Research Article

International Journal of Distributed Sensor Networks

International Journal of Distributed Sensor Networks
2017, Vol. 13(4)

DOI: 10.1177/1550147717701141
journals.sagepub.com/home/ijdsn
SAGE

Percolation analysis for constructing a robust modular topology based on a binary-dynamics model

Shinya Toyonaga[1], Daichi Kominami[2] and Masayuki Murata[1]

Abstract

In the context of Internet of Things, virtualization of wireless sensor networks is a crucial technology for sharing sensors as infrastructure. In our previous work, we proposed a brain-inspired method for constructing a robust and adaptive virtual wireless sensor network topology and showed that the method of constructing links between modules has crucial effect on robustness and adaptivity of the constructed virtual wireless sensor network topology. However, the best way of constructing a robust and adaptive virtual wireless sensor network topology is still unclear. Therefore, in this article, we use an analytical approach and propose a method for clarifying robustness of a topology according to the method of constructing links between modules. We add a new tool to a binary-dynamics model which is an analytical method for investigating percolation dynamics on a modular network. Evaluation by simulation showed that graphs in which the number of nodes selected as endpoint nodes of inter-module links and the degrees of the endpoint nodes before the link addition are large have robust connectivity in terms of the point of fragmentation of the network into modules when we fix the degree of the endpoint nodes after the link addition. After the point, the internal structure of modules may matter more. We additionally investigate an applicable range of our proposed method.

Keywords

Percolation, analysis, modular structure, robust connectivity, graph theory

Date received: 30 May 2016; accepted: 2 March 2017

Academic Editor: Valerio Freschi

Introduction

In the context of Internet of Things, various devices, such as sensor nodes or actuator nodes, are deployed all over the world and each subset of them compose a local network. When we consider user's various service demands, these networks are required to cooperate with each other. Therefore, mechanisms for sharing networks as infrastructure are quite important. As a crucial technique for sharing substrates of networks, virtualization of wireless sensor networks (WSNs) has been attracting a great deal of attention.[1] One way of virtualization of WSN is to construct a logically connected overlay network for each application. In a virtualization scenario, multiple sensors in multiple WSNs can be used as shared infrastructure, with some sensors integrated for running each application. The virtualization of WSNs improves manageability and flexibility.

When we integrate local networks, modular structure emerges. A module consists of a group of nodes connected densely by a large number of intra-module links and modules are connected sparsely by a few number of inter-module links. Such modular structure can

[1]Graduate School of Information Science and Technology, Osaka University, Suita, Japan
[2]Graduate School of Economics, Osaka University, Suita, Japan

Corresponding author:
Shinya Toyonaga, Graduate School of Information Science and Technology, Osaka University, Suita 565-0871, Osaka, Japan.
Email: s-toyonaga@ist.osaka-u.ac.jp

be seen in many real networks such as Internet, social networks, or biological networks. An artificial network integrated by interdependent systems is highly vulnerable to targeted attacks or cascading failures and results in fragmentation.[2] In sensor networks, the robustness of the connectivity is a crucial issue because the robust structure of the networks leads to low overhead of maintaining stable services running over them. The study of the way of connecting sensor networks to earn the robustness thus leads to improve the cooperation of deployed sensor devices. Therefore, it is important to investigate effect of modular connection pattern on efficiency of a network, especially robust connectivity.

In our previous work, we proposed a brain-inspired method for constructing a robust and adaptive virtual wireless sensor network (VWSN) topology.[3] We showed that the method of constructing links between modules has crucial effect on robustness and adaptivity of the resulting VWSN topology.[3] However, the best way of constructing a robust and adaptive VWSN topology, and particularly of constructing links between modules, is still unclear. Toward clarifying this, we use an analytical method to study robustness of a topology according to the method of constructing links between modules. Note that we regard a network topology as an undirected graph in analytical theory.

In this article, we use an analytical approach and show the way of connecting modules so that a constructed network has the most robust connectivity. We propose a method to investigate percolation dynamics on a modular network, especially graph ensembles after addition of inter-module links. In consideration of addition of inter-module links, we add a new tool to a binary-dynamics model[4] which is an analytical method for estimating robustness of modular networks.

Our main contribution is that our analytical method considers the link addition and can be applied to make a policy for embedding a new link. Existing studies can be applied only for estimating robustness of given graph ensembles. However, our proposal enables to investigate percolation behavior according to different embedding patterns of inter-module links when a probability distribution of intra-module graph ensembles and that of inter-module link ensembles are given independently. Note that rewiring strategy in which the probability distribution does not change can make the problem for the analytical theory simple. However, link additions are more general than rewiring in the actual environment. Also, our virtual topology construction method proposed in our previous work[3] is composed of constructing intra-module topology and adding inter-module links to connect them. Therefore, in this article, we focus on the link additions for improving our method proposed in our previous work.[3]

Through simulation evaluations, our analytical results are in good agreement with numerical simulations in a configuration model network. Additionally, we show that it is hard to apply our proposal to the graph in which the number of nodes is small because the target of our approach is average properties of random graph ensembles. For the similar reason, we show that the result of analysis cannot completely capture the result of a percolation process on a graph having special structural properties, such as ring-shaped structure.

Related work

Many researchers have studied percolation processes on various types of graphs using a generating function approach. In this type of approach, the expected size of the giant component of a random graph ensemble can be derived from a probability distribution as given by a degree distribution or a distribution of types of links. We can then estimate robustness of a graph by evaluating percolation transitions of the size of the giant component. However, prior studies have focused on estimating robustness of given graph ensembles and not considered changes in graphs, such as link additions.

A generating function approach has been proposed for estimating robust connectivity of random graph ensembles.[5] In this method, the targeted ensemble of random graphs is defined by a generating function $G(x)$, which represents a probability distribution, such as the degree distribution, using an auxiliary variable x. A generating function for the probability distribution of component sizes, denoted by $H(x)$, can then be calculated from $G(x)$. When a giant component exists, we can calculate the size of the giant component by calculating the ratio of nodes that do not belong to the giant component, from $H(x)$. Note that, for commonly used random networks (configuration model), although the size of the giant component is related to the generating function $H(x)$, there is no need to calculate $H(x)$ to obtain the size of the giant component (although it is possible to do so). In the simpler and more straightforward way, it is sufficient to use the generating functions for the degree distribution ($G_0(x)$) and for the excess degree distribution ($G_1(x)$) to calculate the size of the giant component. In this research area, many researchers have studied percolation processes on various types of graphs, such as random graphs,[6] networks of networks,[7] multiplex networks,[8] and interdependent networks.[9] However, the generating function approach is complex because many auxiliary variables and generating functions are necessary, differing according to the complexity of the targeted graphs.

Another important analytical method is a binary-dynamics model for evaluating percolation and other dynamic processes.[4] This method is relatively simple. In this method, the probability distribution of links is used

to obtain the percolation behavior of the network. The probability distribution of links represents modular structure, degree–degree correlation within modules, and degree–degree correlation between modules. The type of the percolation model can be configured by changing the definition of a response function. The detail of the binary-dynamics model is shown in the next section. The binary-dynamics model can be applied to broad classes of graphs by configuring the probability distribution according to the node types or link types.

Almost all existing methods, however, focus on evaluating percolation processes on graph ensembles where a probability distribution is given, and the problem of how to embed links for constructing a robust topology is not examined. Therefore, we propose an analytical method that takes into account changes in the probability distribution due to addition of inter-module links.

Method

Binary-dynamics model

Before we explain our proposal, we explain the binary-dynamics model in detail. For convenience of explanation, we denote the type of a degree-k node belonging to module i by (i,k) and the type of a link that connects (i,k) node with (i',k') node by $\{(i,k),(i',k')\}$. The probability distribution of links is then defined by tensor $[P^{i,i'}_{k,k'}]$ in which each element represents the probability that a randomly chosen link is an $\{(i,k),(i',k')\}$ type link.

In the binary-dynamics model, each node takes one of two states: active or inactive. An inactive node of which a neighboring node is active changes its status to active stochastically. The dynamics of binary state of nodes can be regarded as a percolation process. The probability that an inactive (i,k) node of which m neighboring nodes are active changes status to active is defined by $F_i(m,k)$. $F_i(m,k)$ is called response function. Note that we can change the way of percolation by configuring only $F_i(m,k)$.

In the binary-dynamics model, when the probability that an (i,k) node is active at time step n is denoted by $q^i_k(n)$, the probability that a neighbor node of an inactive (i,k) node is active at time step n is given by

$$\bar{q}^i_k(n) = \frac{\sum_{i',k'} P^{i,i'}_{k,k'} q^{i'}_{k'}(n)}{\sum_{i',k'} P^{i,i'}_{k,k'}} \tag{1}$$

Then, $q^i_k(n)$ is given by

$$\begin{aligned} q^i_k(n+1) &= \rho^i_k(0) + (1-\rho^i_k(0)) \\ &\sum_{m=0}^{k-1} \binom{k-1}{m} \times (\bar{q}^i_k(n))^m (1-\bar{q}^i_k(n))^{k-1-m} F_i(m,k) \\ q^i_k(0) &= \rho^i_k(0) \end{aligned} \tag{2}$$

where $\rho^i_k(0)$ is the ratio of the number of active (i,k) nodes to all (i,k) nodes at the initial step. The ratio of the number of active (i,k) nodes to all (i,k) nodes at step $(n+1)$ is then given by

$$\begin{aligned} \rho^i_k(n+1) = \rho^i_k(0) + (1-\rho^i_k(0)) &\sum_{m=0}^{k} \binom{k}{m} \\ &\times (\bar{q}^i_k(n))^m (1-\bar{q}^i_k(n))^{k-m} F_i(m,k) \end{aligned} \tag{3}$$

From the above, the ratio of the number of active nodes to all nodes at step n, denoted as $\rho(n)$, is given by

$$\rho(n) = \sum_i \frac{\sum_{i',k,k'} \frac{P^{i,i'}_{k,k'}}{k}}{\sum_{i,i',k,k'} \frac{P^{i,i'}_{k,k'}}{k}} \rho^i(n) \tag{4}$$

$$\text{where } \rho^i(n) = \sum_k \frac{\sum_{i',k'} \frac{P^{i,i'}_{k,k'}}{k}}{\sum_{i',k,k'} \frac{P^{i,i'}_{k,k'}}{k}} \rho^i_k(n) \tag{5}$$

In percolation, the ratio of the active nodes to all nodes at which the dynamics (i.e. the iterative calculation of equations (1), (2), and (4)) converge describes the size of the giant component. Thus, $\rho(n)$ for $n \to \infty$ describes the size of the giant component consisting of active nodes when the dynamics converge.

