no less than a certain threshold. If no such adjacent node exists, the attack stops.

The proposed four schemes may not easily happen in real-life systems. However, they provide some useful benchmarks for estimating the performances of other cases. Specifically, the first two schemes are for evaluating distributed attacks which take down only one node in each step. While the first one is greedy yet memoryless (meaning that the attack always start from the last node it has crashed), the second one with more sophisticated coordination is probably among the worst of this class of attacks. The third and fourth schemes, on the other hand, take down multiple nodes in each step: the third one takes down at most one node starting from each crashed node, while the fourth one adopts brutal force to crash more. Note that the cases without a lower bound of nodal degree can be viewed as the special case where the lower bound value equals to the lowest nodal-degree of the network.

The effects of these distributed attack schemes in the random scale-free networks will be analyzed in the next section.

III. THEORETICAL ANALYSIS

The random networks are defined as networks with random connections between their nodes, subject to the given nodal-degree distribution [13]. It is well known that a random network loses its global connectivity when [4]

$$\kappa \equiv \frac{\langle k^2 \rangle}{\langle k \rangle} < 2, \tag{1}$$

where $\langle k \rangle$ denotes the average nodal degree, and $\langle k^2 \rangle$ the average of nodal-degree squares. Under random node failures, the *crash threshold*, which is defined as the fraction of nodes to be removed for the network to lose its global connectivity, is given as **[**4**]**:

$$1 - p_c = \frac{1}{\kappa_0 - 1}. \tag{2}$$

Here $\kappa_0 = \langle k_0^2 \rangle / \langle k_0 \rangle$ where $\langle k_0 \rangle$ and $\langle k_0^2 \rangle$ denote the average nodal degree and average nodal-degree square in the original network respectively.

For analyzing the robustness of random networks under intentional attack, an approximate solution was proposed in [5]. Specifically, denote the original cutoff in the network as *K* and the new cutoff after the intention attack as $\tilde{K}$, the fraction of removed nodes as *p,* and the corresponding link loss probability as $\tilde{p}$. We have

$$\begin{cases} p = \sum_{\tilde{K}}^{K} p(k) = \dfrac{K^{1-\alpha} - \tilde{K}^{1-\alpha}}{K^{1-\alpha} - m^{1-\alpha}} \\ \tilde{p} = \sum_{\tilde{K}}^{K} \dfrac{kp(k)}{\langle k \rangle} = \dfrac{K^{2-\alpha} - \tilde{K}^{2-\alpha}}{K^{2-\alpha} - m^{2-\alpha}} \end{cases}. \tag{3}$$

For such a case, κ becomes

$$\kappa = \frac{\langle k^2 \rangle}{\langle k \rangle} = \left(\frac{2-\alpha}{3-\alpha} \right) \frac{\tilde{K}^{3-\alpha} - m^{3-\alpha}}{\tilde{K}^{2-\alpha} - m^{2-\alpha}}, \tag{4}$$

where *m* denotes the minimum nodal degree in the network. The new cutoff $\tilde{K}$ can be calculated and the corresponding *p*, which is the crash threshold, can then be obtained by numerically solving the equation

$$1-\widetilde{p}=\frac{1}{\kappa-1}. \tag{5}$$

.

We now proceed to analyze the four distributed attacks separately.

Greedy Sequential Attack

In a random scale-free network, high-degree nodes are generally connected into a dense sub-network. Starting from any node in the network, a greedy sequential attack can reach a highest-degree node in at most a few steps, and starting from there reaches most or all the other hub nodes. When virtually all the hubs have been crashed, the efficiency of each step of the attack drops drastically to be approximately equivalent to that of a random failure. Therefore the greedy sequential attack can be approximately viewed as composed of two different stages: i) an intentional attack that takes down all the hubs; and ii) a random failure of nodes in the remaining network.

Assume that in the first stage the hub nodes with degrees no less than a certain threshold value K_T are all removed. Denote the corresponding fraction of crashed nodes and link loss probability in this stage as p_i and $\widetilde{p}_i$, respectively. We have

$$\begin{cases} p_i=\sum_{K_T}^{K}p(k)=\dfrac{K^{1-\alpha}-{K_T}^{1-\alpha}}{K^{1-\alpha}-m^{1-\alpha}} \\ \tilde{p}_i=\sum_{K_T}^{K}\dfrac{kp(k)}{\langle k\rangle}=\dfrac{K^{2-\alpha}-{K_T}^{2-\alpha}}{K^{2-\alpha}-m^{2-\alpha}} \end{cases}. \tag{6}$$

The ratio of average nodal degree versus the average square of nodal degree after the first stage therefore becomes

$$\kappa'=\left(\frac{2-\alpha}{3-\alpha}\right)\frac{{K_T}^{3-\alpha}-m^{3-\alpha}}{{K_T}^{2-\alpha}-m^{2-\alpha}}, \tag{7}$$

Assume that in the second stage a fraction p_r of nodes is crashed before the network loses its global connectivity. The nodal degree distribution after the second-stage attack is

$$\widetilde{p}(k)=\sum_{k_0=k}^{K_T}p(k_0)\binom{k_0}{k}(1-(p_r+\widetilde{p}_i))^k(p_r+\widetilde{p}_i)^{k_0-k}. \tag{8}$$

In random networks, from Eq. (2) we have

$$\begin{cases} 1-(p_r+\tilde{p}_i)=\dfrac{1}{\kappa'-1} \\ p_r=\dfrac{\kappa'-2}{\kappa'-1}-\tilde{p}_i \end{cases}. \tag{9}$$

The crash threshold of the original network is $p_r + p_i$.

