社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

A Failure-Tolerant Structure in Router–level Internet Topologies

Shin'ichi ARAKAWA†, Tetuya TAKINE††, and Masayuki MURATA†

† Graduate School of Information Science and Technology, Osaka University
1–5 Yamadaoka, Suita, Osaka 565–0871, Japan
†† Graduate School of Engineering, Osaka University, Osaka, Japan

Abstract The degree distribution of Internet topology is known to obey a power-law attribute. However, the degree distribution does not solely determine the topological properties of the Internet. In this paper, we investigate the failure-tolerant characteristics of ISP's router-level topologies, and we reveal what topological properties determine the fault tolerant characteristics. Our results indicate the degree-correlation alone does not determine the failure-tolerant characteristics, and the modularity structure of topologies is important for determining the failure-tolerant characteristics of router-level topologies.

Key words ISP topology, power-law, link capacity

1. Introduction

As the Internet evolves, its ability to perform its functions correctly even in the presence of failures becoming increasingly important. Failure tolerance is one of the characteristics for Internet topologies to keep connectivity against failures of routers and/or links. Thus, understanding the failure tolerance of Internet topologies is essential, and clarifying what is the key to forming failure tolerance is important. In this paper, we investigate the fault tolerance characteristics of router-level Internet topologies, and we herein reveal what topological characteristics determine the fault tolerance characteristics.

The degree distribution of AS-level Internet topologies was revealed to show a power-law attribute [1]. That is, the probability of nodes having degree k obeys $P(k) = a \times k^{-\gamma}$, where a and γ are specific constant values. The theoretical foundation for the power-law network is introduced in Ref. [2], where they also present the Barabashi-Albert (BA) model in which the topologies increase incrementally, and in which links are placed based on the connectivities of topologies to form power-law networks. Albert et al. also investigated the failure tolerant characteristics of topologies obtained using the BA model [3]. The resulting topologies of the BA model have relatively few high degree nodes. Thus, a random failure of nodes will mostly remove low-degree nodes, with little effect on network connectivity(1).

When router-level topologies are concerned, the BA model (and its variants), in which links are attached based on a preferential probability does not adequately model the ISP's router-level topologies, since each ISP constructs its own router-level topology based on strategies such as minimizing the mileage of links and/or maximizing reliability. Li et al. [4] investigated the structural properties of router-level topologies that have the power-law degree distribution. They enumerated various topologies with the same degree distributions and showed the relationship between their structural properties and the performance of these topologies. They pointed out that high-degree nodes accommodate low-bandwidth access lines, while lower-degree nodes accommodate high-bandwidth core lines because of technological constraints in commercial routers. Ref. [5] presents an analysis and generation methods for topologies that are "close" to a (given) topology. Ref. [5] introduces a dK-targeting dK' preserving rewiring method for generating topologies that have a structure resembing the original topology. K is a parameter that specifies the degree of correlation from the original topology; the degree correlation between K nodes is identical to the original topology. When K is 0, the average degree is identical to the original topology. Taking $K = 1$ leads to the same degree distribution. In the case of $K = 2$, the probability that two nodes having degree k' and degree k'' is identical to the original topology. As K increases, a topology that more closely resembles the original topology is generated. The results indicate the average hop counts between nodes and other topological properties are mostly identical to the router-level topologies.

The aforementioned paper clearly indicates that the power-law degree distribution alone does not determine the structural properties of router-level topologies. Thus, several works such as Ref. [4] and Ref. [5] investigated a modeling and analyzing method for the structural properties of topologies based on the degree correlation of two or more nodes, other than the degree distribution. However, the important thing for the modeling and analyzing method is

(1)：Note that when considering the failure-tolerance of power-law networks, the attack tolerance is another concern. However, in this paper, we focus on the topological characteristics due to random failures.

what characteristics of the router-level topologies we want to explain. In this paper, we investigate the failure-tolerant characteristics of router-level topologies and whether or not the degree correlated metrics can be used to explain the failure-tolerant characteristics of router-level topologies. Our results show that even if the degree-correlations of the topologies are the same, the failure-tolerant characteristics are different. Therefore, we investigate what structural properties determines the failure-tolerant characteristics of router-level topologies.

First, we investigate the failure-tolerant characteristics of ISP's router-level topologies by removing nodes and links randomly. We use the connectivity of topologies after the failure as a measure for the failure tolerance. In an actual network, flows that pass through network components are detoured when a failure occurs in the network components. Thus, the amount of flows after failures may be used to assess the failure tolerance. However, we did not consider the flow-level granularity for the failure tolerance because our primary concern is to clarify the structural properties to give connectivity in the router-level topologies.

