Designing P2P Networks Tolerant to Attacks and Faults Based on Bimodal Degree Distribution

Katsuya Suto[1,§], Hiroki Nishiyama[1,†], Xuemin (Sherman) Shen[2,‡], and Nei Kato[1,∓]
[1]Graduate School of Information Sciences, Tohoku University, Japan.
[2]Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Canada.
Email: { suto[§],bigtree[†], kato[∓]}@it.ecei.tohoku.ac.jp, xshen@bbcr.uwaterloo.ca[‡]

***Abstract*—Recently, in contrast with the centralized networks (e.g., traditional client/server systems), the distributed networks such as Peer-to-Peer (P2P) networks and grid networks have attracted much attention due to their scalability. While the distributed networks have the advantage of allowing the node(s) to join or leave the network easily, the issue of lack of resiliency to both attacks and faults still remains. In this paper, we classify the existing distributed networks based on their degree distributions. Then, we demonstrate that they are not resilient to attacks and/or faults. For example, unstructured P2P networks, which have a power-law degree distribution, are vulnerable to attacks such as DOS. To address and resolve this issue, we propose a method to construct a network following bimodal degree distribution, which is robust to deal with both attacks and faults. Performance evaluation is conducted through computer simulations, which show that the proposed method can achieve higher resilience compared with other existing networking approaches.**

***Index Terms*—P2P networks, overlay networks, attack and fault tolerance, degree distribution.**

I. INTRODUCTION

Penetration and development of the Information Communication Technologies (ICT) have been influenced by the overlay networks, which allow us to easily construct scalable network regardless of physical links, such as wireless or wired links [1]. Peer-to-Peer (P2P) networks, grid networks, and cloud computing using overlay technology are particularly essential today. Internet telephony, file sharing, and IPTV services have been deployed based on the P2P technologies [2], [3] while large-scale computing relies on the grid computing and cloud computing technologies [4], [5].

In these networks, each node is able to play either the role of the server or the client according to different situations. Such networks where nodes are equally connected with one other are called distributed networks. In contrast, in the centralized networks such as traditional client/server systems, nodes are either servers or clients. Table I presents the features of the centralized and distributed networks. In comparison with centralized networks, distributed networks, which are more suitable for constructing large-scale networks and distributing traffic loads over the whole network, have attracted much attention.

TABLE I
A COMPARISON BETWEEN CENTRALIZED AND DISTRIBUTED NETWORKS.

Network	Advantage	Disadvantage
Centralized	Management is easy.	Sharing load is difficult. Construction cost is high.
Distributed	departure or leaving is easy. Sharing load is easy.	Management is difficult.

However, distributed networks are intolerant of (i.e., not resilient to) network-failures due to the lack of a centralized infrastructure to manage the frequent joining and departure of an enormous number of nodes. There has been a great discussion on this critical issue. While the distributed network management has been studied to solve this issue in general [6], the present study was undertaken in order to construct distributed networks robust enough against network-failures without a management system. Specifically, We focus on the degree distribution of the distributed networks and propose a method to construct networks based on degree distribution robust against network-failures.

The remainder of this paper is organized as follows. In Section II, we define network-failures as attacks and faults. In Section III, we discuss the degree distribution of existing networks, which are classified into several categories based on their degree distributions, and the method to construct these networks is provided. We highlight the shortcomings of these conventional networks and introduce a network to deal with these problems in Section IV. Section V presents the performance evaluation of the proposed method through computer simulations from the point of view of the network connectivity and communication efficiency. Section VI concludes this paper.

II. NETWORK-FAILURE

A network may collapse because of network-failures, which can be classified into attacks and faults. In the case of the attacks where nodes lose their connectivity with the network by malicious threats such as computer viruses, Denial of Service (DOS) phenomena, and so fourth [7], the probability of dropping out of each node is supposed

Manuscript received February 15, 2011; revised May 15, 2011; accepted June 15, 2011.

doi:10.4304/jcm.7.8.587-595

to be proportional to the number of links connected to the node, i.e., the degree of the node. In contrast, in the case of the faults separating the node from the network due to mechanical troubles, link disconnection, user operation, and so on, a node drops out randomly regardless of the number of links connected to the node.

Faults in which all the nodes are disconnected evenly are inevitable in any network, and it is difficult to completely detect and prevent the network from attacks in which the highest degree nodes are disconnected. These failures degrade the network performance in terms of load concentration, communication efficiency, and communication disruption. Communication efficiency and network connectivity are significantly affected by the attacks when the high degree nodes are disconnected from the network. Therefore, we are interested in studying robust networks which are resilient to attacks.

III. Networks having different degree distributions

We study three specific large-scale distributed networks, namely random, regular, and scale-free networks, and their degree distributions. Degree distribution is the probability distribution of degrees over the network. In the conventional research, degree distribution is a common metric, which is frequently used for quantitative evaluation of the network-failures tolerance [8]. In addition, degree distribution affects node participation method in the networks, i.e., the way how a newly joining node selects a node to establish a connection depends on degree distribution of the networks. Thus, we focus on the node participation method in each network. In this paper, each node having a high degree is called a "hub node", which dominates the performance of the networks.