It is true that $P^{i,i'}_{k,k'}$ for the newly created network can be easily calculated, given the adjacency matrix of the network after inter-module links addition. However, the $P^{i,i'}_{k,k'}$ derived from an adjacent matrix after inter-module links addition denotes only one example, and we only get the robustness of the adjacent matrix. In this strategy, we need to try the whole connection patterns of inter-module links to make topology robust and it is only one result in the situation. This can result in tremendous overhead. In contrast, our method can get the expected robustness of the topology classified according to the strategy of inter-module links addition. Then, our approach narrows the candidates of the link addition strategy to get the robust topology with low overhead when the number of nodes is large. Therefore, our approach can show the policy to make topology robust according to the link addition strategy.

Deriving link probability distribution after addition of inter-module links

To investigate differences in robustness depending on the connection patterns between modules using the binary-dynamics model, we analyze site percolation when the connection patterns between modules are changed and the probability distribution of links within each module is given. However, we need to consider the

change in the probability distribution of links within each module according to addition of inter-module links.

In this article, we consider that two previously isolated modules are connected by newly created a fixed number of inter-module links, and that these links connect a number of nodes with a fixed degree k in module i to a number of nodes with a fixed degree k' in module i' such that the degrees of nodes that receive the inter-module links are raised from k to d or from k' to d'.

First, we define tensor $[Prev^{i,i}_{a,b}]$ in which each element represents the probability that a randomly chosen edge is present in the network and connects a degree-a node to a degree-b node both located in module i. It is actually the probability distribution of links considering the newly added inter-module links but also neglecting the new degrees of the boundary nodes. Because we use the probability distribution of links between modules as the target value, we define tensor $[Target^{i,i'}_{a,b}]$ in which each element represents the probability that a randomly chosen link is an $\{(i,a),(i',b)\}$ type link. Because tensor $[Prev^{i,i}_{a,b}]$ is for intra-module links and tensor $[Target^{i,i'}_{a,b}]$ is for inter-module links, the conditions of equation (6) are satisfied

$$\begin{aligned} Prev^{i,i'}_{a,b} &= 0, \text{ for } i \neq i' \\ Target^{i,i'}_{a,b} &= 0, \text{ for } i = i' \end{aligned} \tag{6}$$

We define T_{intra} as the number of links within modules and T_{inter} as the number of links between modules. Then, we configure the tensors so as to satisfy the following equations

$$\begin{aligned} &\sum_{i,a,b} Prev^{i,i}_{a,b} + \sum_{i,i',a,b} Target^{i,i'}_{a,b} = 1 \\ &\sum_{i,a,b} Prev^{i,i}_{a,b} : \sum_{i,i',a,b} Target^{i,i'}_{a,b} = T_{intra} : T_{inter} \end{aligned} \tag{7}$$

We consider the conditions specified by equations (6) and (7) to calculate the probability distribution of links after addition of inter-module links, denoted by tensor $[Sub^{i,i'}_{a,b}]$, using $[Prev^{i,i'}_{a,b}]$ and $[Target^{i,i'}_{a,b}]$. Therefore, $Sub^{i,i'}_{a,b}$ is given by

$$Sub^{i,i'}_{a,b} = \begin{cases} Prev^{i,i'}_{a,b} + \Delta Prev^{i,i'}_{a,b} & \text{where } i = i' \\ Target^{i,i'}_{a,b} & \text{otherwise} \end{cases} \tag{8}$$

where $\Delta Prev^{i,i'}_{a,b}$ denotes the amount of change in the probability distribution of links, which is what we need to calculate. Then, we use $Sub^{i,i'}_{a,b}$ instead of $P^{i,i'}_{k,k'}$ in equations (1), (4), and (5) for analysis.

In this article, we consider the case that the number of modules is two and the number of types of inter-module links is one. When the type of inter-module links is $\{(i,d),(i',d')\}$, it gives the following equation

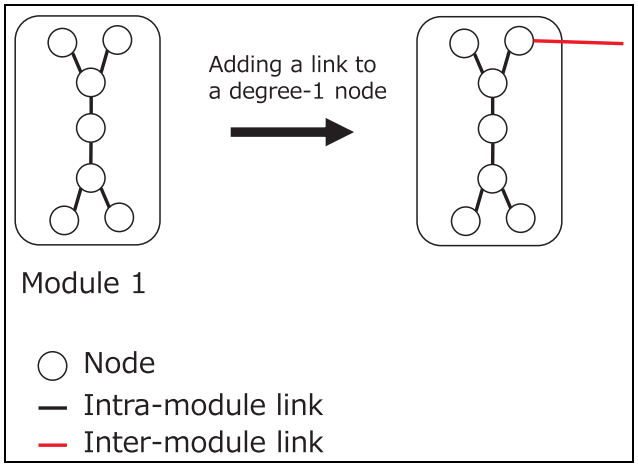

Figure 1. Example of inter-module link addition.

$$Target^{i,i'}_{a,b} = \begin{cases} \frac{T_{inter}}{T_{intra} + T_{inter}} & \text{where } a = d, b = d' \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

Focusing on module i, if we consider that the degree resulting from the addition of inter-module links is d, then we add $(d-k)$ links to some (i,k) nodes. Then, $Sub^{i,i}_{k,b}$ is smaller than or equal to $Prev^{i,i}_{k,b}$, and $Sub^{i,i}_{a,k}$ is smaller than or equal to $Prev^{i,i}_{a,k}$. Simultaneously, $Sub^{i,i}_{d,b}$ is larger than or equal to $Prev^{i,i}_{d,b}$ and $Sub^{i,i}_{a,d}$ is larger than or equal to $Prev^{i,i}_{a,d}$. These relations can be hold because we first configure $Prev^{i,i}_{a,b}$ and $Target^{i,i'}_{a,b}$ so as to satisfy equations (7). This configuration enables us to assume that some amount of the probability of $Prev^{i,i}_{a,k}$ ($Prev^{i,i}_{k,b}$) moves to $Prev^{i,i}_{a,d}$ ($Prev^{i,i}_{d,b}$) when the inter-module links are added in the way mentioned above because some degree-k nodes change to degree-d nodes.

For example, we assume we use the topology shown in Figure 1 and add an inter-module link to a degree-1 node. In this example, $Prev^{1,1}_{a,b}$, $Target^{1,2}_{a,b}$, and $Sub^{1,1}_{a,b}$ are shown in equations (10), (11), and (12), respectively. b' in equation (11) is some constant value. Then, we need to derive equation (12) from equations (10) and (11)

$$b = 1,2,3 \qquad Prev^{1,1}_{a,b} = \frac{1}{26}\begin{pmatrix} 0 & 0 & 4 \\ 0 & 0 & 2 \\ 4 & 2 & 0 \end{pmatrix} \begin{matrix} a=1 \\ a=2 \\ a=3 \end{matrix} \tag{10}$$

$$Target^{1,2}_{a,b} = Target^{2,1}_{b,a} = \begin{cases} \frac{1}{26} & \text{where } a = 2, b = b' \\ 0 & \text{otherwise} \end{cases} \tag{11}$$

$$b = 1,2,3 \qquad Sub^{1,1}_{a,b} = \frac{1}{26}\begin{pmatrix} 0 & 0 & 3 \\ 0 & 0 & 3 \\ 3 & 3 & 0 \end{pmatrix} \begin{matrix} a=1 \\ a=2 \\ a=3 \end{matrix} \tag{12}$$

Next, we define the magnitude of influence by link addition. Here, the magnitude of influence means the ratio of the number of intra-module links which change their type because of the change in degree of their endpoint nodes. The magnitude of influence by link addition to a degree-k node is k times as large as that by link addition to a degree-1 node because the number of links changing their type is proportional to the degree of the node that receives the inter-module links. Also, the magnitude of influence by addition of $(d-k)$ links to a degree-k node is $1/(d-k)$ times as large as that by addition of one link to a degree-k node because the number of links changing their type is proportional to the inverse of the number of links added to one node. Therefore, in the case when the number of created inter-module links is fixed and these inter-module links are connected only to nodes with a fixed degree k such that their degree is raised to d, we can define the magnitude of influence by adding $(d-k)$ links to some degree-k nodes, denoted by $Inf(d,k)$, as follows

$$Inf(d,k) = H(d-k)\frac{k}{(d-k)}Target^{i,i'}_{d,d'} \tag{13}$$

where H is the Heaviside step function. As the networks considered here have only two modules and also as just one fixed value of d and d' is considered, $Target^{i,i'}_{d,d'}$ represents only one scalar quantity.

Moreover, when we add some links to a degree-k node, the probability that degree of its neighbor is k' is $Prev^{i,i}_{k,k'}/\sum_{k'} Prev^{i,i}_{k,k'}$. When we consider the above, the amount of change in the probability distribution of links, denoted by $\Delta Prev^{i,i}_{a,b}(d,k)$, can be calculated by the following equations

$$\begin{aligned}\Delta Prev^{i,i}_{a,b}(d,k) = & -\delta_{a,k}\frac{Prev^{i,i}_{k,b}}{\sum_{k'} Prev^{i,i}_{k,k'}}\cdot Inf(d,k)\\ & -\delta_{b,k}\frac{Prev^{i,i}_{a,k}}{\sum_{k'} Prev^{i,i}_{k,k'}}\cdot Inf(d,k)\\ & +\delta_{a,d}\frac{Prev^{i,i}_{k,b}}{\sum_{k'} Prev^{i,i}_{k,k'}}\cdot Inf(d,k)\\ & +\delta_{b,d}\frac{Prev^{i,i}_{a,k}}{\sum_{k'} Prev^{i,i}_{k,k'}}\cdot Inf(d,k)\end{aligned} \tag{14}$$

where δ is the Kronecker delta function.