Achieving a good estimation of the threshold value K_T may not be easy in some networks. It shall be the value where the remaining network resembles a random network. In our experience it is a good practice to set K_T as $2\times\langle k_0\rangle$ in random scale-free networks with exponent values between 2 to 3.

Coordinated Attack

Coordinated attack can be almost as efficient as the global information-based intentional attack. Specifically, assume that the network is crashed by the intentional attack when the cutoff degree is reduced to K_c. If the network nodes with degrees no less than K_c (i.e., the set of nodes to be removed by the intentional attack in order to crash a network) form into a single connected component, once the coordinated attack reaches any node of this component, it thereafter becomes equivalent to the intentional attack; otherwise, the efficiency of the coordinated attack is slightly lower. By figuring out the number of disconnected components in the sub-network composed by those nodes with degrees no less than K_c, we can get a good estimation of the *difference* between the efficiencies of coordinated attack and intentional attack.

Direct calculation of the number of disconnected components in a network however remains as a challenging problem. In this paper, we calculate a *lower bound* of this number instead. Specifically, as we can see, the subnet composed by those nodes with degrees no less than K_c in the original network still form into a random network, though the nodal-degree distribution is no longer scale-free. In this subnet, nodes with degree 0 are apparently isolated. Nodes with degree 1, if it is connected to another node also with degree 1, these two nodes form into an isolated component. The sum of the numbers of these two types of isolated components safely serves as a lower bound of the number of disconnected components in the subnet. Below we derive the equations for calculating this lower bound.

Denote the fraction of nodes with degrees no less than K_c as p_c and the corresponding portion of links connected to these nodes as $\tilde{p}$. Both of these two parameters can be calculated using Eq. (3),

with $\widetilde{K}$ being replaced by K_c.

For a node with degree k ($k \geq K_c$) in the original network, the probability that it has a degree 0 in the subnet equals to the probability that all of its links connected to the nodes with degrees lower than K_c in the original network, which is $(1-\tilde{p})^k$; the probability that it has a degree 1 in the sub-network is the probability that it has exactly one link connected to another node with degree no less than K_c, which equals to $k \cdot \tilde{p} \cdot (1-\tilde{p})^{k-1}$. Therefore the fraction of nodes in the sub-network with degree 0 and degree 1 can be expressed as:

$$\begin{cases} p_0 = \dfrac{\sum\limits_{k \geq K_c} p(k)(1-\tilde{p})^k}{\sum\limits_{k \geq K_c} p(k)} \\ p_1 = \dfrac{\sum\limits_{k \geq K_c} p(k) \cdot k \cdot \tilde{p} \cdot (1-\tilde{p})^{k-1}}{\sum\limits_{k \geq K_c} p(k)} \end{cases}. \tag{10}$$

The probability that a degree-1 node in the subnet is connected to another degree-1 node, denoted as q_1, is $p_1 / \langle k' \rangle$, where $\langle k' \rangle$ is the average degree in the subnet, i.e., $\langle k' \rangle = \dfrac{\langle k_0 \rangle \cdot \tilde{p} \cdot \tilde{p}}{p_c}$. Hence

$$q_1 = \frac{p_c \cdot p_1}{\langle k_0 \rangle \cdot \tilde{p} \cdot \tilde{p}}. \tag{11}$$

The lower bound of the difference between the crash thresholds of intentional attack and coordinated attack is $p_0 + \dfrac{p_1 \cdot q_1}{2}$. Though the lower bound may not appear to be very tight, as we can see later in Sec. IV, it is actually good enough for most cases. The lower bound of the crash threshold of the coordinated attack is

$$p_{ca} = p_c(1 + p_0 + \frac{p_1 \cdot q_1}{2}). \tag{12}$$

Lower-Bounded Parallel Attack

For the cases with multiple nodes being crashed in each step, since generally a scale-free network loses its global connectivity in just a few steps and then virtually all its nodes, instead of analyzing the

crash threshold, we study the steps needed to crash all the nodes in the networks. Arguably such analysis may be more meaningful for estimating the network robustness and the time for reaction while under attack.

In the lower-bounded parallel attack, starting from each crashed node the largest-degree adjacent live node is crashed if that node's degree is no less than a preset threshold. Denote the threshold value as *T*. In an *N*-node network, denote the total number of nodes with original degrees no less than *T* as N',

$$N' = N \cdot \sum_{k=T}^{K} p(k) = N \cdot \frac{K^{1-\alpha} - T^{1-\alpha}}{K^{1-\alpha} - m^{1-\alpha}}. \tag{13}$$

The probability that a crashed node has an original degree *k* is

$$p'(k) = \frac{p(k)}{\sum_{k \geq T} p(k)} \qquad (k \geq T). \tag{14}$$

Denote the probability that a link leading to a node with degree no less than *T* as p'. We have

$$p' = \sum_{k=T}^{K} \frac{kp(k)}{\langle k \rangle} = \frac{K^{2-\alpha} - T^{2-\alpha}}{K^{2-\alpha} - m^{2-\alpha}}. \tag{15}$$