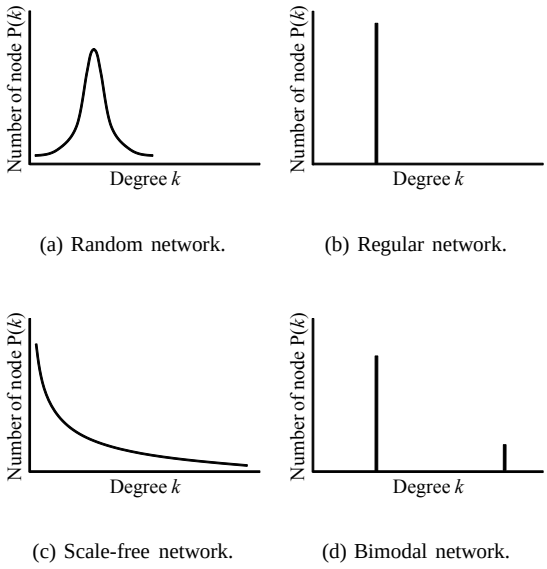
A. Random network

Degree distribution of random networks are shown in Fig. 1(a) and defined by the following equation:

$$P(k) = \binom{N-1}{k} p^k (1-p)^{N-1-k}, \tag{1}$$

where p, N, and k denote the probability of connection to a node, the number of nodes, and the degree of nodes in the network, respectively. Random networks are constructed in such a way that a newly joining node randomly selects a certain number of nodes. The list of nodes within the network is provided to the newly joining nodes when upon their joining the network.

Since the number of nodes having high degree (i.e., far above the average degree of the network) is small in the random networks, the communication efficiency and the network connectivity are low if the average degree of the network is low. While such shortcomings can be addressed by increasing the average degree of the network, it is not a practical solution due to non-negligible overhead to establish connections with large number of nodes.



(a) Random network. (b) Regular network.

(c) Scale-free network. (d) Bimodal network.

Fig. 1. Degree distributions of each considered network.

B. Regular network

In a regular network, all nodes have the same degree as depicted in Fig. 1(b). Structured P2P such as Chord [9] and Pastry [10] follow such a degree distribution, which can be defined by the following equation:

$$P(k) = \begin{cases} N & \text{if} \quad k = \langle k \rangle \\ 0 & \text{otherwise} \end{cases}, \tag{2}$$

where $\langle k \rangle$ denotes the average degree in the network. The regular network is constructed in such a way that a newly joining node selects a certain number of nodes as its neighbors in order to equalize the degrees of each node in the network. By connecting newly joining nodes to the nodes with a lower degree, the network can be approximated to a regular network.

A regular network has the lowest communication efficiency because it does not contain any hub node. Also, it has the highest resiliency against attacks since the variance of degree distribution in the regular network is zero.

C. Scale-free network

Almost all of the real-world networks such as Internet, World Wide Web (WWW) [11], and some social networks are considered as instances of the scale-free network which has a power-low degree distribution as shown in Fig. 1(c). In addition, it is demonstrated that unstructured P2P networks such as Napster, Gnutella, and Kazaa also have power-low degree distributions, which may be formulated as follows [12]–[15]:

$$P(k) \propto k^{-\gamma}, \tag{3}$$

where γ is a parameter typically in the range ($2 \leq \gamma \leq 3$). A scale-free network is constructed by following the Barabási-Albert (BA) model, i.e., a newly joining node

stochastically selects a certain number of nodes to connect to, based on the probability proportional to the degree of each candidate for selection.

In scale-free networks with long tail degree distributions, there are few hub nodes having a quite high degree. Therefore, the performance of these networks in terms of robustness to attacks and load balancing can be drastically degraded, while the communication efficiency achieve a high performance.

IV. Bimodal network

In general, hub nodes in a network are critical to promote the fault tolerance and the communication efficiency because they increase network connectivity [16]. However, nodes having higher degrees than other nodes are potentially exposed to attacks; Thus hub nodes become potential targets of malicious threats because their failure affects the whole network in an adverse manner. Thus, a broader degree distribution such as that of scale-free networks increases the vulnerability to attacks, because failure of a few high degree nodes under attack will disrupt the network. Contrary to this, scale-free networks increase the communication efficiency, as shown in Fig.2. To construct a attack resilient network, a regular network with all nodes having a constant degree is the best choice [17]. Therefore, nodes must have a constant high degree to be both fault-tolerant and resilient to attacks. However, increasing the average degree is difficult in large-scale networks due to the significant amount of network operating overhead, and link maintenance costs.

To achieve high robustness against both attacks and faults without increasing the average degree in a network, we employ a bimodal network, which has mixed features from both regular and scale-free networks to exploit their benefits in the maximum way possible. A bimodal network can achieve high robustness against attacks since it has a lower degree of hub nodes which cause fewer network fragment attributed to attacks compared to scale-free networks. In addition, fault tolerance in bimodal networks is better than in regular networks since they have hub nodes which increase network connectivity. Thus, bimodal networks inherit attack resiliency from regular networks and fault tolerance from scale-free networks. In a bimodal network having bimodal degree distribution shown in Fig. 1(d), the nodes are classified into (i) hub nodes with the same high degree, and (ii) non-hub nodes with the same low degree. The hub nodes allow the bimodal network to achieve high network connectivity, which results in high fault tolerance. On the other hand, the existence of only two types of node reduces the vulnerability against attacks. In the remainder of the chapter, we first explain the bimodal degree distribution, then we propose a method to effectively construct a bimodal network.

