# Structural robustness of scale-free networks against overload failures

Shogo Mizutaka* and Kousuke Yakubo†
*Department of Applied Physics, Hokkaido University, Sapporo 060-8628, Japan*
(Received 21 March 2013; published 8 July 2013)

We study the structural robustness of scale-free networks against overload failures induced by loads exceeding the node capacity, based on analytical and numerical approaches to the percolation problem in which a fixed number of nodes are removed according to the overload probability. Modeling fluctuating loads by random walkers in a network, we find that the degree dependence of the overload probability drastically changes with respect to the total load. We also elucidate that there exist two types of structural robustness of networks against overload failures. One is measured by the critical total load $W_c$ and the other is by the critical node removal fraction $f_c$. Enhancing the scale-free property, networks become fragile in both senses of $W_c$ and $f_c$. By contrast, increasing the node tolerance, scale-free networks become robust in the sense of the critical total load, while they come to be fragile in the sense of the critical node removal fraction. Furthermore, we show that these trends are not affected by degree-degree correlations, although assortative mixing makes networks robust in both senses of $W_c$ and $f_c$.

DOI: 10.1103/PhysRevE.88.012803 PACS number(s): 89.75.Hc, 64.60.ah, 64.60.aq, 05.40.Fb

## I. INTRODUCTION

Networks with complex topologies have been studied extensively to describe a wide range of complex systems [1–7]. Many real-world complex networks provide functions such as electric power supply by a power grid network, information seeking via the World Wide Web, and the decomposition and synthesis of chemical compounds in a metabolic network. These functionalities are supported by the global connectivity of the network. However, if the network is decomposed into smaller disconnected pieces by failures of nodes or edges, the network function cannot be maintained. Thus the robustness of networks against damage is a significant issue from a practical viewpoint. This problem has been studied mainly in two contexts. One is related to the structural robustness argued in a percolation problem where a fixed number of nodes (or edges) are simultaneously removed [8–14] and the other is studied in a sense of the dynamical robustness against cascading failures in which the removal of a few nodes triggers the removal of remaining nodes [15–29]. There have been a number of reports of the percolation problem on complex networks (i.e., structural robustness), particularly on scale-free networks with power-law degree distributions that are ubiquitous in real-world systems [7]. An important finding obtained by these studies is that scale-free networks are fairly robust against random failures, i.e., removing nodes randomly, while they are fragile to the targeted removal of the highest degree nodes [8–11]. Although degree correlations and/or community structures affect the robustness of networks, these trends are persistent [12–14].

Previous works on the structural robustness of scale-free networks have concentrated on percolation transitions caused by random failures and targeted attacks. Random failures represent accidental breakdowns of nodes and targeted ones correspond, for example, to intentional attacks by terrorists. There are, however, many possible causes of node failures in functional networks. One of the most important and common causes is *overload failure*, i.e., a failure induced by loads exceeding node capacities. For instance, increasing the electrical power demand may induce overload failures of substations in power grid networks. On the Internet, the recent rapid rise in smartphone users increases the total amount of packet traffic, which causes overload failures of servers or routers. These examples show that overload failures are common origin of breakdowns of functional networks. Although overload failures have been studied extensively in the context of dynamical robustness against avalanchelike cascading failures [15–25], there is no work on the percolation transition induced by a simultaneous removal of overloaded nodes, which can form a basis of the study of cascading overload failures. Recently, Kishore *et al.* examined the probability of a node having an overload failure as a function of the degree of the node [30,31]. Since the load on a node fluctuates temporally in most networks, each event of overload failures is governed by the load fluctuations. They modeled such fluctuations by random walkers on the network and found that small degree nodes are more likely to have overload failures. This approach can be utilized to examine the percolation transition by overload failures.

In this study, we quantitatively analyze the structural robustness of scale-free networks against overload failures by examining the percolation transition induced by removing a fixed number of nodes according to the overload probability. We adopt the random-walk model [30,31] to describe load fluctuations and calculate analytically the percolation transition point. Our results show that the structural robustness measured by the critical total load $W_c$ should be distinguished from that in the sense of the critical node removal fraction $f_c$. We also find that scale-free networks are fragile to overload failures compared to non-scale-free networks in both senses of $W_c$ and $f_c$. On the contrary, strengthening the node tolerance, the network becomes robust in the sense of the acceptable total load, while it becomes fragile in the sense of the critical node removal fraction.

This paper is organized as follows. In Sec. II, we give the random-walk model to describe fluctuating loads in a network and define the overload failure quantitatively. The original model proposed by Kishore *et al.* [30] is slightly modified to

*s.mizutaka@eng.hokudai.ac.jp
†yakubo@eng.hokudai.ac.jp

 

take into account increases in the total amount of load $W$ from the initial value at the network formation. Using the modified model, we obtain the overload probability as a function of the node degree. In Sec. III, we explain how we calculate the critical point of the percolation transition by removing nodes according to the overload probability, and give our results for scale-free networks. In this analysis, we use the method developed recently by Tanizawa *et al.* [14]. Finally, concluding remarks are presented in Sec. IV.