Assume a just-crashed node with degree k $(k \geq T)$ has an average of n'_k live adjacent nodes with degree no less than *T,* We have

$$n'_k = k \times p' - 1 \qquad (k \geq T). \tag{16}$$

Denote the number of crashed nodes after *l* steps as a_l. We derive the relationship between a_l and a_{l-1} as follows. Let $a_1 = 1$. If in a certain step *l*, starting from every crashed node a live adjacent node is further crashed, then $a_l = 2a_{l-1}$. Now we take into account the probability that all nodes adjacent to a crashed node and with degrees no less than *T* have been crashed. While accurate analysis of this probability is rather complicated, an approximate model can be easily derived: for a crashed node with degree *k*, averagely all its adjacent live nodes with degrees no less than *T* will be crashed in the next n'_T steps. In other words, if a degree-*k* node was crashed in step $l - n'_k$, averagely it has no live adjacent node to be crashed in step *l*. Since the probability that a degree-*k* node is crashed in step $l - n'_k$ equals to $p'(k) \cdot a_{l-1-n'_k}$ and the lowest degree of the nodes to be crashed is *T*, we have

$$a_l = \begin{cases} 1 & l = 1 \\ 2a_{l-1} & 2 \le l \le n'_T \\ 2a_{l-1} - \sum_{k \ge T} p'(k) \times a_{l-1-n'_k} & n'_T < l \end{cases} \tag{17}$$

From Eqs. (13) - (17), we can calculate the number of steps needed to remove all the nodes with degrees no less than *T*. Note that Eq. (17) is an approximate calculation since it utilizes average value rather than detailed nodal-degree distribution. As we will see later in Section IV, however, the accuracy turns out to be satisfactory.

Lower-Bounded Flooding Attack

In the lower-bounded flooding attack, starting from a crashed node all its live adjacent nodes will be crashed as long as their degrees are no less than a certain threshold value *T*. Denote the average degree of those nodes with degrees no less than *T* as K''

$$K'' = \frac{\sum_{k=T}^{K} kp(k)}{\sum_{k=T}^{K} p(k)} = \langle k \rangle \times \frac{\left(K^{2-\alpha} - T^{2-\alpha}\right)\left(K^{1-\alpha} - m^{1-\alpha}\right)}{\left(K^{2-\alpha} - m^{2-\alpha}\right)\left(K^{1-\alpha} - T^{1-\alpha}\right)}. \tag{18}$$

Starting from each crashed node an average of n'' nodes can be crashed in the next step,

$$n'' = K'' \cdot p' - 1 = \langle k \rangle \cdot \frac{\left(K^{2-\alpha} - T^{2-\alpha}\right)^2 \left(K^{1-\alpha} - m^{1-\alpha}\right)}{\left(K^{2-\alpha} - m^{2-\alpha}\right)^2 \left(K^{1-\alpha} - T^{1-\alpha}\right)} - 1, \tag{19}$$

where p' denotes the probability that a link leads to a node with a degree no less than *T*, which can be calculated from Eq. (15).

Assumed that in the first step, only a single node is crashed, and after l'' steps, all the N' nodes as defined in Eq. (13) are taken down. Approximately we have

$$(n'')^{l''-1} \approx N'. \tag{20}$$

Hence,

$$l'' = \log_{n''}^{N'} + 1, \tag{21}$$

which further yields

$$l'' = \frac{\log\left(N \times \frac{K^{1-\alpha} - T^{1-\alpha}}{K^{1-\alpha} - m^{1-\alpha}} \right)}{\log\left[\langle k \rangle \times \frac{\left(K^{2-\alpha} - T^{2-\alpha}\right)^2 \left(K^{1-\alpha} - m^{1-\alpha}\right)}{\left(K^{2-\alpha} - m^{2-\alpha}\right)^2 \left(K^{1-\alpha} - T^{1-\alpha}\right)} - 1 \right]} + 1. \quad (22)$$

IV. Simulation Results and Discussion

In our simulations, random scale-free networks are generated by adopting the algorithm proposed in [14], with α varying from 2 to 3. Unless otherwise specified, the network size N is 10,000; the minimal nodal degree m is 2 and the cutoff degree K is 100, which equals to $\sqrt{N}$. For the lower-bounded parallel attack and lower-bounded flooding attack schemes, we consider the cases where the lower bound T equals to 4 and 10 respectively. The case with no lower bound is also simulated for comparison purpose. We adopt the definition in [4] that a network is crashed once $\langle k^2 \rangle / \langle k \rangle \le 2$ is achieved. Unless otherwise specified, the presented simulation results come from an average of 50 independent realizations.

In Fig. 1, we compare the analytical and simulation results of crash thresholds for the greedy sequential attack and coordinated attack, respectively. For comparison, the results for the case of classic intentional attack are also presented. In the analysis, the threshold degree K_T for the greedy sequential attack is set as $2 \cdot \langle k_0 \rangle$. Analytical and simulation results basically match well, and the lower bound of the crash threshold for coordinated attack turns out to be reasonably tight. For the efficiency of the two types of attacks, we observe that the greedy sequential attack is not very effective in crashing networks. The networks are only crashed after around half of all the nodes are removed. The coordinated attack, on the other hand, performs nearly as efficient as the intentional attack, especially when α is of small values. 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.