A. Bimodal degree distribution

There are two poles in the bimodal degree distribution proposed by T. Tanizawa *et al* [18]. There exist only two

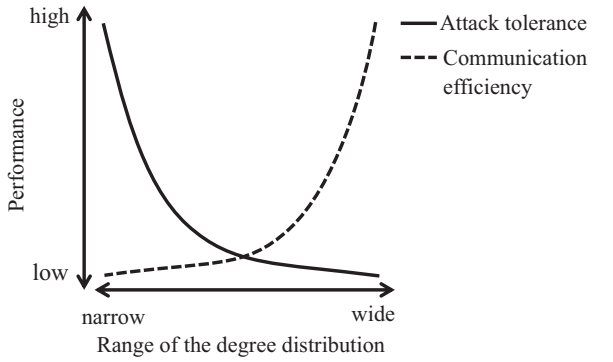


Fig. 2. The effect of the range of degree distribution in the network on attacks tolerance and communication efficiency.

different categories of nodes, i.e., a few hub nodes having a high degree $k_{\rm high}$, and a lot of non-hub nodes having a low degree $k_{\rm low}$, as shown in Fig.1(d). The degree of each category is given by the following function:

$$k_{\rm low} = \langle k \rangle, \tag{4}$$

$$k_{\rm high} = \sqrt{\langle k \rangle N}, \tag{5}$$

where $\langle k \rangle$ is the average degree of the network. The number of nodes N can be expressed as follows:

$$N = N_{\rm low} + N_{\rm high} = (1-r)N + rN, \tag{6}$$

where $N_{\rm high}$ and $N_{\rm low}$ are the number of hub nodes and non-hub nodes, respectively. The value of r optimizes performance in network-failures tolerance. Note that r is derived from the statical analysis [18] as follows:

$$r = \left(\frac{A^2}{\langle k \rangle N} \right)^{\frac{3}{4}}, \tag{7}$$

$$A = \left\{ \frac{2\langle k \rangle^2 (\langle k \rangle - 1)^2}{2\langle k \rangle - 1} \right\}^{\frac{1}{3}}. \tag{8}$$

Therefore, the bimodal degree distribution can be given by N and $\langle k \rangle$ as follows:

$$P(k) = \begin{cases} (1-r)N & \text{if} \quad k = \langle k \rangle \\ rN & \text{if} \quad k = \sqrt{\langle k \rangle N} \\ 0 & \text{otherwise} \end{cases}. \tag{9}$$

In the bimodal network, desired performance can be achieved by varying the parameter of average degree and $k_{\rm high}$. For example, when decreasing the value of $k_{\rm high}$, the attack tolerance (i.e., resiliency to attacks) will be increased. In contrast, the communication efficiency will be increased by increasing $k_{\rm high}$.

B. A method to construct a bimodal network

We have indicated the bimodal degree network tolerant to both the attacks and faults. From hereon, we propose the method to construct a bimodal network in overlay networks. In overlay networks, the method to construct

a network is synonymous with the node participation method for a newly joining node. The node participation algorithm in the proposed method is shown in Algorithm 1.

First, a newly joining node receives the following information from a node list: the number of nodes in each pole $k_{\rm low}$ and $k_{\rm high}$, the average degree $\langle k \rangle$, and the details of each node (i.e., the node's address, attributes such as hub or non-hub node, and the degree of the node). There are several ways to receive the node list from the network, e.g., select a certain number of nodes as node list management servers, which send and share the node list over the network.

Second, the newly joining node determines its attributes, which are computed according to the difference between the current and the ideal degree distribution. The current value of the number of hub nodes $N'_{\rm high}$ and non-hub nodes $N'_{\rm low}$ can be obtained from the node list. On the other hand, the ideal ratio is calculated by using Eq. (7), average degree $\langle k \rangle$, and the number of nodes N. Thus, each difference between the current ratio and ideal ratio is decided as follows:

$$\varepsilon_{\rm high} = \|N_{\rm high} - N'_{\rm high}\|, \quad (10)$$

$$\varepsilon_{\rm low} = \|N_{\rm low} - N'_{\rm low}\|. \quad (11)$$

When ($\varepsilon_{\rm high} > \varepsilon_{\rm low}$), the attributes of the newly joining node is decided to be a hub node, and vice versa. Then, the degree of each pole is calculated according to Eqs. (4) and (5) by using the pre-defined average degree and the number of nodes including the newly joining node.

Next, the newly joining node follows two successive connection procedures. To set up links to appropriate neighbors, the procedures consist of insertion and expansion phases. In the insertion phase, the newly joining node randomly selects a link in the network, and inserts itself into the link as follows: it breaks the existing link and creates new links between itself and each node. The insertion ensures that the connectivity of the network is maintained before and after this phase. The objective of this insertion is to provide equal opportunities in connection for all nodes. After the insertion phase, the newly joining node goes to the expansion phase, in which the node repeats the creation of additional links as long as the degree of the node is lower than the desired degree or the candidate for neighbor is in the node list. Here, candidate nodes are nodes, which have a lower degree than the desired degree. Since the degree of the nodes is limited by the desired degree and the candidates become insufficient, it is possible that the newly joining node cannot create an adequate number of links. In such a situation, the node temporarily waits for participation of other nodes until the criterion is satisfied.

Finally, the newly joining node adds itself to the node list, which is shared in the whole network. Each node receiving the updated node list computes the new degree of each pole, and moves to the expansion phase if the degree is lower than the computed value.

Algorithm 1 Node participation method in bimodal network.

```
Get a node list
if ε_low ≤ ε_high then
  Affiliate to high degree node
  The degree is k_high
else
  Affiliate to low degree node
  The degree is k_low
end if
Insertion process
while Degree does not fully-filled do
  Expansion process
  if Have enough degree then
    Break
  else
    if No candidate for neighbor then
      Break
    end if
  end if
end while
Register self-information to the node list
```