## II. OVERLOAD PROBABILITY

Many functional networks achieve their functionality by means of some kind of flow such as the electric current in a power grid network and packet transfers on the Internet. The flow from one node (source) to another (sink) often follows the shortest path between two nodes. If we consider particle flow in a network along the shortest paths between many randomly selected node pairs in a unit time, the statistical property of the temporal fluctuation of the number of particles on a node is the same as that of the number of random walkers on the node in the network containing many random walkers [32,33]. Based on this fact, Kishore *et al.* have described the uncorrelated load fluctuations by random walkers in a network [30]. Here we adopt this idea to formulate overload failures.

The total number of walkers represents the total load. If the number of walkers $w_i(t)$ on node $i$ at time $t$, which represents the load on node $i$, exceeds the predetermined node capacity $q_i$, the node $i$ fails because of an overload. Let us assume that a network with $N$ nodes is singly connected and undirected and that a random walker on the node $i$ jumps to any one of its neighboring nodes with an equal probability. The probability $P_i(t)$ of finding the walker on node $i$ at time $t$ is then governed by the master equation

$$P_i(t+1) = \sum_j \frac{a_{ij}}{k_j} P_j(t), \tag{1}$$

where $a_{ij}$ is the adjacency matrix element of the network, which takes the value 1 if $i$ and $j$ are directly connected and 0 otherwise, and $k_i = \sum_j a_{ij}$ is the degree of the node $i$. In the steady state, the probability $P_i$ does not depend on $t$ and Eq. (1) becomes the eigenequation $p_i = \sum_j (a_{ij}/k_j) p_j$, where $p_i = \lim_{t\to\infty} P_i(t)$. This equation can be solved easily and the steady-state probability $p_i$ is proportional to the degree $k_i$ as shown by [34]

$$p_i = \frac{k_i}{2M}, \tag{2}$$

where $M = \sum_i k_i/2$ is the number of edges in the network. Since $p_i$ depends only on the degree of the node $i$, the steady-state probability can be denoted by $p_k$ $(= k/2M)$. Hereafter, we concentrate on the steady-state distribution of random walkers in the network. Considering the uncorrelated character of random walkers, the probability $h_k^{W_0}(w)$ to find $w$ walkers on a degree-$k$ node in the network containing totally $W_0$ walkers is given by the binomial probability

$$h_k^{W_0}(w) = \binom{W_0}{w} p_k^w (1-p_k)^{W_0-w}. \tag{3}$$

Thus the mean value and the variance of the number of walkers on the degree-$k$ node are

$$\langle w \rangle_k = W_0 p_k \tag{4}$$

and

$$\sigma_k^2 = W_0 p_k (1-p_k), \tag{5}$$

respectively. It is natural to set the capacity $q_k$ of the degree-$k$ node as

$$q_k(W_0) = \langle w \rangle_k + m\sigma_k, \tag{6}$$

where $m$ is a real parameter representing the tolerance of nodes against loads. It should be noted that this capacity depends on the total number of walkers $W_0$ through Eqs. (4) and (5) though $W_0$ is not written explicitly on the right-hand side of Eq. (6). The overload probability, i.e., the probability that $w$ exceeds $q_k(W_0)$, is then calculated by summing up the distribution function given by Eq. (3) over $w$ larger than $q_k(W_0)$.

In the above treatment, we must never overlook the fact that the total load is not temporally constant. The total load $W$ when an overload failure occurs is generally not the same as $W_0$ at the initial time when the node capacity is assigned. The total load at a later stage is often higher than the initial total load, as in the case of the increasing electrical power demand. Taking this situation into account, we use the distribution function given by Eq. (3) with $W$ instead of $W_0$, while the capacity $q_k$ is given by $W_0$. Therefore, the overload probability $F_W(k)$ of the degree-$k$ node is given by

$$F_W(k) = \sum_{w=[q_k(W_0)]+1}^{W} \binom{W}{w} p_k^w (1-p_k)^{W-w}, \tag{7}$$

where $[x]$ represents the greatest integer not greater than $x$. This expression can be simplified as

$$F_W(k) = I_{k/2M}([q_k(W_0)]+1, W-[q_k(W_0)]), \tag{8}$$

where $I_x(a,b)$ is the regularized incomplete beta function [35]. Kishore *et al.* [30,31] have shown that the probability $F_W(k)$ at $W = W_0$ is a decreasing function of $k$ as shown by the thin line at the bottom in Fig. 1. This result, corresponding to the case where the total load does not change over time, exhibits that small degree nodes are more likely to experience overload failures than hubs. Recalling that a scale-free network is quite robust to random failures or the selective removal of lower degree nodes, it seems that scale-free networks are resilient to overload failures. However, the probability $F_W(k)$ changes its profile significantly when $W$ becomes larger than $W_0$. The thick lines in Fig. 1 indicate the $k$ dependences of $F_W(k)$ for various values of $W$ larger than $W_0$. For $W = 1.3W_0$, for instance, $F_W(k)$ is an increasing function of $k$, which implies that the node removal by overload failures is similar to the selective removal of higher degree nodes. Thus scale-free networks might be fragile against overload failures when the total load $W$ is much larger than the initial value $W_0$. The profile of $F_W(k)$ also depends on the value of the node tolerance parameter $m$ (thick gray line in Fig. 1). It is therefore necessary to evaluate quantitatively the resilience of scale-free networks to overload failures.