When we calculate $\Delta Prev^{1,1}_{a,b}(2,1)$ for the example shown in Figure 1, $\Delta Prev^{1,1}_{1,3}(2,1) = \Delta Prev^{1,1}_{3,1}(2,1) = -1/26$, $\Delta Prev^{1,1}_{2,3}(2,1) = \Delta Prev^{1,1}_{3,2}(2,1) = 1/26$, and the others equal to zero. This is consistent with equation (12). In another example shown in Figure 2, we can get different probability distributions according to the connected node. We assume an inter-module link is added to a degree-1 node. $Prev^{1,1}_{a,b}$ and $Target^{1,2}_{a,b}$ are

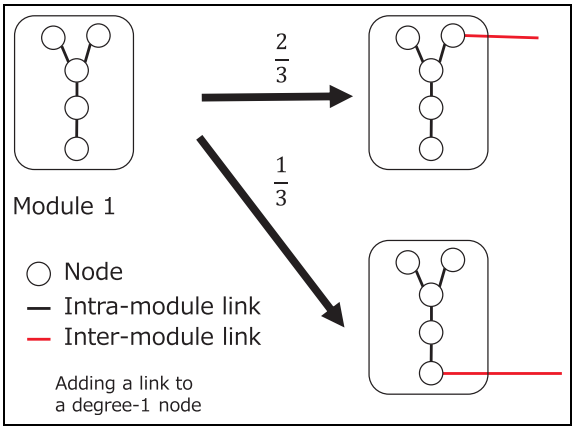

Figure 2. Example of link addition in which different probability distributions arise according to the connected node.

shown in equations (15) and (16), respectively. b' in equation (16) is some constant value. In this case, $\{(1,1),(1,3)\}$ link changes its type to $\{(1,2),(1,3)\}$ and $\{(1,3),(1,1)\}$ link changes its type to $\{(1,3),(1,2)\}$ with probability 2/3. Also, $\{(1,1),(1,2)\}$ link changes its type to $\{(1,2),(1,2)\}$ and $\{(1,2),(1,1)\}$ link changes its type to $\{(1,2),(1,2)\}$ with probability 1/3. $Sub^{1,1}_{a,b}$ is shown in equation (17) for the former case and in equation (18) for the latter case. We average them and can obtain the expected probability distribution shown in equation (19). When we calculate $\Delta Prev^{1,1}_{a,b}(2,1)$ for this example, the result is consistent with equation (19)

$$b = 1,2,3,\quad Prev^{1,1}_{a,b} = \frac{1}{18}\begin{pmatrix}0 & 1 & 2\\ 1 & 0 & 1\\ 2 & 1 & 0\end{pmatrix}\begin{matrix}a=1\\ a=2\\ a=3\end{matrix} \tag{15}$$

$$Target^{1,2}_{a,b} = Target^{2,1}_{b,a} = \begin{pmatrix}\frac{1}{18} & \text{where } a=2, b=b'\\ 0 & \text{otherwise}\end{pmatrix} \tag{16}$$

$$b = 1,2,3\quad Sub^{1,1}_{a,b} = \frac{1}{18}\begin{pmatrix}0 & 1 & 1\\ 1 & 0 & 2\\ 1 & 2 & 0\end{pmatrix}\begin{matrix}a=1\\ a=2\\ a=3\end{matrix} \tag{17}$$

$$b = 1,2,3\quad Sub^{1,1}_{a,b} = \frac{1}{18}\begin{pmatrix}0 & 0 & 2\\ 0 & 2 & 1\\ 2 & 1 & 0\end{pmatrix}\begin{matrix}a=1\\ a=2\\ a=3\end{matrix} \tag{18}$$

$$b = 1,2,3\quad Sub^{1,1}_{a,b} = \frac{1}{54}\begin{pmatrix}0 & 2 & 4\\ 2 & 2 & 5\\ 4 & 5 & 0\end{pmatrix}\begin{matrix}a=1\\ a=2\\ a=3\end{matrix} \tag{19}$$

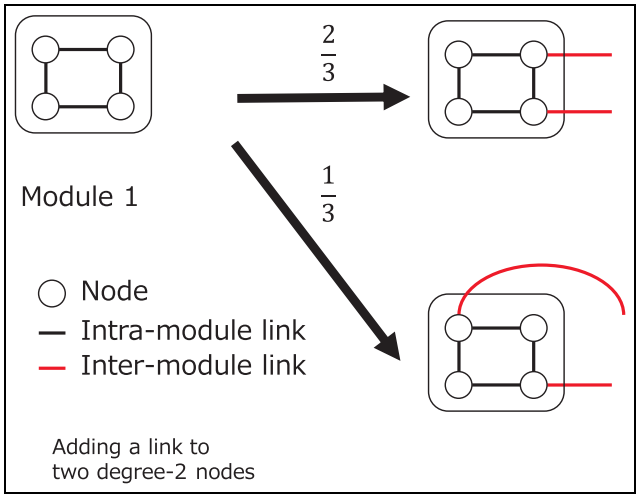

Figure 3. Example of multiple links addition in which different probability distributions arise according to the connected node.

However, the case of adding links to multiple nodes is not considered in equation (14) because the equation cannot describe the change in link type from $\{(i,k),(i,k)\}$ to $\{(i,d),(i,d)\}$ even though it can describe the change from $\{(i,k),(i,b)\}$ to $\{(i,d),(i,b)\}$ and from $\{(i,a),(i,k)\}$ to $\{(i,a),(i,d)\}$. Our method cannot be directly applied to the example shown in Figure 3. We assume two inter-module links are added to two degree-2 nodes, respectively. In this example, $Prev^{1,1}_{a,b}$ and $Target^{1,2}_{a,b}$ are shown in equations (20) and (21), respectively. b' in equation (21) is some constant value. The expected probability distribution after inter-module link addition is shown in equation (22). When we calculate $\Delta Prev^{1,1}_{a,b}(3,2)$ for this example, equation (23) is derived and $Sub^{1,1}_{3,3}$ remains zero

$$Prev^{1,1}_{a,b} = \frac{1}{20}\begin{pmatrix} 8 & 0 \\ 0 & 0 \end{pmatrix} \begin{matrix} a=2 \\ a=3 \end{matrix} \quad \begin{matrix} b=2,3 \end{matrix} \tag{20}$$

$$Target^{1,2}_{a,b} = Target^{2,1}_{b,a} = \begin{cases} \frac{2}{20} & \text{where } a=3, b=b' \\ 0 & \text{otherwise} \end{cases} \tag{21}$$

$$Sub^{1,1}_{a,b} = \frac{1}{60}\begin{pmatrix} 4 & 8 \\ 8 & 4 \end{pmatrix} \begin{matrix} a=2 \\ a=3 \end{matrix} \quad \begin{matrix} b=2,3 \end{matrix} \tag{22}$$

$$Sub^{1,1}_{a,b} = \frac{1}{20}\begin{pmatrix} 0 & 4 \\ 4 & 0 \end{pmatrix} \begin{matrix} a=2 \\ a=3 \end{matrix} \quad \begin{matrix} b=2,3 \end{matrix} \tag{23}$$

This problem can be solved by replacing $Inf(d,k)$ with $Inf(d,k)/M^i_k(d)$ and applying equation (14) $M^i_k(d)$ times with recalculating $[Prev^{i,i}_{a,b}]$ each time, where $M^i_k(d)$ is the number of (i,k) nodes selected as boundary nodes (i.e. endpoint nodes of inter-module links) and connected by $(d-k)$ inter-module links. This configuration enables our method to derive equation (22) for the example shown in Figure 3.

To calculate $M^i_k(d)$, we calculate the total number of inter-module links between (i,d) nodes and (i',d') nodes after the link addition, denoted by $M^{i,i'}_{d,d'}$. This is given as follows

$$\begin{aligned} M^{i,i'}_{d,d'} &= \frac{1}{2} Nz_{prev} \frac{(Target^{i,i'}_{d,d'} + Target^{i',i}_{d',d})}{\sum_{i,i',a,b} Prev^{i,i'}_{a,b}} \\ &= Nz_{prev} \frac{Target^{i,i'}_{d,d'}}{\sum_{i,i',a,b} Prev^{i,i'}_{a,b}} \end{aligned} \tag{24}$$

where N is the total number of nodes and z_{prev} is the average degree of the graph before adding inter-module links. For this, z_{prev} equals $\sum_{i,k} kp^i_k$ where p^i_k is the ratio of the number of (i,k) nodes to the total number of nodes before the inter-module link additions and can be calculated as follows

$$p^i_k = \frac{\sum_b \frac{Prev^{i,i}_{k,b}}{k}}{\sum_{i,i',a,b} \frac{Prev^{i,i'}_{a,b}}{a}} \tag{25}$$

Note that $(1/2)Nz_{prev}$ describes the total number of intra-module links and $(Target^{i,i'}_{d,d'} + Target^{i',i}_{d',d})/\sum_{i,a,b} Prev^{i,i}_{a,b}$ describes the ratio of the number of inter-module links that connect degree-d nodes from one module to degree-d' nodes of another module to the number of intra-module links. The second equality in equation (24) is satisfied because our target is an undirected graph. When we add all inter-module links to some degree-k nodes and add $(d-k)$ inter-module links to each of them, $M^i_k(d)$ can be calculated by the following equation

$$M^i_k(d) = \frac{M^{i,i'}_{d,d'}}{d-k} \tag{26}$$

Therefore, when the expected total number of nodes is given, $M^i_k(d)$ can be calculated.