Table 1 lists the number of steps needed for the lower-bounded parallel attack to crash all the nodes with degrees no less than the lower bound. The analytical and simulation results achieve a reasonable match. We see that the lower-bounded parallel attack is very efficient in not only crashing but eliminating a large network as long as the lower bound T is small enough. Note that since we set the same minimum and cutoff nodal degrees for all the networks, the link density is higher when α is

of a smaller value, which allows the parallel attack to become even more efficient.

Table 1. Analytical and simulation results of the numbers of steps needed to remove all the nodes with high-enough degrees in different networks by the lower-bounded parallel attack

	$T = 2$		$T = 4$		$\mathbf{T} = 10$	
	Analytical result	Simulation result	Analytical result	Simulation result	Analytical result	Simulation result
$\alpha = 2.1$	17	18	15	16	12	13
$\alpha = 2.3$	18	18	15	16	12	13
$\alpha = 2.5$	18	19	17	17	12	13
$\alpha = 2.7$	19	19	17	17	13	14
$\alpha = 2.9$	20	20	18	18	14	15

The results of lower-bounded flooding attack are presented in Table 2. The analytical and simulation results match quite well. Comparing Table 1 and Table 2, we see that compared to that of the lower-bounded parallel attack, the lower-bound flooding attack, by removing more nodes in each step, gives the defending side a much shorter time to react.

Table 2. Comparison of the analytical and simulation results of the numbers of steps needed to remove all the candidate nodes in different networks by the lower-bounded flooding attack

	$T = 2$		$T = 4$		$T = 10$	
	Analytical result	Simulation result	Analytical result	Simulation result	Analytical result	Simulation result
$\alpha = 2.1$	7	7	5	5	4	5
$\alpha = 2.3$	7	7	6	6	5	6
$\alpha = 2.5$	8	8	6	6	5	6
$\alpha = 2.7$	9	9	7	7	6	7
$\alpha = 2.9$	10	10	8	8	7	7

In Fig. 2, the procedures of the two attacks are plotted with further details for the case where $\alpha = 2.5$. We show in each step of attack the *largest cluster size*, defined as the number of nodes in the biggest connected component versus the number of nodes in the original network [3]. An interesting observation we can make in Fig. 2(a) is that for the lower-bounded parallel attack, the largest cluster size is smaller when the lower bound is higher until the attack stops. This can be easily explained: since in each step a live adjacent node with degree no less than the lower bound is randomly selected as the next-step target, a higher lower bound makes the high-degree nodes to be crashed faster, which reduces the largest cluster size. In the lower-bounded flooding attack, however, the situation is totally reversed: a lower value of *T* makes more nodes crashed in each step and consequently a smaller largest cluster size, as we observe in Fig. 2(b).

Another interesting observation is when the threshold is set at a relatively high value of 10, the attack is terminated when $\langle k^2 \rangle / \langle k \rangle$ is still much higher than 2 and the network is still largely connected, as can be seen in Fig. 2(a).

V. SIMULATIONS ON REAL-LIFE NETWORK MODELS

To evaluate the effects of the proposed distributed attack schemes in real-life networks, we carry out simulations on two different models as follows:

- A real-world Internet model on the AS-level as measured by the Applied Network Research (NLANR) Project on January 2, 2000 [15], which contains 6470 inter-connected nodes and 12,566 links. We have verified that it is indeed a scale-free network.
- A real-world Internet model on the Router-level as measured by the Cooperative Association for Internet Data Analysis (CAIDA), which contains 192,244 nodes and 609,066 links [16].

As in most existing studies [3-6], we evaluate the robustness of a network by measuring its (i) largest cluster size; and (ii) cluster diameter, defined as the average length of the shortest paths between all the node pairs in the largest cluster.

The earlier definition of crash threshold p_c where $\langle k^2 \rangle / \langle k \rangle \le 2$ does not apply to these two networks since neither of them is a random network. To differentiate, we evaluate the *threshold of crash* (TOC), defined as the percentage of network nodes that has to be removed to reduce the largest cluster size to be no more than 5%.

The presented simulation results for the AS-level model come from an average of 100 independent realizations. For the router-level model, due to its extra-large size, it is prohibitively time-consuming to carry out extensive realizations. Therefore only 10 realizations have been conducted.

Fig. 3 shows the largest cluster sizes under greedy sequential and coordinated attack, respectively. For comparison purpose, results under the intentional attack are also presented. We observe that though the two Internet models are not random networks, they confirm the conclusion that the greedy sequential attack is not quite efficient in crashing scale-free networks, whereas the coordinated attack, though based on local information only, performs nearly as efficient as intentional attack.

For the two lower-bounded attack schemes, we set up the lower-bound degree of the crashed nodes at 1, 4 and 10 respectively. The simulation results of lower-bounded parallel attack are reported in Fig. 4. For the AS-level model, the attack is highly efficient when the lower bound is 10. In fact, the TOC value is only slightly increased from 3.2% of the intentional attack to 4%. If we set the lower bound at 4, more nodes have to be removed before the network is crashed: the TOC becomes 9.6%. With no lower bound (or equivalently by setting the lower bound at 1), 25.3% of all the nodes have been removed when the network is finally crashed. The conclusion remains the same as that in the random scale-free networks; i.e., higher lower-bound values make the largest cluster size decrease faster. In the router-level model, setting the lower bound at 10 makes the distributed attack almost as efficient as the intentional attack -- the TOC only increased slightly from 13.6% to 13.84%. The efficiency drops when the lower bound gets lower.