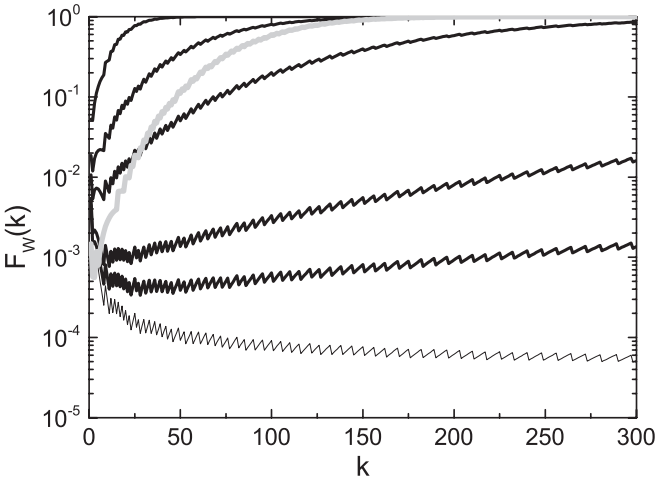


FIG. 1. Profiles of the overload probability $F_W(k)$ for various values of $W$. The thin line at the bottom shows $F_W(k)$ at $W = W_0$. The thick black lines from the top show the profiles of $F_W(k)$ for $W = 2W_0$, $1.5W_0$, $1.3W_0$, $1.1W_0$, and $1.05W_0$, respectively. The parameter $m$ is fixed at $m = 4$ for these lines. The thick gray line represents $F_W(k)$ for $W = 1.628W_0$ and $m = 6.0$. The initial total load $W_0$ is set at $W_0 = 2M$ with $M = 200\,000$. The zigzag structure in these curves is due to the quantity $[q_k(W_0)]$ in Eq. (8).

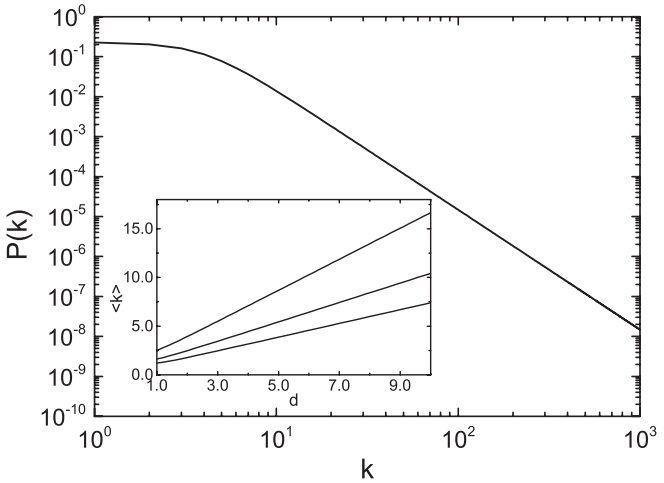


FIG. 2. Degree distribution function $P(k)$ given by Eq. (12) with $\gamma = 3.0$ and $d = 4.0$. The average degree of this distribution function is $\langle k\rangle = 4.44$. The inset shows the $d$ dependence of $\langle k\rangle$ for $\gamma = 2.5$, 3.0, and 4.0 from top to bottom, respectively.

## III. ROBUSTNESS AGAINST OVERLOAD FAILURES

In order to assess the structural robustness of scale-free networks against overload failures, we calculate the critical point of the percolation transition by removing nodes according to the overload probability. To this end, we employ the method developed recently by Tanizawa *et al.* [14]. This method allows us to treat percolation problems for an arbitrary degree distribution, arbitrary degree-degree correlations, and an arbitrary removal process depending on the degree of nodes if the network has a treelike structure near the percolation transition. The critical total load $W_c$ and the critical node removal fraction $f_c$ are calculated from the branching matrix defined by

$$B_{k'k} = (k' - 1)b_{k'}P(k'|k), \tag{9}$$

where $b_k$ is the remaining fraction of degree-$k$ nodes and $P(k'|k)$ is the conditional probability that an arbitrary neighbor of a degree-$k$ node has the degree of $k'$. At criticality, the largest eigenvalue of $B_{k'k}$ becomes unity [14,36]. In the specific case that the network does not possess degree-degree correlations, the conditional probability becomes $P(k'|k) = k'P(k')/\langle k\rangle$ depending only on $k'$, where $P(k)$ is the degree distribution function and $\langle k\rangle$ is the average degree. In this case, the branching matrix $B_{k'k} = b_{k'}k'(k' - 1)P(k')/\langle k\rangle$ also depends only on $k'$ and has the eigenvalues $\{\lambda_{\max},0,0,\ldots,0\}$, where $\lambda_{\max} = \sum_k b_k k(k - 1)P(k)/\langle k\rangle$. Since the remaining fraction $b_k$ is given by $1 - F_W(k)$ in our case, the condition for the transition point of the percolation by overload failures is given by