Next, we investigate what structural properties contribute to keep the connectivity of topologies after failures occur. Our results show that the failure-tolerant characteristics of router-level topologies depends on the degree distribution; if topologies have different degree distributions, the failure-tolerant characteristics of the topologies are also different. Our results also show that the failure-tolerant characteristics does not depend on the degree-correlation with K = 3 in [5]. That is, only the degree-correlation does not determine the failure-tolerant characteristics. Therefore, we apply the analyzing method in Ref. [6], which was originally proposed for analyzing biology network, to reveal what structural properties determine the failure-tolerant characteristics. The results show that the modularity structure of topologies determines the failure-tolerant characteristics of router-level topologies.

This paper is organized as follows. Section 2 presents related works for the modeling and analyzing method for the Internet topology. Section 3 discusses the failure tolerance of router-level topologies against failures of nodes. In Section 4, we discuss our investigation of structural properties of router-level topologies and reveal what structural properties are important to enable the router-level topologies to have the failure tolerance. Finally, we conclude the paper in Section 5.

2. Related works

Modeling methods for Internet topologies that have a power-law-like degree distribution have been investigated to understand the fundamental characteristics of the topologies.

Barabasi and Albert [2] presents a BA model in which the topologies grow incrementally and links are attached to nodes based on a preferential probability, $\Pi(i) = d_i / \sum_j d_j$, where d_i is the degree of node i. They show that, with these simple rules, the resulting topologies have the power-law attribute. Bu and Towsley [7] compares the structure of the BA model with the AS-level topology. Their results show that the degree distribution as well as the cluster coefficient with the BA model does not match those with the AS topology because new ASs have a stronger preference for hub nodes compared to the linear preference used with the BA model. They then propose a new preferential probability, $\Pi'(i) = (d_i - \beta)/\sum_j (d_j - \beta)$, to generate AS-like topologies. β (< 1) is a parameter that increases the preferential probability for high-degree nodes.

As far as router-level topologies are concerned, the BA model (and its variants), in which links are attached based on a preferential probability, does not model the ISP's router-level topologies correctly, because each ISP constructs its own router-level topology based on strategies such as minimizing the mileage of links and/or maximizing reliability. The FKP model proposed by Fabrikant et al. [8] revealed that the power-law properties of the degree distribution can still be obtained by minimizing the "distance" metrics. This model does not use a preferential attachment to add links, and instead it uses ma inimization-based link attachment. However, Ref. [9] points out that topologies based on the FKP model have too many nodes that have one out going links and are different from ISP's router-level topologies [10].

Li et al. [4] enumerated various topologies with the same degree distributions, and they showed the relationship between their structure and the performance of these topologies. They pointed out that because of a technological constraint in commercial routers, high-degree nodes accommodate low-bandwidth access lines, while lower-degree nodes accommodate high-bandwidth core lines because of technological constraints with commercial routers. When we consider such link capacity constraints, topologies based on the BA model show poor throughput due to technological constraints. That is, because hub nodes tend to be connected each other, low-bandwidth access lines between hub nodes will be a bottleneck in the network. With a three-level hierarchical structure based on the Abilene network and the previously mentioned link capacity constraints, Li et al. show a case where throughput of a topology is maximized while the degree distribution follows a power law. Although Li et al.'s approach is significant, the router-level topologies in the Internet and Abilene-based topologies are quite different in terms of the cluster coefficient. More importantly, these differences greatly affect the methods of network control. One typical example is routing control; the link utilization in the router-level topologies is much far from the one in the conventional modeling method [10].

Ref. [5] introduces a dK-targeting $dK^{'}$ preserving rewriting method for generating topologies that have a structure resembling the original topology. K is a parameter that specifies the degree of correlation from the original topology; the correlation of degree between K nodes is identical to the original topology. As K increases, more resembled topology to the original topology is generated. However, the method described in Ref. [5] aims to generate topology that is close to the original. Therefore, it is insufficient to understand the structural properties of the router-level topology and to answer the question of what structural properties determine the failure-tolerant characteristics of the topology.

3. Failure-tolerant characteristics in ISP's router-level topologies

In this section, we investigate the failure-tolerance in ISP topologies that was obtained in Ref. [11]. A failure tolerance is one of important properties for the Internet topologies to keep connectivity against failures of routers and/or links. In this paper, we regard the failure tolerance as connectivities between nodes after failures occur. If no connectivity is lost, every node in the topology communicates with the other nodes by re-routing the traffic. Even when the connectivity is lost, the size of the largest connected component is the next concern. As the size of the largest connected-component increases, more nodes are connected. Note that the amount of flows after failures may be used to assess the failure tolerance. However, we did not consider the flow-level failure-tolerance here because our primary concern is to clarify the structural properties to give connectivity in the router-level topologies.