The above observations show that in real-life complex networks where high-degree nodes largely form a *connected* sub-network, taking down these nodes does not need global information of network topology; local information-based attacks can be almost equally effective. To prevent a complex system from being crashed by such highly effective distributed attacks, it is crucial to identify and stop the attack at an early stage: as we can see, the networks' decomposition is slow at the first several steps and then quickly speeds up.

Fig. 5 shows the largest cluster sizes under the lower-bounded flooding attack. In both of the two Internet models, the attack quickly eliminates a large portion of the network in just a few steps. Different lower bound values lead to only slight differences and the reaction time is very short.

Lastly we present the results of cluster diameters under attack. Since it is extremely

time-consuming to carry out even a moderate number of realizations of diameter calculations in the router-level model in order to achieve an acceptable error range, we present only the results for the AS-level model. As can be observed in Fig. 6(a), the coordinated attack quickly increases the cluster diameter; and shortly after that, the network is totally crashed. The greedy sequential attack, though not quite efficient in crashing the whole network, also quickly increases the cluster diameter, showing that it may nevertheless make the networks to be inefficient in supporting some applications, e.g., data communications.

For the lower-bounded parallel attacks, as can be seen from Fig. 6(b), the cluster diameter increases slowly at the beginning and then speeds up quickly. Note that when we set the lower bound at 10, the cluster diameter remains at a constant value, averaged about 6.65, after 12 steps of attacks. This large diameter belongs to a sparsely-connected cluster with an average size of 62 nodes, in which there is no node with a degree higher than 10. The error bar for such a case is smaller than the symbol size.

VI. Conclusion

In this paper, we examined the robustness of complex networks under a few different types of distributed attacks. Analytical and extensive simulation results showed that such local information-based distributed attacks can be highly effective, sometimes almost as efficient as the global information-based intentional attack, and they typically leave rather limited time for reaction. Such insights, as we believe, will be helpful for developing effective attacking/protecting strategies for future complex systems.

One possible extension of this work will be to evaluate the efficiency of distributed attacks in correlated scale-free networks. It is known that different nodal-degree correlations lead to different network robustness levels though the crash threshold of any scale-free network remains low [17-20]. It would be interesting to find out whether different correlations make significant difference to network robustness under distributed attack.

References

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

[2] Ben-Naim E and Frauenfelder H 2004 *Complex Networks,* ed Z Toroczkai (Berlin, Heidelberg: Springer-Verlag)

[3] Albert R, Jeong H and Barabási A -L 2000 Error and attack tolerance of complex networks *Nature* **406** 378-82

[4] Cohen R, Erez K, ben-Avraham D and Havlin S 2000 Resilience of the Internet to random breakdown *Phy. Review Lett.* **85** 4626

[5] Cohen R, Erez K, ben-Avraham D and Havlin S 2001 Breakdown of the Internet under intentional attack *Phy. Review Lett.* **86** 3682

[6] Paul G, Sreenivasan S and Stanley H E 2005 Resilience of complex networks to random breakdown *Phy. Rev. E* **72** 056130

[7] López E, Parshani R, Cohen R, Carmi S and Havlin S 2007 Limited path percolation in complex networks *Phys. Rev. Lett.* **99** 188701

[8] Gallos L K, Cohen R, Argyrakis P, Bunde A and Havlin S 2005 Stability and topology of scale-free networks under attack and defense strategies *Phys. Rev. Lett.* **94** 188701

[9] Beygelzimer A, Grinstein G M, Linsker R and Rish I 2005 Improving network robustness by edge modification *Physica A* **357** 593-612

[10] Zhao J and Xu K 2009 Enhancing the robustness of scale-free networks *J. Phys. A*: *Math. Theor.* **42** 195003

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

[12] Rezaei B A, Sarshar N, Boykin P O and Roychowdhury V P 2007 Disaster management in power-law networks: recovery from and protection against intentional attacks *Physical A* **381** 497-514

[13] Erdös P and Rényi A 1959 On random graphs I *Publ. Math. Debrecen* **6** 290-7.

[14] Catanzaro M, Boguñá M and Pastor-Satorras R 2005 Generation of uncorrelated random scale-free networks *Phy. Review E* **71** 027103

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

[16] http://www.caida.org/tools/measurement/skitter/router_topology/

[17] Newman M E J 2002 Assortative mixing in networks *Phys. Rev. Lett.* **89** 208701

[18] Holme P and Zhao J 2007 Exploring the assortativity-clustering space of a network's degree sequence *Phy. Review E* **75** 046111

[19] Weber S and Porto M 2007 Generation of arbitrarily two-point-correlated random networks *Phy. Review E* **76** 046111

[20] Xiao S, Xiao G, Cheng T H, Ma S, Fu X and Soh H Robustness of Complex Communication Networks under Rewiring Operations *Europhysics Lett.*, in press.