$$\sum_k [(k - 1)F_W(k) - k + 2]kP(k) = 0 \tag{10}$$

for networks without degree correlations, where the definition $\langle k\rangle = \sum_k kP(k)$ is used. If $W$ is the only tunable parameter among the other fixed parameters $W_0$, $m$, etc., this equation with Eq. (8) for $F_W(k)$ provides the critical value of the total load $W_c$. The critical node removal fraction $f_c$ is then calculated by

$$f_c = \sum_k F_{W_c}(k)P(k). \tag{11}$$

Hereafter, we assess the structural robustness of networks from the perspectives of $W_c$ and $f_c$. A network is fragile if $W_c$ or $f_c$ is small.

First, we consider generalized random graphs with the degree distribution function presented by

$$P(k) = \frac{C}{k^\gamma + d^\gamma} \quad (1 \leqslant k < \infty), \tag{12}$$

where $d$ and $\gamma$ are real parameters and $C = [\sum_{k=1}^{\infty} 1/(k^\gamma + d^\gamma)]^{-1}$ is the normalization constant. The exponent $\gamma$ is assumed to be greater than 2 to have a finite average degree $\langle k\rangle$. This distribution function is proportional to $k^{-\gamma}$ for $k \gg 1$, which means that the generalized random graph has the scale-free property, as shown in Fig. 2. We can tune the average degree $\langle k\rangle$ by controlling the parameter $d$ for any value of $\gamma$. The inset of Fig. 2 shows the $d$ dependence of $\langle k\rangle$. Since the generalized random graph has no degree correlations, we can apply Eq. (10) to calculate the transition point of the percolation by overload failures. In order to confirm the validity of our analytical approach, we compare the critical total load $W_c$ and the critical node removal fraction $f_c$ obtained by Eqs. (10) and (11), respectively, with numerical results. Figure 3 shows that the vanishing points of the numerically calculated order parameter $S$ (the number of nodes included in the giant component divided by the total node number $N$) agree quite well with the theoretically predicted values (vertical dashed lines), which confirms the validity of the analytical treatment.

Figure 4 shows the critical total load $W_c$ rescaled by the initial total load $W_0$ as a function of the scale-free exponent $\gamma$. In this calculation, we truncate the size of the branching matrix

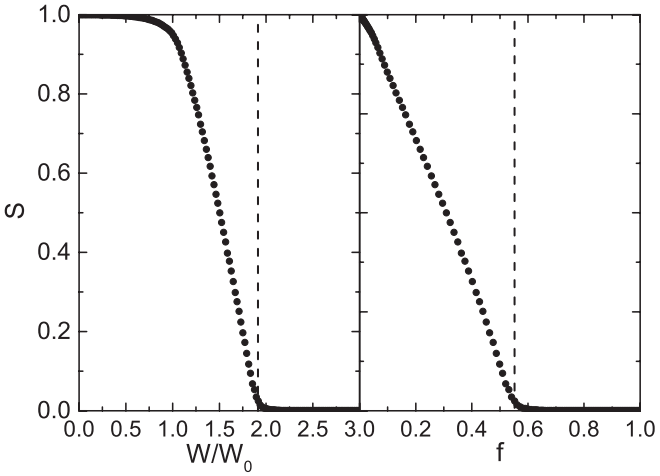


FIG. 3. Numerical confirmation of the analytical treatment. The symbols represent the numerically calculated order parameter $S$ (the number of nodes in the giant component divided by the total node number $N$) as a function of (a) the rescaled total load $W/W_0$ and (b) the node removal fraction $f$, where $W_0$ is the initial total load. The degree distribution $P(k)$ is given by Eq. (12) with $\gamma = 2.5$ and $d = 5.8272$ ($\langle k\rangle = 10.0$) and the generalized random graph for the numerical calculations contains $N = 10\,000$ nodes. The overload failure occurs under the condition of $m = 2$ and $W_0 = 2M$, where $M$ is the number of edges. The numerical results are averaged over 50 samples. The vertical dashed lines represent the critical total load $W_c/W_0 = 1.912$ and the critical removal fraction $f_c = 0.547$ obtained theoretically by Eqs. (10) and (11).