Constraints of input variables

In our approach, $[Target^{i,i'}_{k,k'}]$ needs to satisfy some constraints. First, the number of endpoint (i,k) nodes of inter-module links must be less than the number of (i,k) nodes. Second, the number of endpoint (i,k) nodes of inter-module links must be more than $(d'-k')$ and the number of endpoint (i',k') nodes of inter-module links must be more than $(d-k)$ because we assume that

multiple links between a pair of nodes are not allowed. Therefore, the constraints can be described as follows

$$\begin{aligned}(d'-k') &\le M_k^i(d) \le Np_k^i \\ (d-k) &\le M_{k'}^{i'}(d') \le Np_{k'}^{i'}\end{aligned} \tag{27}$$

We can rewrite the above into a constraint on $Target_{d,d'}^{i,i'}$ as follows

$$\begin{aligned}(d-k)(d'-k')\frac{\sum_{i,a,b} Prev_{a,b}^{i,i}}{N\, z_{prev}} &\le Target_{d,d'}^{i,i'} \\ &\le \min\left((d-k)p_k^i, (d'-k')p_{k'}^{i'}\right)\frac{\sum_{i,a,b} Prev_{a,b}^{i,i}}{z_{prev}}\end{aligned} \tag{28}$$

Because the lower bound depends on N, there are cases where the desired graph cannot be constructed if N is small.

Simulation evaluation

We investigate robustness according to the connection patterns of inter-module links using our proposed method. To evaluate validity of our proposal, we compare the analysis results with the numerical results. In numerical simulations, we evaluate the site percolation process on a graph constructed by a configuration model according to $[Prev_{a,b}^{i,i}]$, $[Target_{a,b}^{i,i'}]$, and N.

The method for constructing a graph based on $[Prev_{a,b}^{i,i}]$, $[Target_{a,b}^{i,i'}]$, and N is listed as follows:

1. Constructing a graph within each module
   (a) Calculating a degree distribution of each module from $[Prev_{a,b}^{i,i}]$ and assigning degree to each node;
   (b) Calculating the number of each type of intra-module links from $[Prev_{a,b}^{i,i}]$ and N;
   (c) Selecting a pair of endpoint nodes of each intra-module link from the candidates at random and connecting them.
2. Adding inter-module links
   (a) Calculating the number of the specified type of inter-module links from the ratio of T_{inter} to T_{intra};
   (b) Determining a set of the candidates for the boundary nodes at random according to the connection pattern of inter-module links;
   (c) Selecting a pair of boundary nodes of each inter-module link from the candidates at random and connecting them.

In numerical simulations, we assume that inactive nodes are failed nodes.

Percolation on graph ensembles with a given probability distribution

Simulation settings. We assume that the number of modules is two and the probability distributions of intra-module and inter-module links are given by equations (29) and (30), respectively. Equation (29) describes that the degree distribution of each module is uniform. In this case, the ratio of the number of intra-module links to inter-module links is 200 to 3. The expected total number of nodes is 1000 when we analyze the percolation process using our proposed method. We analyze the site percolation process with various combinations of d, d', k, and k'

$$\begin{aligned}&b = 2,\quad 3,\quad 4,\quad 5,\quad 6 \\ &Prev_{a,b}^{i,i} = \frac{1}{812}\begin{pmatrix} 4 & 6 & 8 & 10 & 12 \\ 6 & 9 & 12 & 15 & 18 \\ 8 & 12 & 16 & 20 & 24 \\ 10 & 15 & 20 & 25 & 30 \\ 12 & 18 & 24 & 30 & 36 \end{pmatrix} \begin{matrix} a=2 \\ a=3 \\ a=4 \\ a=5 \\ a=6 \end{matrix}\end{aligned} \tag{29}$$

$$Target_{a,b}^{1,2} = Target_{b,a}^{2,1} = \begin{pmatrix} \frac{6}{812} & \text{where } a=d, b=d' \\ 0 & \text{otherwise} \end{pmatrix} \tag{30}$$

In the percolation process, we use two modes of node removal: random failure and targeted attack. In random failure mode, a removal node is selected uniformly at random, while in targeted attack mode, a removal node is selected in order of decreasing degree. We then define a response function for each node removal mode in order to analyze the site percolation process using our method. In the binary-dynamics model,[4] the response function for the site percolation is defined as follows

$$F_i(m,k) = \begin{pmatrix} 0 & \text{where } m=0 \\ Q_k^i & \text{otherwise} \end{pmatrix} \tag{31}$$

where Q_k^i is the occupation probability of (i,k) nodes. When we assume $(1-p)$ of all nodes have failed, then Q_k^i is defined by equation (32) for random failure mode[4] and by equation (33) for targeted attack mode

$$Q_k^i = p \tag{32}$$

$$Q_k^i = \begin{cases} 1 & \text{where } \sum_{l=1}^{k}\sum_i \phi_l^i \le p \\ \dfrac{p-\sum_{l=1}^{k-1}\sum_i \phi_l^i}{\sum_i \phi_k^i} & \text{where } \left(\sum_{l=1}^{k-1}\sum_i \phi_l^i < p < \sum_{l=1}^{k}\sum_i \phi_l^i\right) \\ 0 & \text{otherwise} \end{cases} \tag{33}$$

where ϕ_l^i is the ratio of the number of (i, l) nodes to the total number of nodes after the inter-module links addition and can be calculated from $Sub_{a,b}^{i,i'}$. $\sum_{l=1}^{k-1} \sum_i \phi_l^i$ describes the ratio of the number of nodes that have lower degree than k to the total number of nodes. Therefore, the first line of equation (33) means that all nodes that have lower degree relative to the value of p are occupied. The second line means that degree-k nodes are occupied with the probability which equals to the ratio of active degree-k nodes to all degree-k nodes. The third line means that all nodes that have higher degree relative to the value of p are not occupied.

Here, we consider that analytical results are obtained by iterative calculation of equations (1), (2), and (4).

Analysis of percolation in random failure mode. The results of analysis in random failure mode are shown in Figure 4. We evaluate the percolation with various combinations of d, d', k, and k'. The results for the case of $d = 5$ and $d' = 5$ are shown in Figure 4(a) and the results for the case of $d = 7$ and $d' = 7$ are shown in Figure 4(b). Each legend shows the connection pattern of inter-module links and formatted as i-k-(d-k)_i'-k'-($d' - k'$). In each figure, the horizontal axis shows the ratio of the failed nodes, denoted by $(1 - p)$, and the vertical axis shows the size of the giant component. We assume that the ranking of the robustness of networks is equivalent to the ranking of the size of the giant component at each p value.

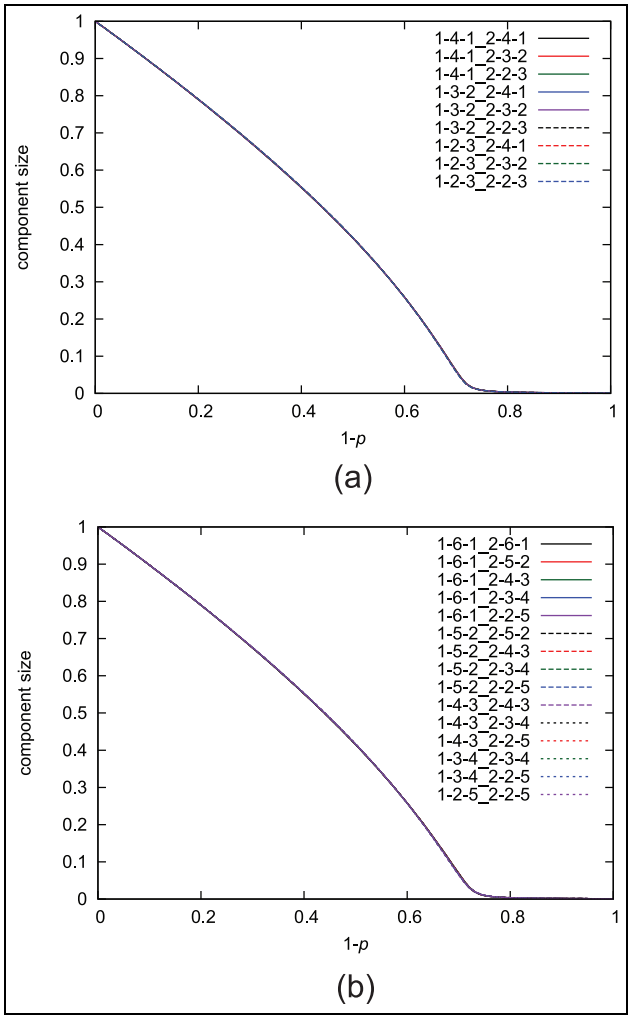

Figure 4. Analytical results of percolation analysis in random failure mode: (a) $d = 5, d' = 5$ and (b) $d = 7, d' = 7$.

As shown in Figure 4, there is little difference depending on the connection pattern of inter-module links in random failure mode.

To evaluate validity of our analytical results shown in Figure 4, we construct a graph with the number of nodes set at 1000 and investigate the site percolation process on it in random failure mode. The number of trials is 500. Figure 5 shows the results of the site percolation process in random failure mode with k and k' fixed. Each figure shows that there is little difference but the graph in which the number of boundary nodes is small has a slightly more vulnerable structure. Because the graph is divided into modules when the boundary nodes are removed, the graph in which the number of boundary nodes is large has a slightly more robust connectivity.

To compare the graphs in which the number of boundary nodes is the same, we show the results of the site percolation process in random failure mode with $(d - k)$ and $(d' - k')$ fixed in Figure 6. There are small differences in each of the figures even though the number of boundary nodes is the same. This difference arises from differences in the number of neighbors of boundary nodes. Because the graph is divided and isolated when all neighbors of boundary nodes are removed, the graph in which the average number of intra-modular connections of the boundary nodes is large has a slightly more robust connectivity.