The failure scenario that we use is the random failure in nodes (routers). The node failure occurs due to, e.g., a power-failure at routers.

3.1 ISP topologies

We use an AT&T topology (523 nodes, 1304 links) and a Sprint topology (467 nodes, 1280 links) obtained in Ref. [11] for the ISP topologies. For comparison purposes, we also prepare two other topologies, having the same number of nodes/links to the Sprint topology, by using BA and ER models. The average degree of the Sprint, BA, and ER topologies is the same, but the degree distributions differ.

3.2 Cover rate

To represent the failure-tolerance characteristics of the Internet topology (that has N nodes), we introduce *cover rate*, C, which is defined using the following equation:

$$C(N_c) = \frac{S_{N_c}}{N - N_c}, \tag{1}$$

where N_c is the number of failures occuring, and S_{N_c} is the number of nodes in the largest connected components (also known as the giant component) after the N_c-node failure. By this definition, the cover rate is 1.0 if all nodes are connected after an N_c-node failure. As the cover rate decreases, the network is more divided, which we regard as lower failure tolerance. According to the experimental results of [12], the failure probability of a route is around 95% to 99.8%. Thus, we consider the cover rate of more than 95% in this paper.

3.3 Failure-tolerant characteristics of ISP topologies

Figure 1 shows the cover rate for each topology dependent on the number of node-failures. The horizontal axis is normalized using the number of nodes in the original topology to compare the cover rate for different topologies. We observe that the cover rate of the ISP topologies (AT&T topology and Sprint topology) is lower than that of BA/ER topologies. This means that the ISP's structural properties are less failure-tolerant of random node failures. We will discuss what structural properties affect the failure-tolerant characteristics in Sec. 4. We also observe that the difference between the

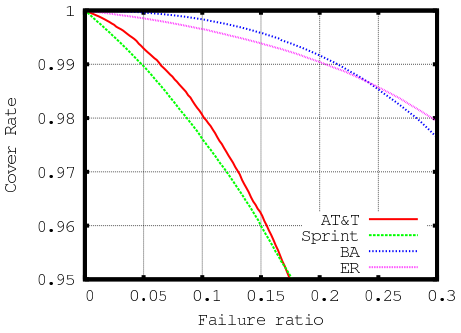


Fig. 1 The cover rate of ISP topologies: Random node failures, averaged over 3000 experiments.

results of the BA topology and the results of the ER topology are not significant. Note that the average degree of the Sprint and BA/ER topologies is the same, i.e., these topologies belong to Class $K = 0$ in Ref. [5]. Thus, these results indicate that we cannot characterize the failure tolerance by the average degree. More detailed topological properties have to be investigated to explain the failure-tolerant characteristics in the Internet topologies.

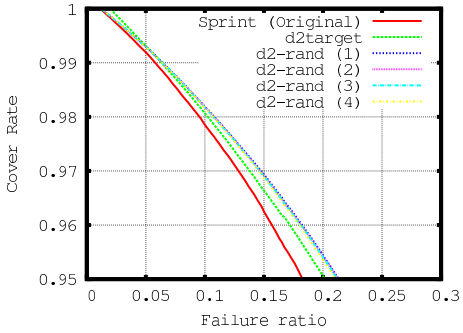
3.4 Do degree-related metrics explain the failure-tolerant characteristics?

The results of the previous section indicate the average degree cannot be used to explain the failure-tolerance characteristics of the topologies. The question then is whether or not other degree-related metrics can explain these characteristics. This section descibes our investigation into the other degree-related metrics by applying methods in Ref. [5].

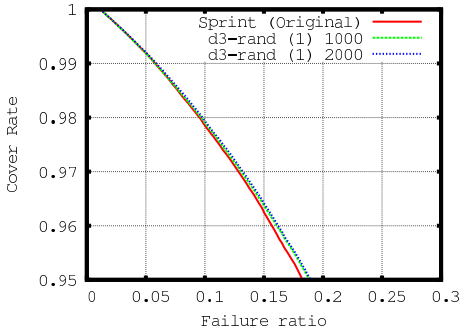
Ref. [5] introduces a dK-randomization method that rewires links randomly while keeping the distribution of degree correlation between K neighboring nodes. K is a parameter that specifies the degree of correlation from the original topology. Ref. [5] introduces the dK-targeting dK' preserving rewiring method, where links are rewired so that the degree correlation of K nodes is close to the given value while keeping the degree correlation of K' nodes.