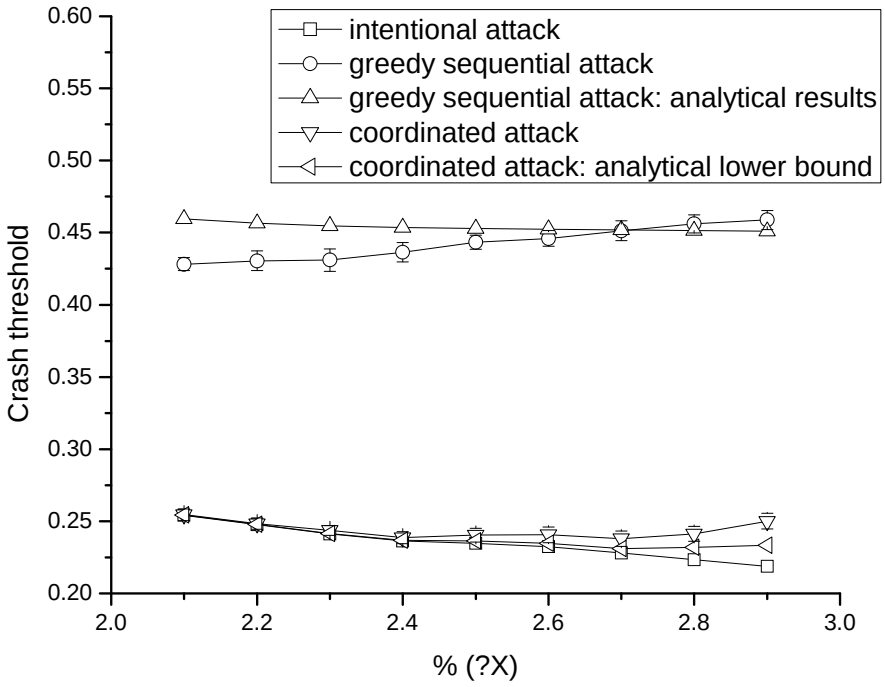
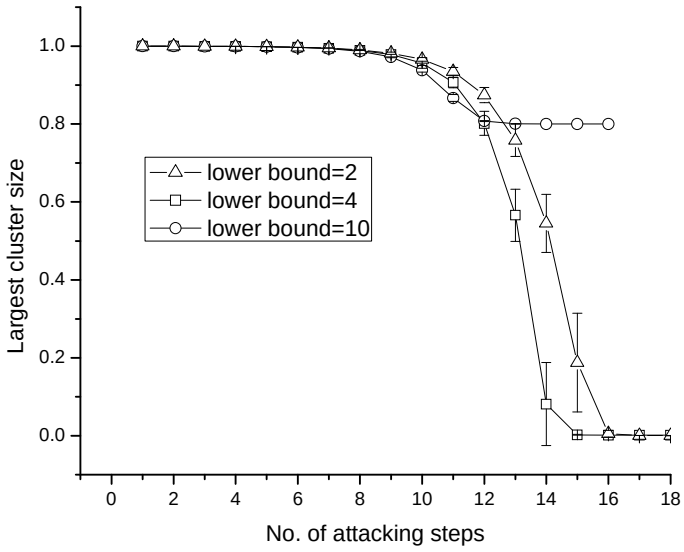
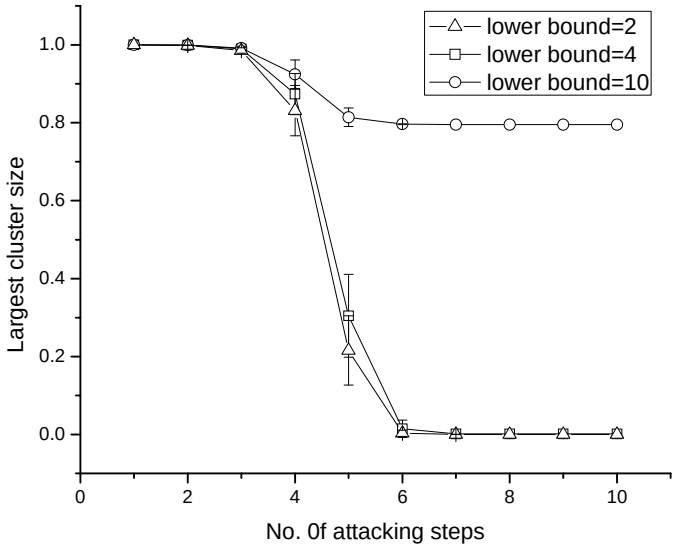


Fig. 1. The crash thresholds of the greedy sequential attack and coordinated attack in random scale-free networks.