Analysis of percolation in targeted attack mode. The results of analysis in targeted attack mode are shown in Figure 7. The results for the case of $d = 5$ and $d' = 5$ are shown in Figure 7(a) and the results for the case of $d = 7$ and $d' = 7$ are shown in Figure 7(b).

In Figure 7(a), all results show that the size of the giant component decreases sharply at $(1 - p) \simeq 0.4$ and there is little difference between them. Because nodes are removed in order of decreasing degree, all degree-6 and degree-5 nodes are removed when $(1 - p)$ is larger than 0.4. In this evaluation, the fragmentation of a graph within a module occurs before the removal of all inter-module links because d and d' are set to 5.

In Figure 7(b), every result shows a phase transition at small $(1 - p)$ value, and the size of the giant component decreases gradually after that. In this evaluation, a

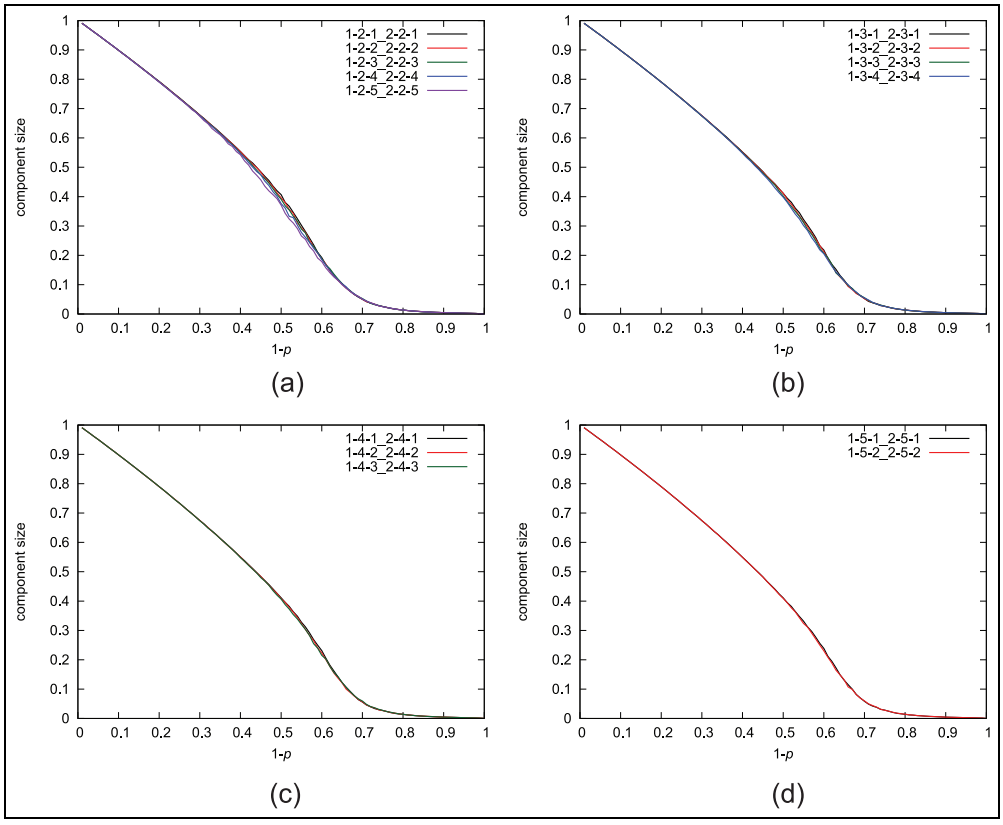

Figure 5. Numerical results of the site percolation process on graphs in random failure mode with k and k' fixed: (a) $k = 2, k' = 2$, (b) $k = 3, k' = 3$, (c) $k = 4, k' = 4$, and (d) $k = 5, k' = 5$.

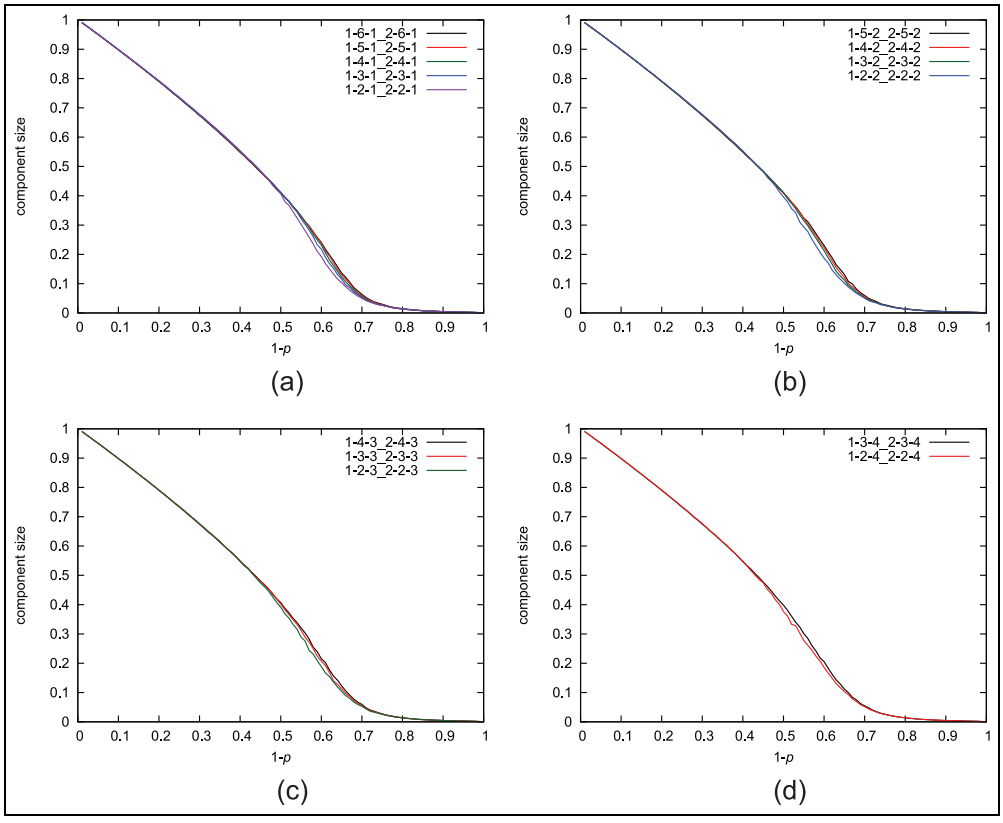

Figure 6. Numerical results of the site percolation process on graphs in random failure mode with $(d - k)$ and $(d' - k')$ fixed: (a) $d - k = 1, d' - k' = 1$, (b) $d - k = 2, d' - k' = 2$, (c) $d - k = 3, d' - k' = 3$, and (d) $d - k = 4, d' - k' = 4$.

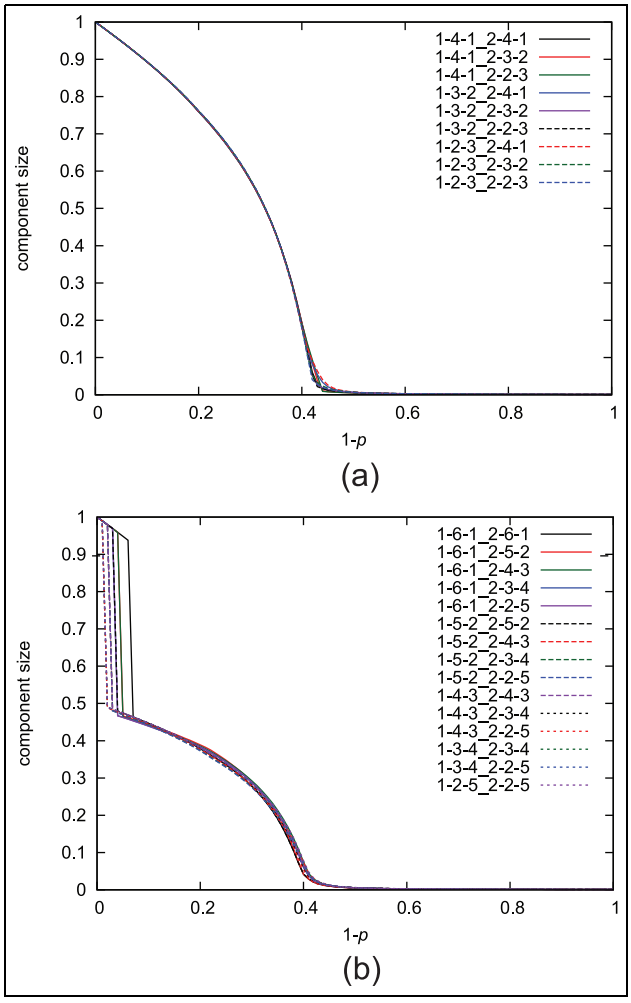

Figure 7. Analytical results of percolation analysis in targeted attack mode: (a) $d = 5, d' = 5$ and (b) $d = 7, d' = 7$.