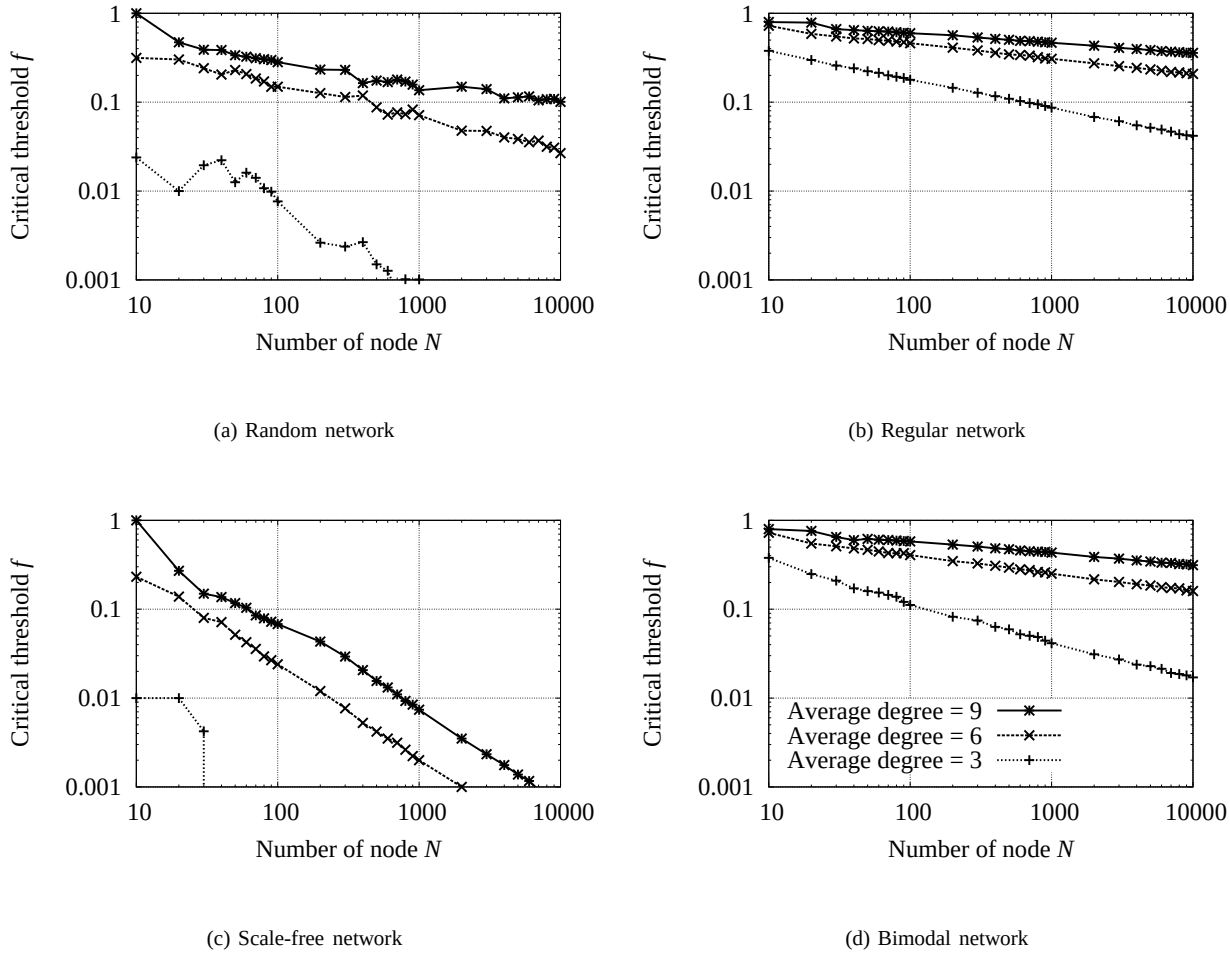
TABLE II
EXPERIMENTAL ENVIRONMENT.

	Part 1	Part 2
Average degree	3, 6, 9	3
Number of nodes	10 - 10000	10000
Networks	Random network Regular network Scale-free network Bimodal network	
Node removal method	Attack or Fault	
Number of trial	1000	

V. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the bimodal network constructed by the proposed method through computer simulations using MATLAB. The performance evaluation consists of two parts. In the first part, we evaluate the global network connectivity by measuring how many nodes can be disconnected from a network without disrupting the network. In the second part, we evaluate the local network connectivity and communication efficiency when a certain number of nodes leaving from the original global network [19].

In all simulations, we compare four different types of networks, namely random, regular, scale-free, and bimodal networks. Each network is constructed by the method mentioned in Sections III and IV. The performance of each network is evaluated in terms of tolerance of network-failures. Two different types of network-failure, attacks and faults, are simulated as the node removal from the network. Although nodes are left from the network in a descending order of node degree in the case of attacks, they are randomly made to leave the network regardless of the degree of each node in case of faults. Table II lists the set of environmental parameters



(a) Random network

(b) Regular network

(c) Scale-free network

(d) Bimodal network

Fig. 3. Attack tolerance of global network connectivity in different sizes of network with different average node degrees.

used in each evaluation part.

A. Global network connectivity

First, we evaluate the global connectivity of the network, which is the most important performance metric of the network-failures tolerance. In general, a leaving node might disconnect the network. Therefore, the number of nodes can be removed without separating a network is one of the typical metrics of global connectivity.

1) Critical threshold, f: To evaluate network connectivity, we focus on the critical threshold f, given by the following equation.