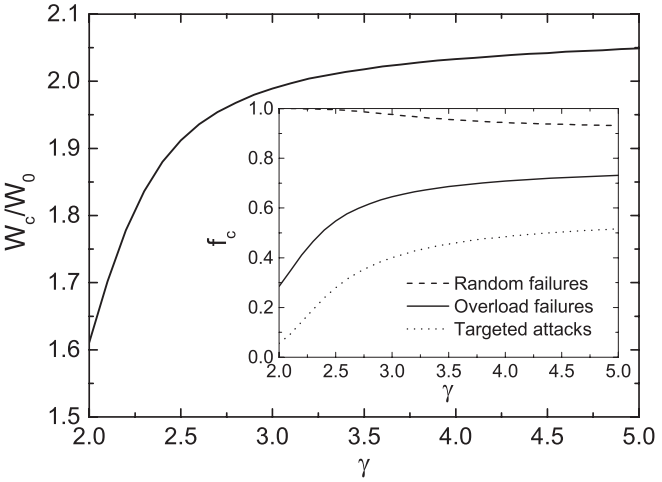


FIG. 4. Critical total load $W_c$ rescaled by the initial load $W_0$ as a function of the scale-free exponent $\gamma$. The result is analytically calculated for the scale-free random graphs whose degree distribution is described by Eq. (12) with the fixed average degree $\langle k\rangle = 10.0$ and by setting $m = 2$ and $W_0 = 2M$. The solid, dashed, and dotted lines in the inset show the $\gamma$ dependence of the critical node removal fraction $f_c$ for overload failures, random failures, and targeted attacks, respectively.

$B_{kk'}$ to $k_{\max} \times k_{\max}$, where $k_{\max}$ is the maximum degree in a network with a finite but large number of nodes ($N = 10^5$) estimated by $\int_{k_{\max}}^{N} P(k)\,dk = 1/N$. In addition, we fix the average degree at $\langle k\rangle = 10$ independently of the value of $\gamma$ and the node tolerance parameter and the initial total load are set as $m = 2$ and $W_0 = 2M$ with $M = N\langle k\rangle/2 = 500\,000$, respectively. The solid line in Fig. 4 increases with $\gamma$, which means that the scale-free property makes a network fragile against overload failures in the sense of $W_c$. The solid line in the inset of Fig. 4 displays the critical node removal fraction $f_c$ calculated by Eq. (11). The quantity $f_c$ is also an increasing function of $\gamma$. This implies that scale-free networks are fragile also in the sense of $f_c$. The reason why $f_c$ is an increasing function of $\gamma$ can be easily understood as follows. Consider a situation where nodes are removed from two scale-free networks $G_1$ and $G_2$ with different exponents $\gamma_1$ and $\gamma_2$ ($>\gamma_1$) by the same node removal fraction $f$. Hub nodes in the network $G_1$ are more preferentially removed than in $G_2$ because $F_W(k)$ is an increasing function of $k$, as shown by Fig. 1. Since scale-free networks are fragile to the removal of hub nodes, $G_1$ has a smaller $f_c$ than that for $G_2$. In order to explain the $\gamma$ dependence of $W_c$, let us consider the average degree of the removed nodes $\langle k\rangle_{\rm rem} = \sum_k k F_W(k) P(k)$. From the profiles of $F_W(k)$ and $P(k)$, $\langle k\rangle_{\rm rem}$ for a fixed $W$ decreases as $\gamma$ increases. Thus, if we remove nodes from $G_1$ and $G_2$ under a fixed $W$, hub nodes in $G_1$ are also more preferentially removed than in $G_2$ as in the case of a fixed $f$, which makes $W_c$ an increasing function of $\gamma$.

The dashed and dotted lines in the inset of Fig. 4 show the critical fractions for random failures and targeted attacks (selective removal of the highest degree nodes), respectively, for the same networks. The critical fraction for overload failures behaves similarly to $f_c$ for targeted attacks because the overload probability $F_W(k)$ is an increasing function of $k$ for $W > W_0$. This inset shows that a network is much more fragile against overload failures than against random failures, while it is robust compared to the case of targeted attacks. This is because $F_W(k)$ has an intermediate profile between the removal probabilities for random failures and targeted attacks. The removal probability $F_{\rm TA}(k)$ for targeted attacks is given by $F_{\rm TA}(k) = \theta(k - k_c)$, where $\theta(x)$ is the step function and $k_c$ is a fixed degree, while $F_{\rm RF}(k) = p$ for random failures, where $p$ is a constant probability. Therefore, hub nodes are more selectively removed by $F_{\rm TA}(k)$ than by $F_W(k)$ and more selectively by $F_W(k)$ than by $F_{\rm RF}(k)$. Because of the fragility of scale-free networks to hub removal, $f_c$ for overload failures takes an intermediate value between those for random failures and targeted attacks.

It is interesting to clarify how the network resilience to overload failures depends on the node tolerance parameter $m$. Figure 5 shows the $m$ dependences of $W_c/W_0$ and $f_c$ for the scale-free random graphs described by Eq. (12) with $\gamma = 2.5$ and 4.5 and the Erdős-Rényi random graph ($\gamma \to \infty$). The critical total load $W_c/W_0$ is an increasing function of $m$ regardless of the degree of the scale-free property, which implies that the network becomes robust in the sense of $W_c$ by increasing $m$. This is obvious because a network can accept a larger total load if the capacity of each node increases. On the contrary, the fact that the critical node removal fraction $f_c$ is a decreasing function of $m$ indicates that the network becomes fragile in the sense of $f_c$ when strengthening the node tolerance. To understand the $m$ dependence of $f_c$, let us consider a situation where we remove a fixed fraction of nodes from two networks with the same structure but with different