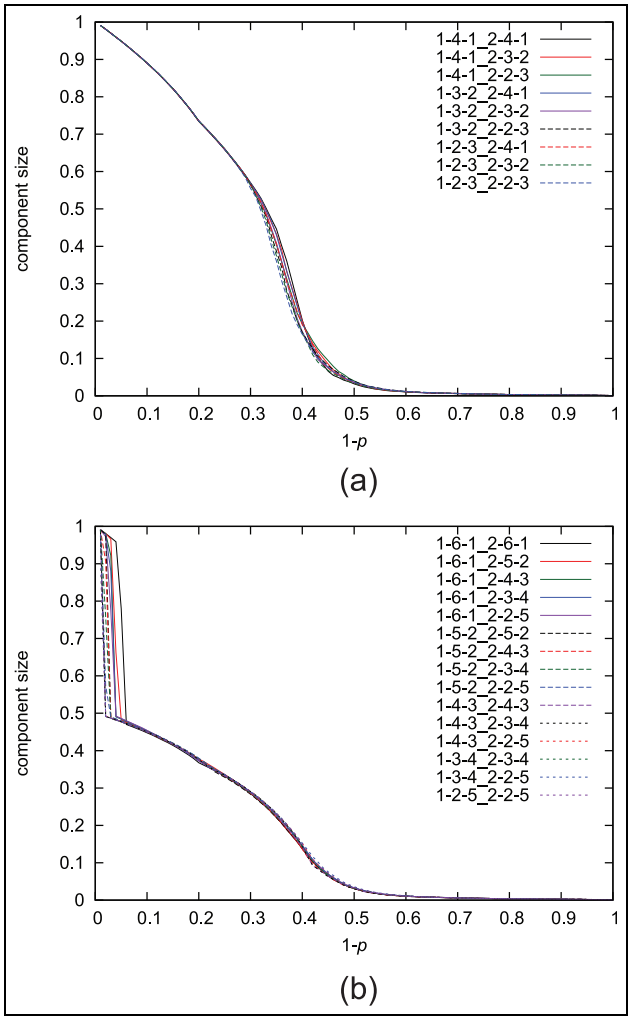

Figure 8. Numerical results of the site percolation process on graph in targeted attack mode: (a) $d = 5, d' = 5$ and (b) $d = 7, d' = 7$.

phase transition indicates the division of the graph into modules by removal of all inter-module links. Because the maximum degree is 7 when d and d' equal 7, connectivity of the graph makes it vulnerable to targeted attack. In addition, robustness of connectivity is different according to k and k'. The larger $M_k^i(d)$ means the graph has more robust connectivity for small $(1-p)$ values because modules are connected until removal of all (i,d) or (i',d') nodes. In this evaluation, because all $(1,7)$ nodes and all $(2,7)$ nodes are the boundary nodes and a removal node is selected uniformly and randomly from degree-7 nodes at small $(1-p)$, the larger $(M_k^1(7) + M_{k'}^2(7))$ means the graph has more robust connectivity for small $(1-p)$ values. Therefore, the graph with larger $(1/(d-k) + 1/(d-k'))$ has more robust connectivity in terms of the point at which the network fragments into two modules. But for large $(1-p)$ values, the network robustness is not significantly different for networks with different $M_k^i(d)$ values. For such $(1-p)$ values, parameters of the intra-modular structure determine the slight differences between the sizes of the giant component for different networks exemplified. Note that the targeted attack we use in this evaluation is based on the nodes' degrees. This means these results can be different according to the definition of Q_k^i.

To evaluate validity of our analytical results showed in Figure 7, we construct a graph with the number of nodes set at 1000 and investigate the site percolation process on it in targeted attack mode. The number of trials is 500. Figure 8 shows the results of the site percolation process in targeted attack mode. By comparison with Figure 7, although the giant component size in each method is slightly different, the order of robustness of each connection pattern is the same. From these results, analytical results are in good agreement with numerical results and the graph in which the number of boundary nodes is large has more robust connectivity

for small $(1 - p)$ values when we use the targeted attack mode in which a removal node is selected in order of decreasing degree. After the fragmentation of the network, the network robustness is not significantly different for networks with different $M_k^i(d)$ values.

Applicable range of our proposed method. When we consider the IoT environment, there may be cases where the number of nodes belonging to each module is large. Given this context, we need to investigate the applicable range of our proposed method for making policies according to the results of analysis.

To show the applicable range of our proposed method, we compare the results of analysis to the results of the percolation process on the graph when the number of nodes is one of 100, 200, 500, 1000, 10,000 and 20,000, respectively. We use the method of 1-6-1_2-6-1 as an example, the number of trials is 100, and the expected number of nodes for analysis is 1000.

Figure 9(a) shows the results in random failure mode and Figure 9(b) shows the results in targeted attack mode. Both show that difference between analytical and numerical results becomes larger as the number of nodes becomes smaller. This means that it is hard to apply our proposal to a graph in which the number of nodes is small because our approach derives average properties of random graph ensembles. However, such a small graph can be analyzed by numerical simulations. Therefore, this is not a problem for our proposal whose target is the graphs in which the number of nodes is large.

In Figure 9(b), however, the results of analysis cannot completely capture any of the numerical results. In this evaluation, degree-7 nodes are 6% of the total nodes and half of them belong to module 1 and the rest belong to module 2. In the analysis method, the selection of a removal node is regarded as completely uniform. This means that the graph is not divided into modules until all degree-7 nodes are removed. In the numerical simulations, however, the graph can be divided into modules when half of degree-7 nodes are removed because removal of all degree-7 nodes belonging to module 1 or 2 results in fragmentation of the graph. Therefore, the numerical results show a phase transition at an earlier stage than the analysis. In addition, Figure 9(b) shows that a graph with a small number of nodes becomes vulnerable because the number of degree-7 nodes is small and the graph fragments easily.

The analytical results cannot completely capture any of the numerical results in targeted attack mode because of the reasons described above. The result for 10,000 nodes is almost the same as for 20,000 nodes, which means that the difference between numerical and analytical results cannot get any closer. Because this difference comes from the difference of an order of node that fails in the numerical simulation, the way that nodes fail is also an important factor which determines whether analytic results completely capture numerical results or not.

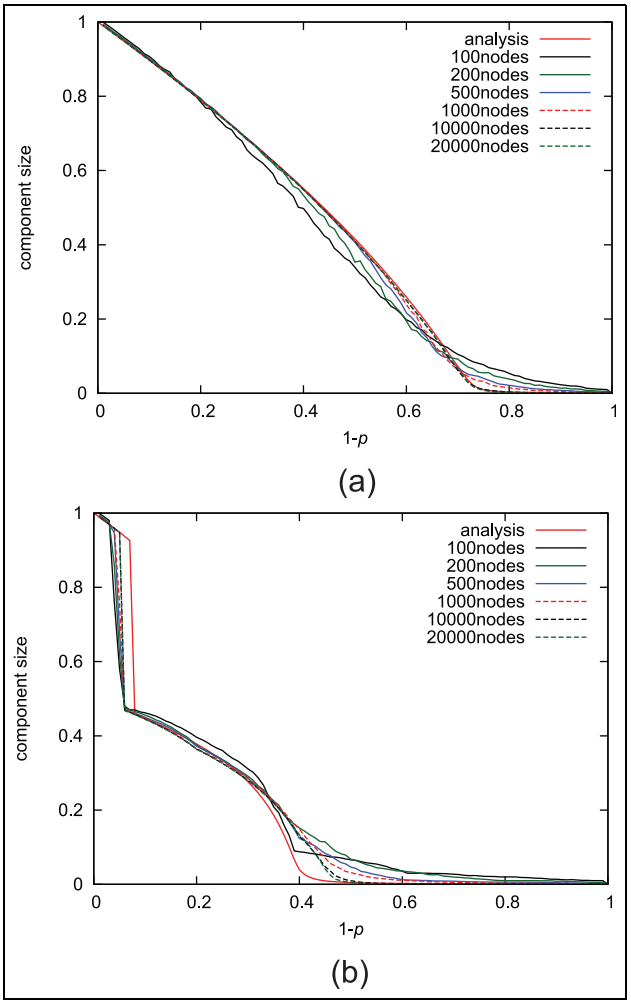

Figure 9. Comparison of the analytical and numerical results: (a) random failure mode and (b) targeted attack mode.

Percolation on graph ensembles with a probability distribution derived from a given intra-module topology

The results shown above are obtained when we first give a probability distribution and investigate the site percolation process on a graph constructed by the configuration model to evaluate validity of our proposed method. When we consider an actual situation, however, we need to show a policy to make a graph robust by connecting multiple existing networks.

Table 1. Parameters for constructing a topology within a module.

Model	Parameter	Value
ER	$p_{(ER)}$	0.012
BA	$m_{0(BA)}$	7
	$m_{(BA)}$	6
WS	$m_{(WS)}$	6
	$\beta_{(WS)}$	0.01

ER model: Erdős–Rényi model; BA model: Barabási–Albert model; WS model: Watts–Strogatz model.

Simulation settings. In this part, we investigate robustness of a graph in which modules are constructed by Erdős–Rényi (ER) model, Barabási–Albert (BA) model, and Watts–Strogatz (WS) model,[10] respectively. We use the parameters shown in Table 1 for constructing a module. Using these parameters, the expectation of the average degree in a module is 6 when the number of nodes in a module is 500. The number of modules is two, the number of nodes in a module is 500, and the number of links added between modules is 1% of the total number of links within modules. We compare the numerical results for the site percolation process on a graph constructed by modules and inter-module link, with the analytical results using the probability distribution obtained from existing modules.

Results using ER model. The numerical and analytical results for the random failure mode in a network composed of ER modules are shown in Figure 10. The number of trials for numerical simulations in each topology is 100. The minimum degree within a module is 1 and the maximum degree within a module is 15.

The numerical and analytical results for the case of $d = 7$ and $d' = 7$ are shown in Figure 10(a) and (b), respectively. All of them are consistent with the results shown above. For the random failure mode, the analytical results depend only slightly on the connection pattern of inter-module links. In numerical results, the graph in which the number of boundary nodes is small has a slightly vulnerable structure.