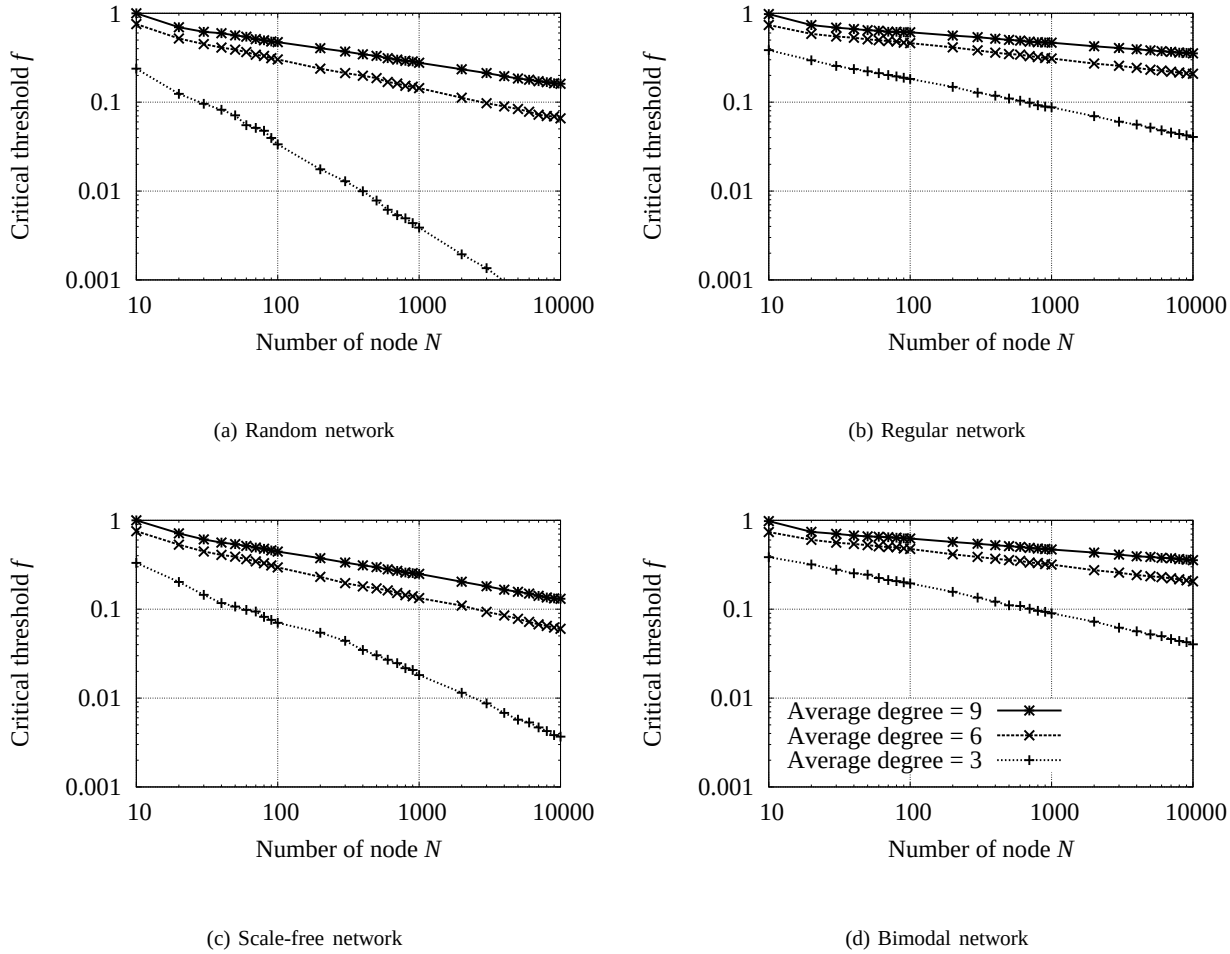
$$f = \frac{N_{\rm th}}{N} \quad (0 \leq f \leq 1), \tag{12}$$

where N denotes the number of nodes, and $N_{\rm th}$ denotes the number of nodes, which can be removed from network without separating the network. Note that f closer to 1 is necessary to achieve high connectivity.

2) Performance comparison with f: Figs. 3 and 4 show the critical threshold, f, in case of attacks and faults with different number of nodes and average degrees in each type of network, respectively. The number of nodes is varied from 10 to 10^4 and the average degree is set to any of the following values $\{3, 6, 9\}$. In case of attacks, the bimodal network and the regular network have high tolerance while the scale-free and random networks exhibit low tolerance. It should be noted that the bimodal network achieves high tolerance of attacks next to the regular network although vulnerable nodes exist in the bimodal network. Similarly, the tolerance of these networks is higher than that of other networks in case of faults. It, thus, becomes clear that the bimodal network achieves comparable tolerance of faults compared with the regular network. On the other hand, the performance can be improved by increasing the average degree in each network, especially in the random network and the scale-free network. However, the increasing of the average degree leads to the increase of network operating overhead. Therefore, these networks, which have high tolerance (regardless of the average degree of the network), appear to be the best choice.

B. Local network connectivity

We refer the local network created by node removal as a cluster. By measuring the size of clusters, the connectivity of the global network is evaluated. Thus, the local network



(a) Random network

(b) Regular network

(c) Scale-free network

(d) Bimodal network

Fig. 4. Fault tolerance of global network connectivity in different sizes of network with different average node degrees.

connectivity measures the impact of the communication failure due to the network separation.

1) Maximum cluster ratio, S: The maximum cluster ratio, denoted by S, is the ratio of the size of the maximum cluster to that of the original network. It is defined as follows:

$$S = \frac{N_c}{N} \quad (0 \leq S \leq 1), \tag{13}$$

where N_c is the number of nodes in the maximum cluster. S closer to 1 implies a higher local network connectivity.