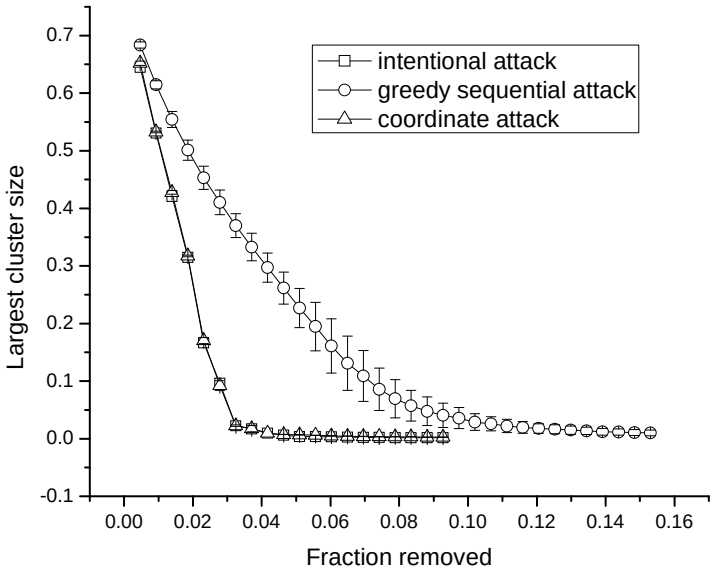


(a) lower-bounded parallel attack

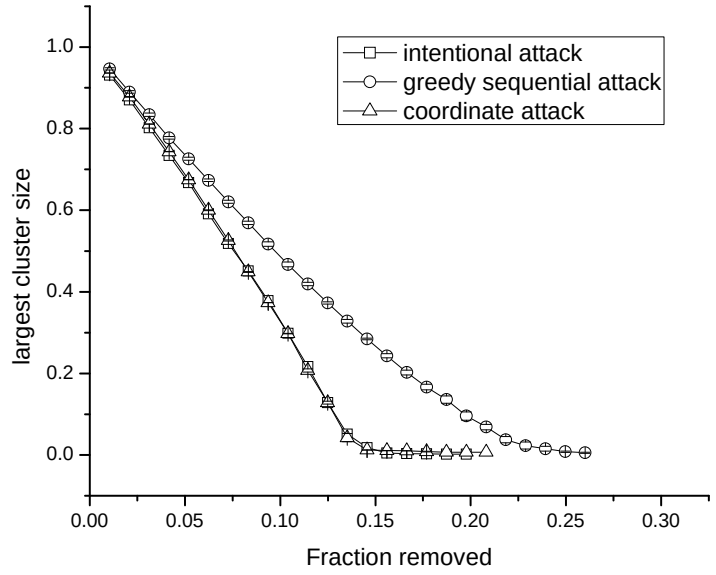


(b) lower-bounded flooding attack

Fig. 2. The efficiencies of the lower-bounded parallel attack and flooding attack for random scale-free network ($\alpha = 2.5$) with nodal-degree lower bounds set at 4 and 10 and without lower bound (or equivalently with lower bound at 2), respectively.

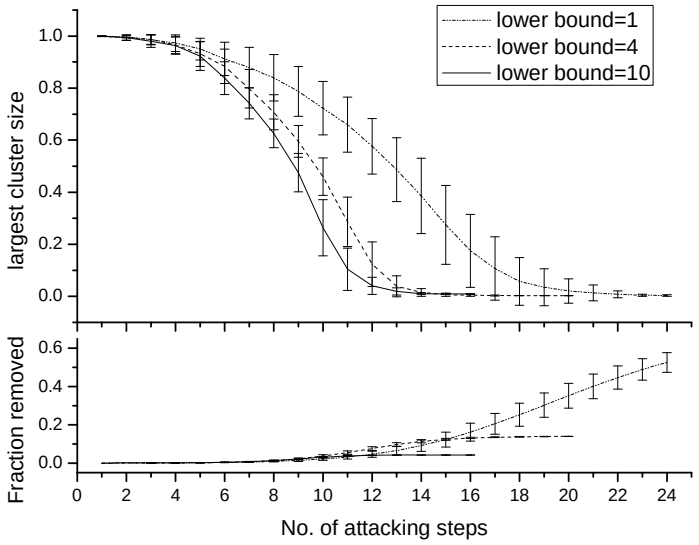


(a) Internet AS-level model

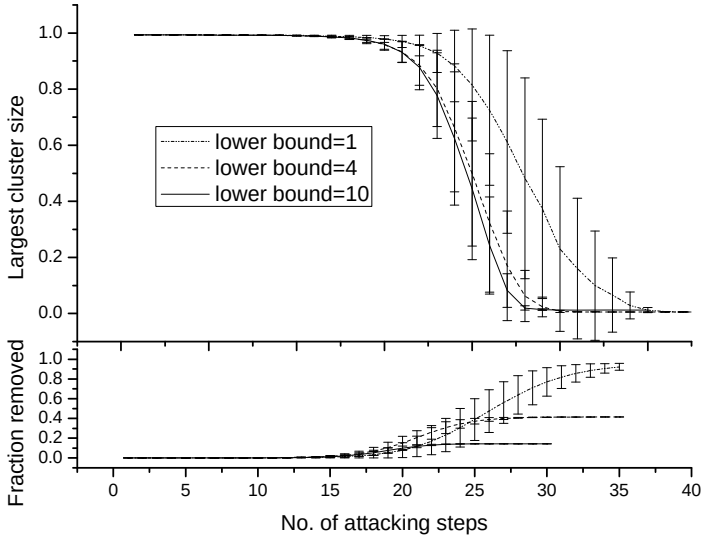


(b) Internet Router-level model

Fig. 3. The efficiencies of the greedy sequential attack and the coordinated attack in the two Internet models, respectively.