When we use the ER model for constructing a topology within a module, the numerical and analytical results in targeted attack mode are shown in Figure 11. The results in Figure 11(b) are consistent with the results shown above in terms of the first sudden decay of the size of the giant component. After the fragmentation of the network, the ranking of the size of the giant component changes. This is because the connectivity of the intra-module network remains high after the fragmentation when k (or k') is set to small value. When we set k and d to 6 and 7, respectively, little number of degree-6 nodes remain after all degree-7

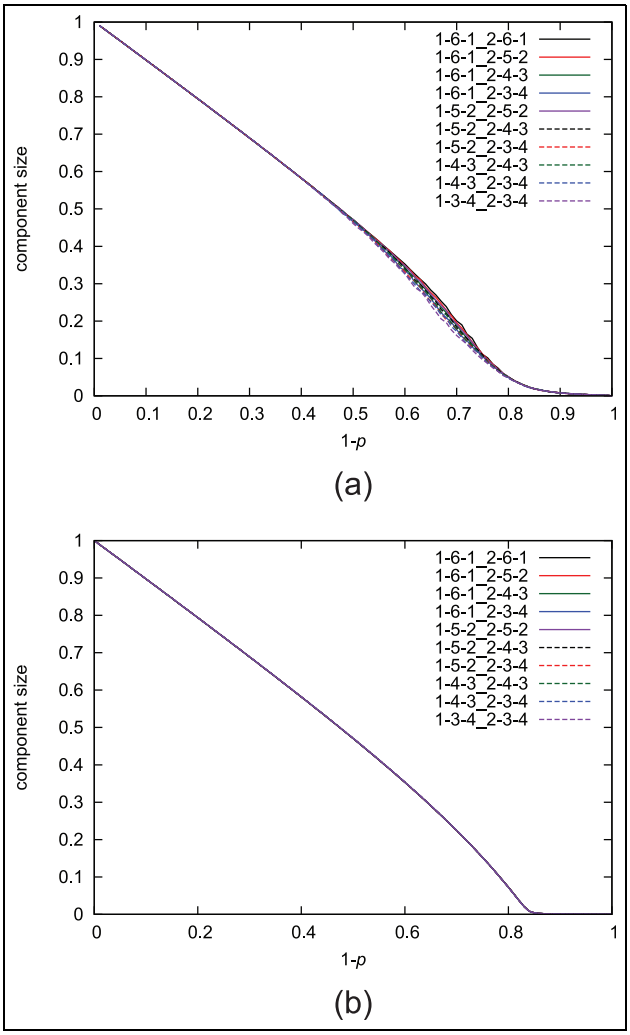

Figure 10. The results in random failure mode (ER model): (a) numerical and (b) analytical results.

nodes are removed, and degree-6 nodes are crucial for the connectivity of the intra-module because of their high degrees. This leads to the vulnerable connectivity of intra-module network after the fragmentation. In most of the results of Figure 11, after removal of the boundary nodes, the internal connectivity of module 1 is larger than that of module 2. Therefore, in such cases, k is more dominant than k' after the fragmentation. Figure 11(a) shows that the order of robustness of each connection pattern is the same as the results of analysis although the giant component sizes are not completely the same.

Results using BA model. The numerical and analytical results for the random failure mode in a network composed of BA modules are shown in Figure 12. The number of trials for numerical simulations in each topology is 100. The minimum degree within a module is 3 and the maximum degree within a module is 76.

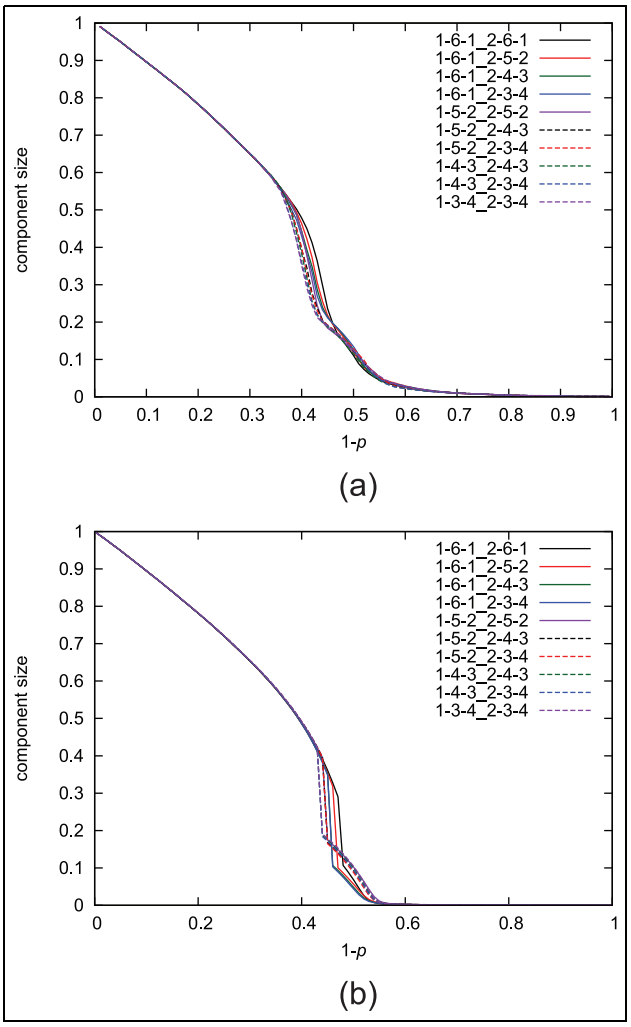

Figure 11. The results in targeted attack mode (ER model): (a) numerical and (b) analytical results.

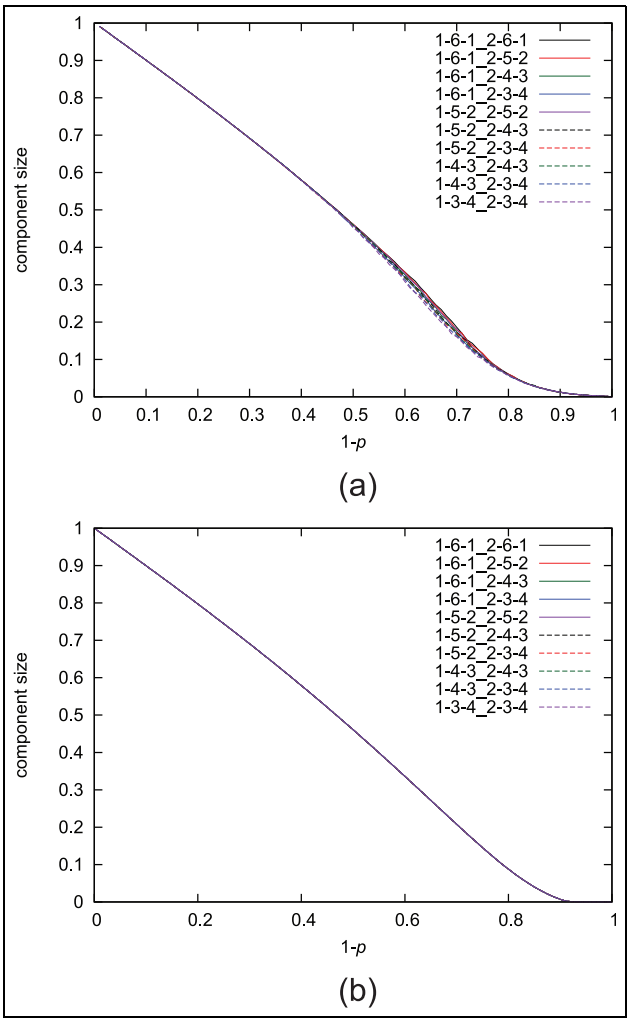

Figure 12. The results in random failure mode (BA model): (a) numerical and (b) analytical results.

The numerical and analytical results for the case of $d = 7$ and $d' = 7$ are shown in Figure 12(a) and (b), respectively. These results show that there is little difference depending on the connection pattern of inter-module links in random failure mode. Because we use BA model for constructing an intra-module graph, it has a power-law degree distribution. Therefore, difference of robustness will not occur unless we set d and d' to greatly high value.

When we use the BA model for constructing a graph within a module, the numerical and analytical results in targeted attack mode are shown in Figure 13. The numerical and analytical results for the case of $d = 7$ and $d' = 7$ are shown in Figure 13(a) and (b), respectively. Although the sizes of the giant components are almost the same, the graph in which the number of boundary nodes is large has a slightly higher robust connectivity before the fragmentation of the network into two modules, in both analytical and numerical simulations. After the fragmentation of the network, the ranking of the sizes of the giant components changes. The reason for this is the same as that mentioned for the results of Figure 11.

Results using WS model. The numerical and analytical results for the random failure mode in a network composed of WS modules are shown in Figure 14. The number of trials for numerical simulations in each topology is 100. The minimum degree within a module is 4 and the maximum degree within a module is 8.

The numerical and analytical results for the case of $d = 7$ and $d' = 7$ are shown in Figure 14(a) and (b), respectively. Each figure shows that the locus of giant component size in each method is almost same. However, the giant component size in numerical simulation decreases at an earlier step compared with the results of analysis. This is because the graph constructed by the WS model has a ring-shaped structure

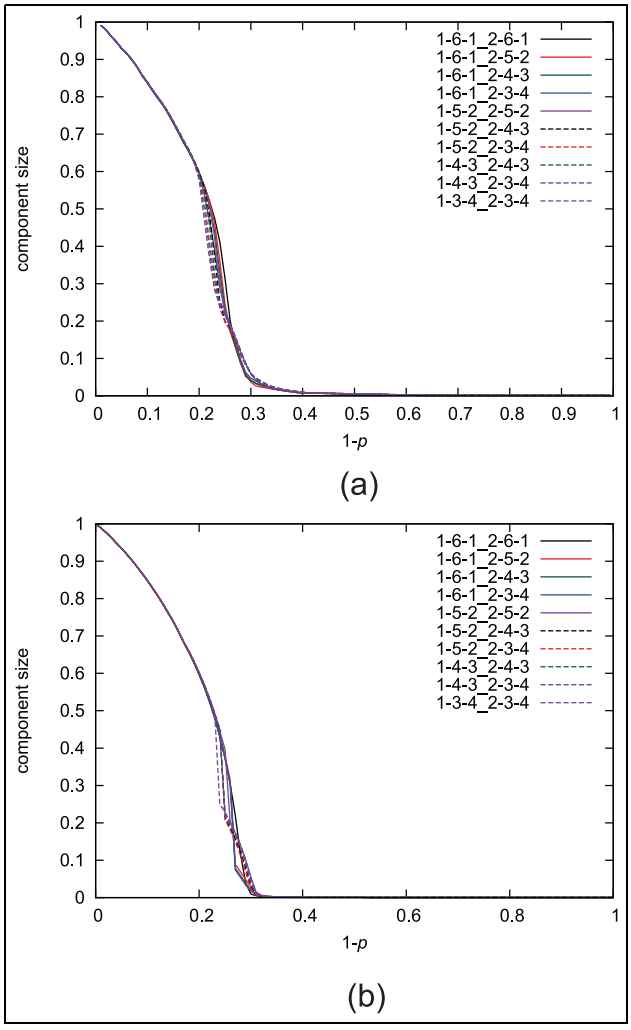

Figure 13. The results in targeted attack mode (BA model): (a) numerical and (b) analytical results.