2) Average cluster size, $\langle s \rangle$: Average cluster size $\langle s \rangle$ represents the average value of the cluster size for all clusters except the maximum cluster. $\langle s \rangle$ can be formulated as follows:

$$\langle s \rangle = \frac{1}{M} \sum_{i=1}^{M} N_i, \tag{14}$$

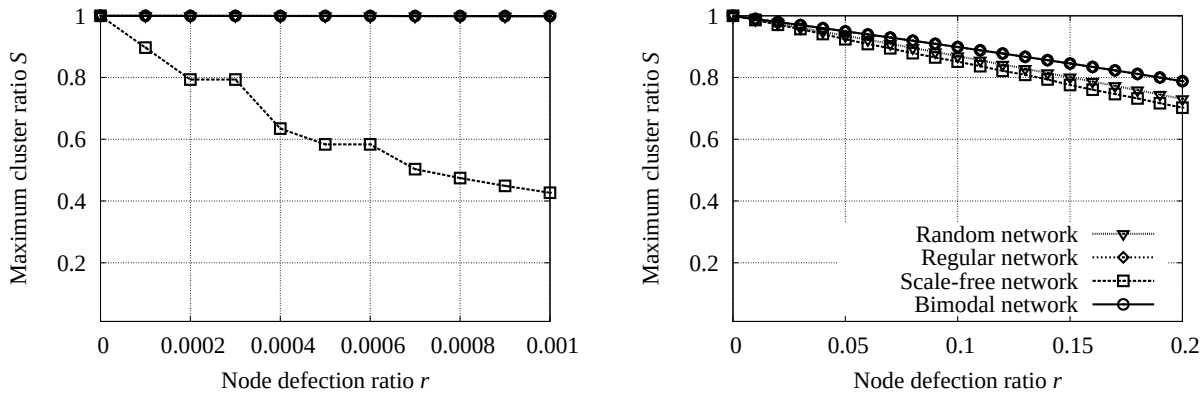
where N_i and M denote the size of the i^{th} cluster and the number of clusters except the maximum cluster, respectively. If $\langle s \rangle$ is around 1, it means that the global network has been divided into one large local network and a number of small local networks. It is obvious that if $\langle s \rangle$ equals zero, the network connectivity achieve a high value.

3) Performance comparison with S and $\langle s \rangle$: Figs. 5 and 6 show the impact of node defection ratio in the local network connectivity, which includes the maximum cluster ratio S, and the average cluster size $\langle s \rangle$. To evaluate the performance of the proposed approach in terms of realistic probabilities of attacks and faults, the value of r is varied in the range from zero to 10^{-3} in case of attacks and from zero to 0.2 in case of faults. In addition, the number of nodes is set to 10^4, and the average degrees of each network are fixed to 3

The results regarding attack tolerance are as follows. The bimodal and regular networks exhibit almost the perfect performance. In case of faults, the average cluster size $\langle s \rangle$ in bimodal and regular networks is less than 1.0 when the node defection ratio r is lower than 0.06. In other words, the network separation rarely occurs in the regular and bimodal networks when r is small. This means that both the networks are able to inhibit node isolation.

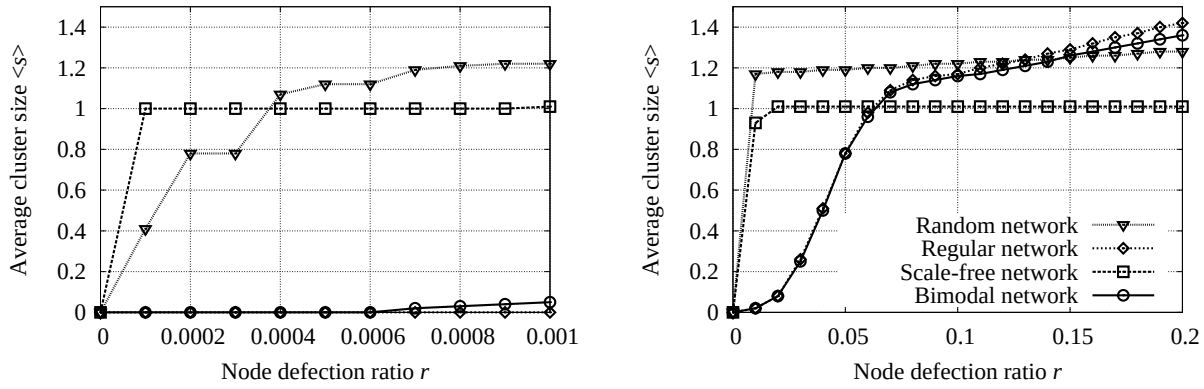
C. Communication efficiency

From the above discussion, we can conclude that both bimodal and regular networks are good candidates for



(a) Attack tolerance. (b) Fault tolerance.

Fig. 5. Relation between node departure ratio and the maximum cluster ratio S.



(a) Attack tolerance. (b) Fault tolerance.

Fig. 6. Relation between node departure ratio r and the average cluster size $\langle s \rangle$.

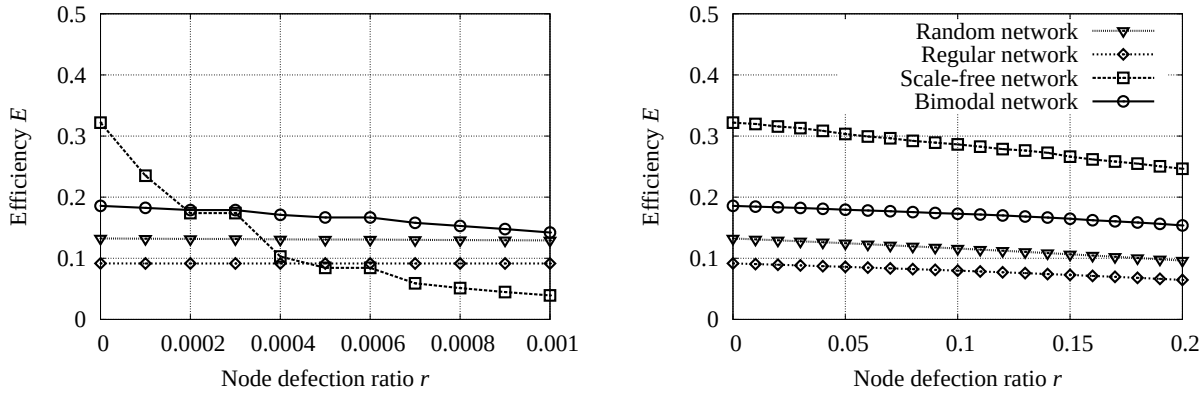
failure-tolerant large-scale distributed network. Next, we turn to communication efficiency, which is essential to evaluate the performance of distributed networks. Then, we will demonstrate that the bimodal network has the best performance conclusively.