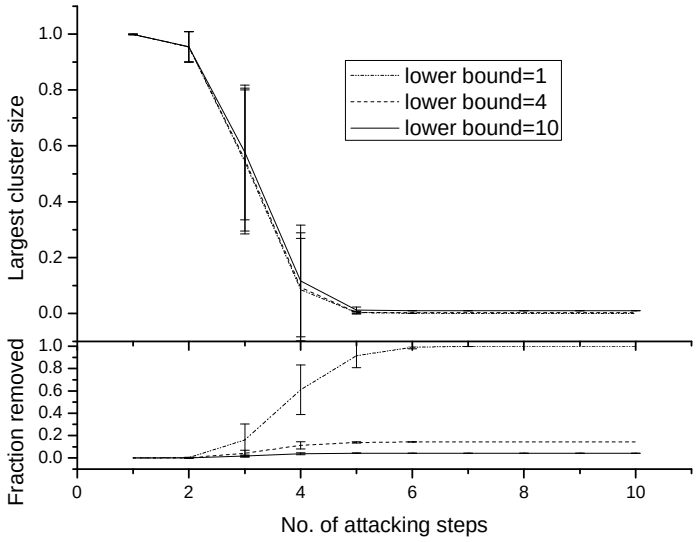


(a) AS-level Internet model

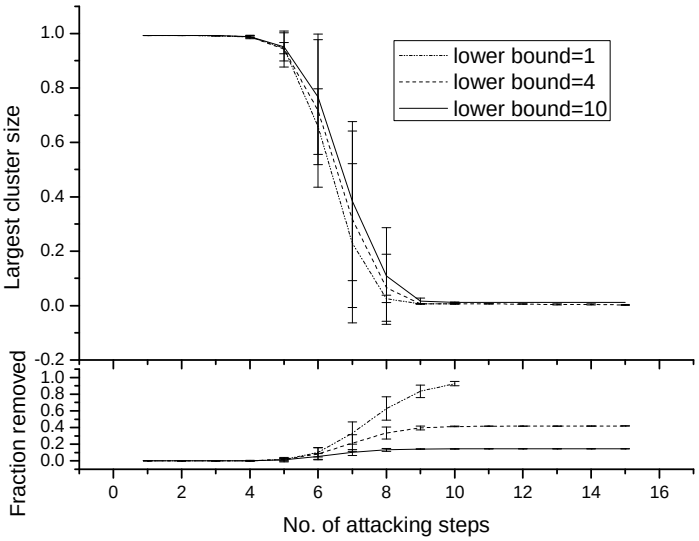


(b) Router-level Internet model

Fig. 4. The efficiencies of the lower-bounded parallel attack with nodal-degree lower bounds being set at 1, 4 and 10, respectively.

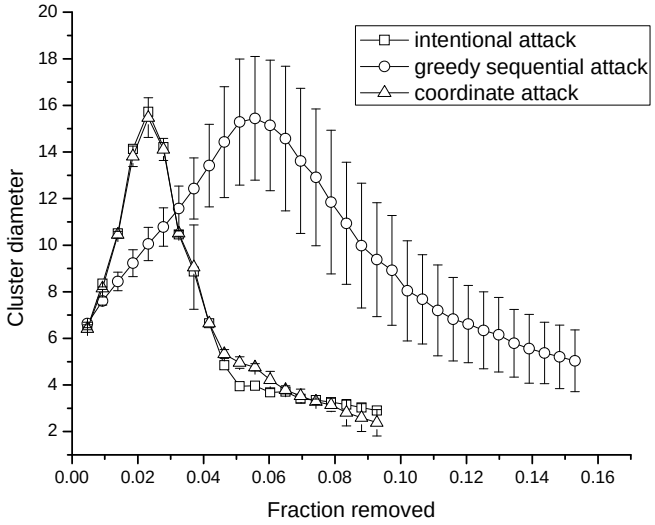


(a) Internet AS-level model

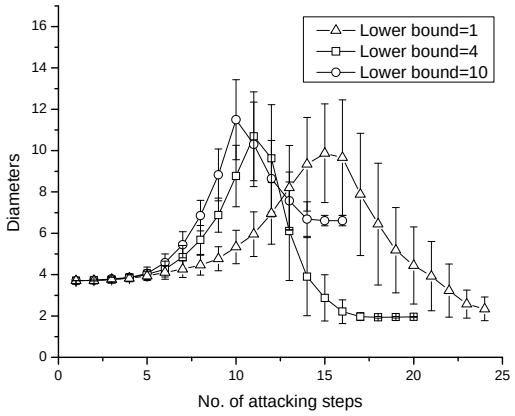


(b) Internet Router-level model

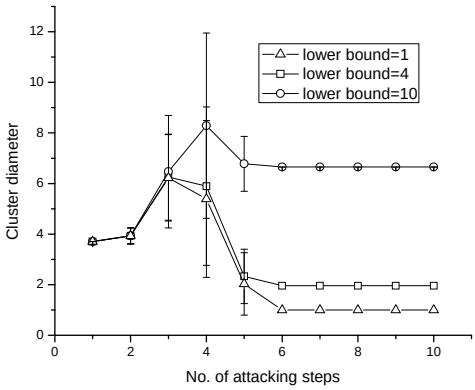
Fig. 5. The efficiencies of the lower-bounded flooding attack with nodal-degree lower bounds being set at 1, 4 and 10, respectively.



(a) Greedy sequential attack and coordinated attack



(b) Lower-bounded parallel attack



(c) Lower-bounded flooding attack

Fig. 6. The cluster diameters of the AS-level Internet model under different types of attacks.