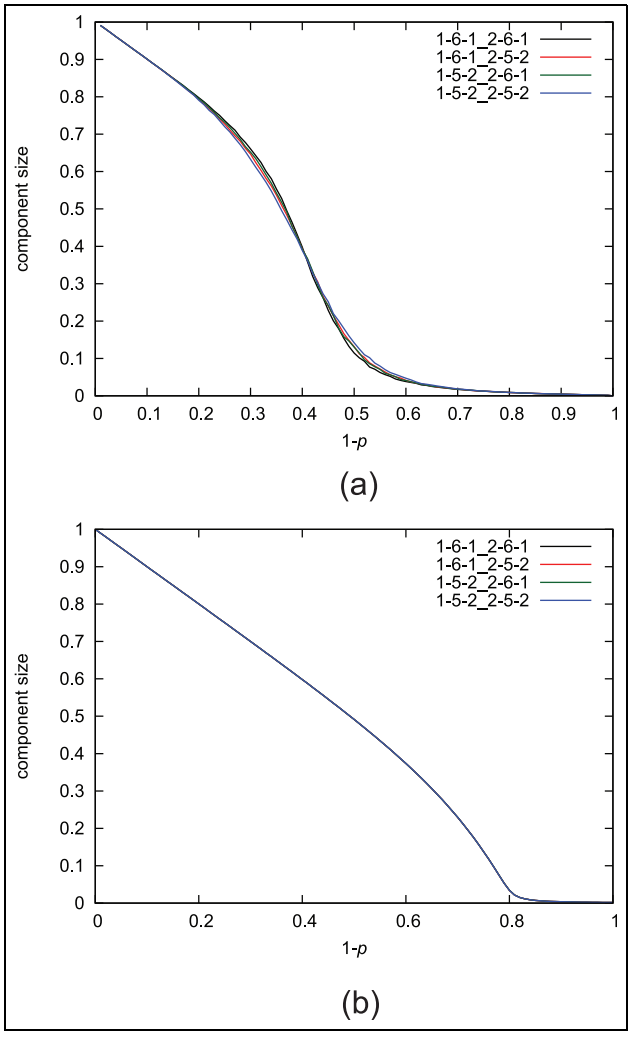

Figure 14. The results in random failure mode (WS model): (a) numerical and (b) analytical results.

and can fragment easily in numerical simulations, while the theory assumes random intra-module connections.

When we use the WS model for constructing a graph within a module, the numerical and analytical results in targeted attack mode are shown in Figure 15. From the results shown in Figure 15(a) and (b), the results of analysis are consistent with the results shown above. A graph constructed by method in which $(1/(d - k) + 1/(d - k'))$ is large has high robustness for small $(1 - p)$ values. After a graph fragments into modules, however, the giant component size in numerical simulation decreases at an earlier step compared with the results of analysis because of the same reason discussed in random failure mode.

From these results, our proposal can capture the order according to which the networks fragment into two modules. However, because we do not consider the structural properties of a graph within a module, a difference of analytical and numerical results occurs when a graph within a module has a special structure. It is our future work how to resolve this problem.

Conclusion

In this article, we propose a method for estimating robustness of graph ensembles after addition of inter-module links when the probability distribution of links within a module is given. Our proposal is to a binary-dynamics model[4] and add a new tool for the model. We investigate robustness according to the connection patterns of inter-module links.

In our simulation evaluation, we compare the robustness of the networks in various connection patterns of inter-module links when we fixed the values d and d' that describe the degrees of the boundary nodes after the link addition. Simulation experiments showed that graphs have robust connectivity in terms of the point at which the network fragments into two modules

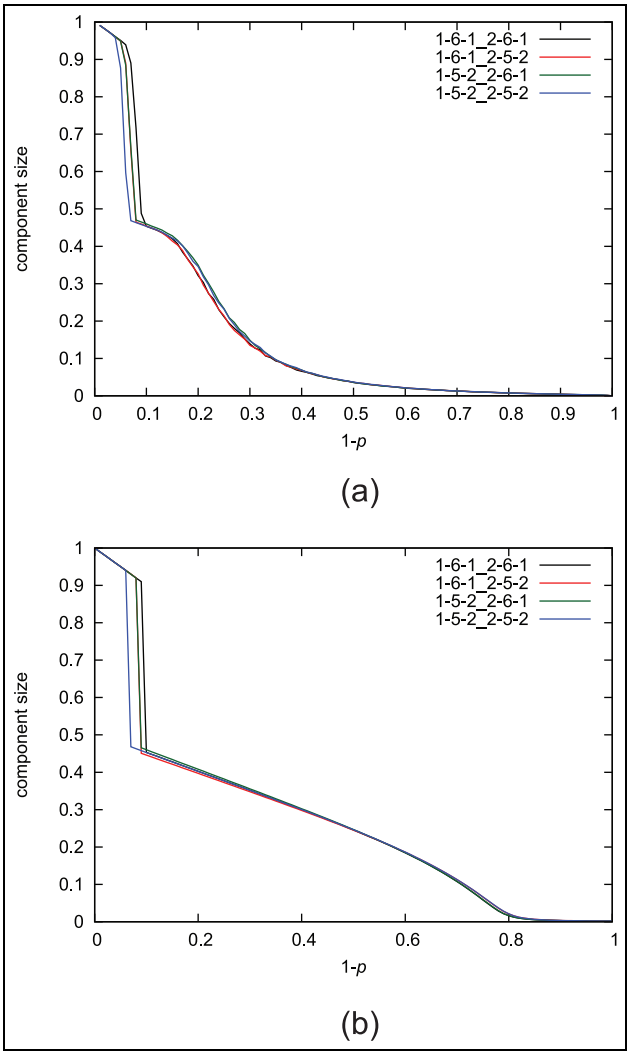

Figure 15. The results in targeted attack mode (WS model): (a) numerical and (b) analytical results.

when the number of nodes selected as boundary nodes and the degrees of the boundary nodes before the link addition are large. After the point, the internal structure of modules may matter more. To evaluate validity of the analysis results, we evaluate the percolation process on a graph constructed by a configuration model and find that the analysis results are in agreement with the numerical results. For the targeted attack mode, although the analytical results do not match well to the numerical results, the results are in agreement qualitatively. Moreover, we investigate the applicable range of our proposed method and showed that the difference between the analysis and numerical results increases as the number of nodes decreases.

To show a policy to make a graph robust by connecting multiple existing networks, we investigate robustness of a graph composed of modules with a given internal structure. The results show that our proposal can explain the order of the ranking of robustness (measured by the removal probability at which the network fragments into two modules) observed in the numerical results. Then, the number of nodes selected as boundary nodes and the degrees of boundary nodes before the link addition should be large in terms of the point of fragmentation of the network into modules when we fix the degree of the boundary nodes after the link addition.

However, because we do not consider the structural properties of a graph within a module, a difference of analytical and numerical results occurs when a graph within a module has a special structure. It is our future work how to resolve this problem.

For further investigation, we want to consider addition of multiple types of inter-module links. When multiple types of inter-module links are added, we cannot ignore the order of addition of the inter-module links because the conditional probability of the probability distribution of links changes after each addition of an inter-module link. This analysis will be realized when we use equation (14) multiple times according to the sequence of the type of new added link. Therefore, our method can also be applied to the graph in which multiple modules exist.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by a Grant-in-Aid for JSPS Fellows JP26·1639.

References

1. Khan I, Belqasmi F, Glitho R, et al. Wireless sensor network virtualization: a survey. *IEEE Commun Surv Tut* 2015; 18: 553–576.
2. Hong S, Lv C, Zhao T, et al. Cascading failure analysis and restoration strategy in an interdependent network. *J Phys A: Math Theor* 2016; 49(19): 195101, http://stacks.iop.org/1751-8121/49/i=19/a=195101
3. Toyonaga S, Kominami D and Murata M. Brain-inspired method for constructing a robust virtual wireless sensor network. In: *Proceedings of the 10th international conference on computing and network communications (CoCoNet 2015)*, Thiruvananthapuram, India, 16–19 December 2015, pp.1–7. IEEE.
4. Melnik S, Porter MA, Mucha PJ, et al. Dynamics on modular networks with heterogeneous correlations. *Chaos* 2014; 24(2): 023106, http://www.ncbi.nlm.nih.gov/pubmed/24985420
5. Newman ME. The structure and function of complex networks. *SIAM Rev* 2003; 45(2): 167–256. http://dx.doi.org/10.1137/S003614450342480

6. Newman ME, Strogatz SH and Watts DJ. Random graphs with arbitrary degree distributions and their applications. *Phys Rev E* 2001; 64(2 Pt 2): 026118.
7. Leicht EA and D'Souza RM. Percolation on interacting networks. *ArXiv e-prints* 2009; 2: 5, http://arxiv.org/abs/0907.0894
8. Min B, Yi SD, Lee KM, et al. Network robustness of multiplex networks with interlayer degree correlations. *Phys Rev E* 2014; 89(4): 1–9.
9. Dong G, Gao J, Du R, et al. Robustness of network of networks under targeted attack. *Phys Rev E* 2013; 87(5): 1–11.
10. Chopra M and Madan M. Network analysis by using various models of the online social media networks. *Int J Adv Res Comput Sci* 2015; 6(1): 111–116.