1) Metric for communication efficiency E: To quantify the communication efficiency, we introduce the metric E, defined by the following equation using the inverse of the average hop counts between any two nodes in the network.

$$E = \frac{1}{N(N-1)} \sum_{i \neq j} \frac{1}{d_{ij}} \quad , (0 \leq E \leq 1), \tag{15}$$

where d_{ij} denotes the number of hops between the i^{th} and j^{th} nodes. Here, if there is no available path between two nodes, the hop count between them is infinity large, i.e., the inverse of the hop count is equal to zero. The maximum value of E is one and a larger value indicates higher communication efficiency.

2) Performance comparison with E: Fig. 7 depicts the values of E for different ratios of node departure. The setting of simulation parameters is similar to that in the evaluation of network disruption. Although the scale-free network exhibits the best performance in fault tolerance among all types of network, its tolerance of attacks drastically decreases as the node leaving ratio increases. This is because the performance of the scale-free network can be easily degraded by removing a few number of hub nodes from the network. On the other hand, we can observe that the bimodal network is superior to the regular network while both networks achieve similar performances in terms of network connectivity. Since there is no hub node in the regular network, the distance between any two nodes becomes larger than that in the other network(s) including hub nodes that results in low communication efficiency. Thus, we can conclude that the bimodal network constructed by the proposed method can offer not only high connectivity resulting in high tolerance



(a) Attack tolerance.

(b) Fault tolerance.

Fig. 7. Relation between the node departure ratio r and communication efficiency E.

of attacks and faults but also lead to high communication efficiency, which is essential for large-scale distributed networks.

VI. Conclusion

Distributed networks have attracted much attention due to their higher scalability and lower expense in contrast with the conventional client/server systems. However, since there is no centralized infrastructure managing the whole network, it is difficult to make these networks tolerant to network-failures due to malfunctions/faults and malicious attacks. Thus, we proposed a method to construct a robust distributed network against network-failures. Since the bimodal network is one of the best solutions to achieve both attack and fault tolerances, we focused on the bimodal degree distribution, and proposed an effective way for constructing a bimodal network based on the bimodal degree distribution. Through the performance evaluation based on computer simulations, we demonstrated that the networks constructed by the proposed method can offer high network connectivity which increases the tolerance of network-failures without compromising communication efficiency. To the best of our knowledge, this is the first work presenting an effective method to construct such bimodal networks along with its performance evaluation.

References

[1] E. K. Lua, J. Crowcroft, and M. Pias, "A survey and comparison of peer-to-peer overlay network schemes," *IEEE Communications Surveys & Tutorials*, vol. 7, no. 2, pp. 72–93, 2nd Quarter 2005.

[2] D. Chopra, H. Schulzrinne, E. Marocco, and E. Ivov, "Peer-to-peer overlays for real-time communication: Security issues and solutions," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 4–12, 1st Quarter 2009.

[3] X. Hei, Y. Liu, and K. W. Ross, "Iptv over p2p streaming networks: The mesh-pull approach," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 86–92, Feb. 2008.

[4] R. Ranjan, A. Harwood, and R. Buyya, "Peer-to-peer-based resource discovery in global grids: A tutorial," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 2, pp. 6–33, 2nd Quarter 2008.

[5] J. J. R. Fernando, D. Vila, and J. P. Gardner, "Scientific computing in the cloud," *IEEE Computing in Sience & Engineering*, vol. 12, no. 3, pp. 34–43, 2nd Quarter 2010.

[6] D. Raz and Y. Shavitt, "Active networks for efficient distributed network management," *IEEE Communications Magazine*, vol. 38, no. 3, pp. 138–143, Aug. 2002.

[7] M. Engle, "Vulnerabilities of p2p systems and a critical look at their solutions," Kent State University, Tech. Rep., Apr. 2006.

[8] R. Albert, H. Jeong, and A.-L. Barabasi, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, Jul. 2000.

[9] I. Stoica, R. Morris, D. Liben-Nowell, D. R. Karger, M. F. Kaashoek, F. Debek, and H. Balakrishnan, "Chord: a scalable peer-to-peer lookup protocol for internet applications," *IEEE/ACM Transactions on Networking*, vol. 11, no. 1, pp. 17–32, 2003.

[10] A. I. T. Rowstron and P. Druschel, "Pastry: Scalable, decentralized object location, and routing for large-scale peer-to-peer system," in *Proc. of the IFIP/ACM International Conference on Distributed Systems Platforms Heidelberg*, Nov. 2001, pp. 329–350.

[11] R. Albert, H. Jeong, and A.-L. Barabasi, "Error and attack tolerance of complex networks," *Nature*, vol. 401, pp. 130–131, Sep. 1999.

[12] L. A. Adamic, R. M. Lukose, A. R. Puniyani, and B. A. Huberman, "Search in power-law networks," *Physical Review E*, vol. 64, p. 046135, Sep. 2001.