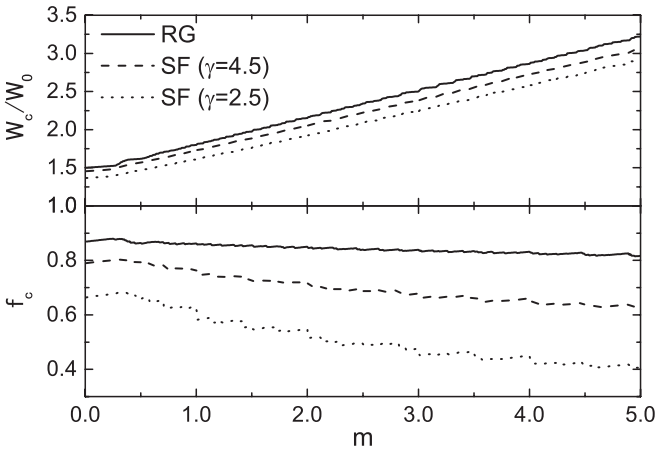


FIG. 5. Rescaled critical total load $W_c/W_0$ (upper panel) and the critical node removal fraction $f_c$ (lower panel) as a function of the node tolerance parameter $m$. The dashed and dotted lines represent the analytical results for the scale-free random graphs (SF) described by Eq. (12) with $\gamma = 4.5$ and 2.5, respectively. The solid lines indicate the results for the Erdős-Rényi random graph (RG). We set $\langle k\rangle = 10.0$ and $W_0 = 2M$ as in the case of Fig. 4.

node tolerances. The overload probabilities for the same node removal fraction $f$ but different tolerances are compared in Fig. 1, as indicated by the third black line from the top ($m = 4.0$, $W = 1.3W_0$) and the gray line ($m = 6.0$, $W = 1.628W_0$), where the total load $W$ for the gray line is tuned so that $f$ becomes the same as that for the black line. These two lines show that the overload probability of the network with the tolerance of $m = 4.0$ is higher than that of the network with $m = 6.0$ for low-degree nodes, whereas this relationship is the opposite for high-degree nodes. This implies that hub nodes are more selectively removed in a network with a larger node tolerance. Thus the critical node removal fraction $f_c$ decreases as $m$ increases. The opposite behaviors in the $m$ dependences of $W_c$ and $f_c$ suggest that the network robustness in the sense of $W_c$ should be distinguished from that in the sense of $f_c$.

Next we study how the nearest-neighbor degree-degree correlation affects the robustness of scale-free networks against overload failures. As is well known, many social networks exhibit assortative mixing, i.e., high-degree nodes are more likely to be connected to hubs, while technological or biological networks show disassortative mixing [12,13]. It is therefore important to clarify whether the degree correlation make networks robust or fragile. The degree correlation is described by the conditional probability $P(k'|k)$ or the joint probability $P(k,k') = R(k)P(k'|k)$, which is the probability that a randomly selected edge connects a degree-$k$ node to a degree-$k'$ node. The function $R(k)$ is defined by

$$R(k) = \frac{kP(k)}{\langle k\rangle}, \tag{13}$$

which represents the probability that a randomly selected edge connects to a degree-$k$ node. Since $P(k'|k) = R(k')$ for networks without degree correlations, $P(k,k')$ for uncorrelated networks can be written as the product of the functions of $k$ and $k'$ as $P(k,k') = P_0(k,k') \equiv R(k)R(k')$. Conversely, we can introduce the degree correlations into a network by using $P(k,k')$, which cannot be decomposed by $R(k)$ and $R(k')$. Here we use the joint probability $P(k,k')$ proposed by Newman [13], which is given by

$$P(k,k') = P_0(k,k') - \frac{r}{r^*}[P_0(k,k') - Q(k,k')], \tag{14}$$

where

$$Q(k,k') = R(k)\tilde{R}(k') + R(k')\tilde{R}(k) - \tilde{R}(k)\tilde{R}(k'), \tag{15}$$

$$\tilde{R}(k) = \frac{kX(k)}{\langle k\rangle_X}, \tag{16}$$

$$\langle k^n\rangle_X = \sum_k k^n X(k), \tag{17}$$

$$r^* = -\frac{1}{\sigma^2}\left(\frac{\langle k^2\rangle}{\langle k\rangle} - \frac{\langle k^2\rangle_X}{\langle k\rangle_X}\right)^2, \tag{18}$$

and

$$\sigma^2 = \frac{\langle k^3\rangle}{\langle k\rangle} - \frac{\langle k^2\rangle^2}{\langle k\rangle^2}, \tag{19}$$

with an arbitrary distribution function $X(k)$ normalized as $\sum_k X(k) = 1$. The parameter $r$ in Eq. (14) gives the Pearson correlation coefficient defined by $\sum_{k,k'}(k-1)(k'-1)[P(k,k') - P_0(k,k')]/\sigma^2$, regardless of the choice of $X(k)$. The Pearson correlation coefficient quantifies the strength of the degree-degree correlations of the network. If $r > 0$, the network exhibits assortative mixing on its degrees, while it exhibits disassortative mixing if $r < 0$. Although the distribution function $X(k)$ is arbitrary, the permissible range of $r$ determined by the condition $0 \leqslant P(k,k') \leqslant 1$ depends on the choice of $X(k)$. In this work, we employ a functional form of $X(k)$ similar to Eq. (12), i.e.,

$$X(k) \propto \frac{1}{k^\alpha + D^\alpha} \quad (1 \leqslant k < \infty), \tag{20}$$

where $\alpha = 8.0$ and $D = 12.0$. The degree distribution $P(k)$ is given by Eq. (12) with $\gamma = 4.5$ and $d = 15.854$, which leads to $\langle k\rangle = 10.0$. Here we choose $\gamma > 4$ to have a finite third moment $\langle k^3\rangle$.

The percolation transition point of degree-correlated networks is also calculated by evaluating the largest eigenvalue of the branching matrix $B_{k'k}$ defined by Eq. (9). Since the conditional probability $P(k'|k)$ obtained by $P(k'|k) = P(k,k')/R(k)$ depends not only on $k'$ but also on $k$ when $P(k,k')$ is presented by Eq. (14), we need to diagonalize the branching matrix $B_{k'k}$ numerically. In actual diagonalizations, the matrix size is truncated by $k_{max} = 276$, which corresponds to the finite number of nodes $N = 10^5$. The initial total load $W_0$ is set as $W_0 = 2M$ $(=N\langle k\rangle)$. Figure 6 shows the $r$ dependences of the critical node removal fraction $f_c$ for three values of the node tolerance parameter $m$. The fact that $f_c$ is an increasing function of $r$ implies that scale-free networks with assortative mixing are more robust (in the sense of $f_c$) against overload failures than those with disassortative mixing. The critical total load $W_c$ also increases with increasing $r$ (not shown). Thus the degree correlation operates on two types of robustness (in the senses of $W_c$ and $f_c$) in the same manner. This trend is similar to the case of targeted attacks in scale-free networks [12,13]. This is because the overload probability $F_W(k)$ of a hub is larger than that of a small degree node, like the node removal probability $1 - b_k$ for targeted attacks.

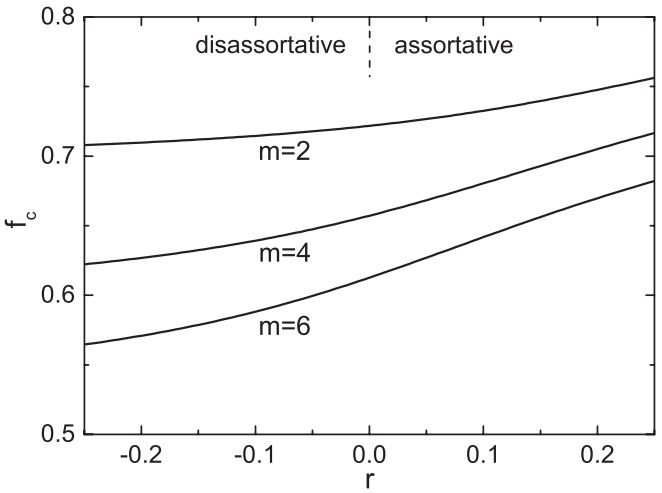


FIG. 6. Critical node removal fraction $f_c$ as a function of the Pearson correlation coefficient $r$. The parameters used for the calculations are given in the text. The three lines indicate the results for $m = 2$, 4, and 6 from top to bottom, respectively.

## IV. CONCLUSION

In this study, we have analyzed the structural robustness of scale-free networks against overload failures. Using the idea presented by Kishore *et al.* [30], fluctuating loads inducing overload failures are modeled by random walkers in networks. We examined the robustness of degree-correlated and -uncorrelated networks by considering the percolation problem where we remove nodes according to the overload probability $F_W(k)$ given by the regularized incomplete beta function. The percolation critical point has been analyzed by employing the method proposed recently by Tanizawa *et al.* [14]. Investigating uncorrelated scale-free networks, we found that there exist at least two types of network robustness against overload failures. One is measured by the critical total load $W_c$ and the other is by the critical node removal fraction $f_c$. Networks become fragile in both senses of $W_c$ and $f_c$ when enhancing the scale-free nature (i.e., decreasing the scale-free exponent $\gamma$) while keeping the average degree $\langle k \rangle$ constant. If we increase the node tolerance parameter $m$, which determines the node capacity $q_k$, however, scale-free networks become robust in the sense of the critical total load $W_c$, while they become fragile in the sense of $f_c$. Furthermore, our results for degree-correlated scale-free networks demonstrate that positive correlations (assortative mixing) between the degrees of adjacent nodes make networks robust in both senses of $W_c$ and $f_c$. This trend observed for overload failures is similar to the case of targeted attacks because the overload probability is an increasing function of $k$.