[13] E. K. Lua, J. Crowcroft, M. Pias, R. Sharma, and S. Lim, "A survey and comparison of peer-to-peer overlay network schemes," *IEEE Communications Surveys and Tutorials*, vol. 7, no. 2, pp. 72–93, 2005.

[14] Y. Wang, X. Yun, and Y. Li, "Analyzing the characteristics of gnutella overlays," in *Proc. of International Conference on Information Technology-New Generations*, Las Vegas, Nevada, USA, Apr. 2007, pp. 1095–1100.

[15] M. Ripeanu, A. Iamnitchi, and I. Foster, "Mapping the gnutella network," *IEEE Internet Computing*, vol. 6, no. 1, pp. 50–57, Jan.-Feb. 2002.

[16] S. V. Buldrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, pp. 1025–1028, Apr. 2010.

[17] T. Tanizawa, "Percolation on correlated complex networks," *Computer Software JSS*, vol. 28, no. 1, pp. 135–144, 2011.

[18] T. Tanizawa, G. Paul, R. Cohen, S. Havlin, and H. E. Stanley, "Optimization of network robustness to waves of targeted and random attacks," *Physical Review E*, vol. 71, no. 4, p. 047101, Apr. 2005.

[19] S. Sun, Z. Liu, Z. Chen, and Z. Yuan, "Error and attack tolerance of evolving networks with local preferential attachment," *Physica A: Statistical and Theoretical Physics*, vol. 373, no. 1, pp. 851–860, Jan. 2007.

Katsuya Suto received his B.E. in Information Engineering from Iwate University, Japan, in 2011. Currently, he is pursuing the M.S degree in the Graduate School of information Science (GSIS) at Tohoku University. His research interests are the areas of overlay networks, ad hoc networks and sensor networks. He is a student member of the Institute of Electronics, Information and Communication Engineers (IEICE).

Hiroki Nishiyama received his M.S. and Ph.D. in Information Science from Tohoku University, Japan, in 2007 and 2008, respectively. He was a Research Fellow of the Japan Society for the Promotion of Science (JSPS) until finishing his Ph.D, following which he went on to become an Assistant Professor at the Graduate School of Information Sciences at Tohoku University. He has received Best Paper Awards from the IEEE Global Communications Conference 2010 (GLOBECOM 2010) as well as the 2009 IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC 2009). He was also a recipient of the 2009 FUNAI Foundation's Research Incentive Award for Information Technology. His active areas of research include, traffic engineering, congestion control, satellite communications, ad hoc and sensor networks, and network security. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and an IEEE member.

Xumin (Sherman) Shen received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a University Research Chair Professor, Department of Electrical and Computer Engineering, University of Waterloo, Canada. His research focuses on mobility and resource management in interconnected wireless/wired networks, UWB wireless communications networks, wireless network security, wireless body area networks and vehicular ad hoc and sensor networks.

He is a co-author of three books, and has published more than 400 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen serves as the Tutorial Chair for IEEE ICC08, the Technical Program Committee Chair for IEEE Globecom07, the General Co-Chair for Chinacom07 and QShine06, the Founding Chair for IEEE Communications Society Technical Committee on P2P Communications and Networking. He also serves as a Founding Area Editor for IEEE Transactions on Wireless Communications; Editor-in-Chief for Peer-to-Peer Networking and Application; Associate Editor for IEEE Transactions on Vehicular Technology; KICS/IEEE Journal of Communications and Networks, Computer Networks; ACM/Wireless Networks; and Wireless Communications and Mobile Computing (Wiley), etc. He has also served as Guest Editor for IEEE JSAC, IEEE Wireless Communications, IEEE Communications Magazine, and ACM Mobile Networks and Applications, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004 and 2008 from the University of Waterloo, the Premiers Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada.

Nei Kato received his M.S. and Ph.D. Degrees in Information Science from Tohoku University, Japan, in 1988 and 1991, respectively. He joined the Computer Center of Tohoku University in 1991, and has been a full professor at the Graduate School of Information Sciences since 2003. He has been engaged in research on computer networking, wireless mobile communications, image processing and neural networks, and has published more than 200 papers in journals and peer-reviewed conference proceedings.

Nei Kato currently serves as the chair of the IEEE Satellite and Space Communications Technical Community (TC), the secretary for the IEEE Ad Hoc & Sensor Networks TC, the vice chair of the IEICE Satellite Communications TC, a technical editor for IEEE Wireless Communications (since 2006), an editor of IEEE Transactions on Wireless Communications (since 2008), and as an associate editor of IEEE Transactions on Vehicular Technology (since 2009). He also served as a co-guest-editor for IEEE Wireless Communications Magazine SI on "Wireless Communications for E-healthcare", a symposium co-chair of GLOBECOM'07, ICC'10, ICC'11, ChinaCom'08, ChinaCom'09, and the WCNC2010-2011 TPC Vice Chair.

His awards include the Minoru Ishida Foundation Research Encouragement Prize (2003), the Distinguished Contributions to Satellite Communications Award from the IEEE , Satellite and Space Communications Technical Committee (2005), the FUNAI information Science Award (2007), the TELCOM System Technology Award from the Foundation for Electrical Communications Diffusion (2008), the IEICE Network System Research Award (2009), and many best paper awards from prestigious international conferences such as IEEE GLEBECOM, IWCMC, and so on.

Besides his academic activities, he also serves as a member on the Telecommunications Council expert committee, the special commissioner of the Telecommunications Business Dispute Settlement Commission, for the Ministry of Internal Affairs and Communications, in Japan, and as the chairperson of ITU-R SG4, in Japan. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and a senior member of IEEE.