In our work, we simultaneously remove nodes from the network with the probability $F_W(k)$. This procedure is the same as that used in previous studies of percolation processes by random failures or targeted attacks. In an actual network with overload failures, the failure of a node or an edge in the network often triggers successive failures of other elements, which constitutes a cascade of failures. The problem of cascading failures by overloads has been extensively studied so far [15–25]. These studies are based on many assumptions regarding the initial load, the load propagation process, the load distribution update method, etc. The random-walk model of overload failures employed in this work is based on observational evidence of load fluctuations [32,33] and easy to handle analytically. If we describe a cascade of overload failures by the random-walk model, the critical total load and critical node removal fraction leading to the global cascade must be much lower than those given by Eqs. (10) and (11). The present results provide a basis for the study of a dynamical robustness against cascading overload failures. Thus it would be meaningful to study the problem of cascading overload failures by means of the random-walk model to clarify the resilience of realistic networks to damage and identify effective protection and cascade control strategies.

## ACKNOWLEDGMENT

This work was supported by a Grant-in-Aid for Scientific Research (No. 22560058) from the Japan Society for the Promotion of Science. Numerical calculations in this work were performed in part at the facilities of the Supercomputer Center, Institute for Solid State Physics, University of Tokyo.

[1] R. Albert and A.-L. Barabási, Rev. Mod. Phys. **74**, 47 (2002).
[2] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, Phys. Rep. **424**, 175 (2006).
[3] S. N. Dorogovtsev, A. V. Goltsev, and J. F. F. Mendes, Rev. Mod. Phys. **80**, 1275 (2008).
[4] M. E. J. Newman, *Networks: An Introduction* (Oxford University Press, Oxford, 2010).
[5] S. N. Dorogovtsev, *Lectures on Complex Networks* (Oxford University Press, Oxford, 2010).
[6] A. Barrat, M. Barthélemy, and A. Vespignani, *Dynamical Processes on Complex Networks* (Cambridge University Press, Cambridge, 2012).
[7] G. Caldarelli, *Scale-Free Networks: Complex Webs in Nature and Technology* (Oxford University Press, Oxford, 2013).
[8] R. Albert, H. Jeong, and A.-L. Barabási, Nature (London) **406**, 378 (2000).
[9] D. S. Callaway, M. E. J. Newman, S. H. Strogatz, and D. J. Watts, Phys. Rev. Lett. **85**, 5468 (2000).
[10] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, Phys. Rev. Lett. **85**, 4626 (2000).
[11] R. Cohen, K. Erez, D. ben-Avraham, and S. Havlin, Phys. Rev. Lett. **86**, 3682 (2001).
[12] M. E. J. Newman, Phys. Rev. Lett. **89**, 208701 (2002).
[13] M. E. J. Newman, Phys. Rev. E **67**, 026126 (2003).
[14] T. Tanizawa, S. Havlin, and H. E. Stanley, Phys. Rev. E **85**, 046109 (2012).
[15] M. L. Sachtjen, B. A. Carreras, and V. E. Lynch, Phys. Rev. E **61**, 4877 (2000).

[16] Y. Moreno, J. B. Gómez, and A. F. Pacheco, Europhys. Lett. **58**, 630 (2002).
[17] P. Holme and B. J. Kim, Phys. Rev. E **65**, 066109 (2002).
[18] A. E. Motter and Y.-C. Lai, Phys. Rev. E **66**, 065102(R) (2002).
[19] A. E. Motter, Phys. Rev. Lett. **93**, 098701 (2004).
[20] P. Crucitti, V. Latora, and M. Marchiori, Phys. Rev. E **69**, 045104(R) (2004).
[21] D. Heide, M. Schäfer, and M. Greiner, Phys. Rev. E **77**, 056103 (2008).
[22] I. Simonsen, L. Buzna, K. Peters, S. Bornholdt, and D. Helbing, Phys. Rev. Lett. **100**, 218701 (2008).
[23] W.-X. Wang and G. Chen, Phys. Rev. E **77**, 026101 (2008).
[24] A. Asztalos, S. Sreenivasan, B. K. Szymanski, and G. Korniss, Eur. Phys. J. B **85**, 288 (2012).
[25] J. Wang, Physica A **392**, 2257 (2013).
[26] D. J. Watts, Proc. Natl. Acad. Sci. USA **99**, 5766 (2002).
[27] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, Nature (London) **464**, 1025 (2010).
[28] J. Gao, S. V. Buldyrev, S. Havlin, and H. E. Stanley, Phys. Rev. Lett. **107**, 195701 (2011).
[29] D. Zhou, H. E. Stanley, G. D'Agostino, and A. Scala, Phys. Rev. E **86**, 066103 (2012).
[30] V. Kishore, M. S. Santhanam, and R. E. Amritkar, Phys. Rev. Lett. **106**, 188701 (2011).
[31] V. Kishore, M. S. Santhanam, and R. E. Amritkar, Phys. Rev. E **85**, 056120 (2012).
[32] M. A. de Menezes and A.-L. Barabási, Phys. Rev. Lett. **92**, 028701 (2004).
[33] S. Meloni, J. Gómez-Gardeñes, V. Latora, and Y. Moreno, Phys. Rev. Lett. **100**, 208701 (2008).
[34] J. D. Noh and H. Rieger, Phys. Rev. Lett. **92**, 118701 (2004).
[35] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions* (Dover, New York, 1964).
[36] A. V. Goltsev, S. N. Dorogovtsev, and J. F. F. Mendes, Phys. Rev. E **78**, 051105 (2008).