Figure 2 depicts the cover rate when the d2-targeting d1 preserving rewiring method (denoted as "d2target") and the d2-randomization method (denoted as "d2-rand") are applied to the Sprint topology. For obtaining the "d2target," we use the pseudograph approach [5] to obtain an initial topology that has a $K = 1$ property because the approach has shown good agreement to obtain the $K = 2$ topology. For the dK-randomization method, we perform rewiring 2000 times. Hereafter, these settings are used unless explicitly specified. We also change the seed for randomization, and part of the results are plotted in Fig. 2. We also obtain the case for the AT&T topology in Fig. 3.

First of all, in either ISP topology, the difference in the random seed does not affect the cover rate. Thus, we will omit the results of different seeds in the following. When we see the results of the Sprint topology, the cover rate of the d3-randomization method is close to the cover rate of the original topology, whereas the cover rate of the d2-randomization method is different from the original topology. That is, the degree correlation between three nodes is

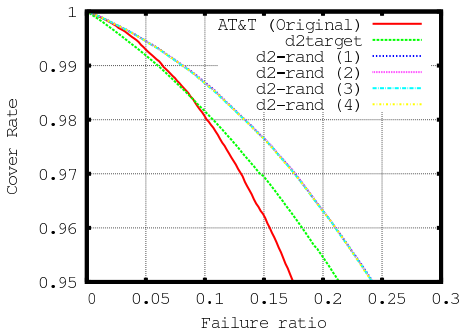


(a) D2 randomization

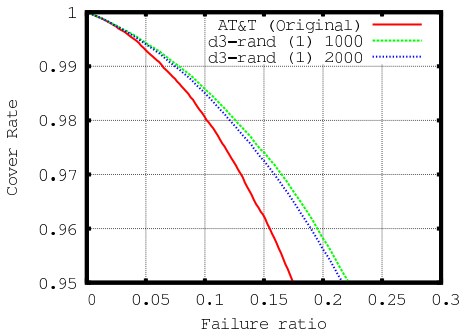


(b) D3 randomization

Fig. 2 Sprint topology: random node failure



(a) D2 randomization



(b) D3 randomization

Fig. 3 AT&T topology: random node failure

required to represent the cover rate in the Sprint topology. Looking at Fig. 3 (the case for the AT&T topology), we can see that the difference in the cover rate between the original and randomized topologies increases. That is, the degree correlation does not represent and explain the failure-tolerant characteristics of the ISP topologies. This fact can be easily observed from Fig. 4: As the number of rewiring processes increases (from 8 to 100), the cover

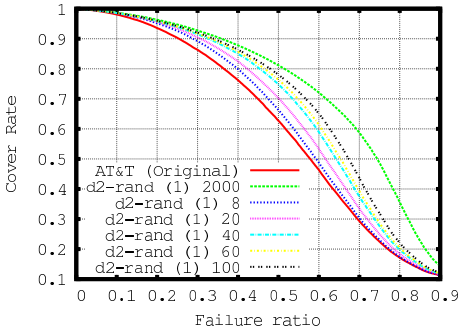


Fig. 4 AT&T topology: The number of rewiring is set to 8, 20, 40, 60, 100 as depicted in the legend.

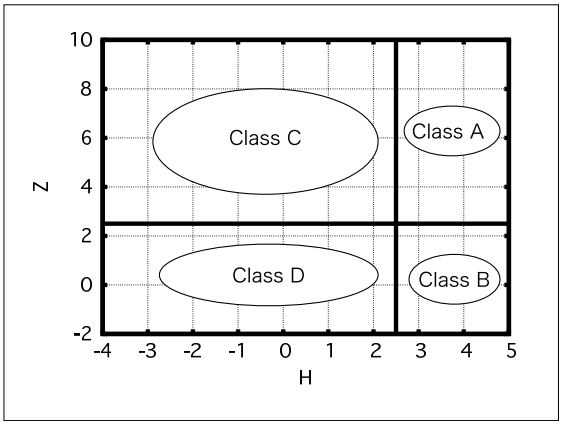


Fig. 5 Classification of node functionality

Table 1 Node functionalities

	Z_i	H_i	Functionality
Class A	high	high	hub-core
Class B	low	high	non-hub core
Class C	high	low	provincial hub
Class D	low	low	leaf (non-hub)

rate increases. The topologies obtained with the d2-targeting d1-preserving rewiring method are closer to the original topology than those obtained with the randomization method, but it still shows a difference. Note that we can obtain a parameter $\hat{K}$, which is enough to represent the failure-tolerant characteristics of ISP topologies by using the method in [5]. However, we do not increase the parameter K because our purpose is to reveal what structural properties determine the failure-tolerant characteristics of router-level topologies.

4. failure-tolerant structures in ISP's router-level topologies

The results of the previous section show that the degree distribution or the degree correlation does not determine the failure-tolerant characteristics of router-level topologies. This section investigate structural properties of ISP topologies, and we reveal what structural properties contribute to keep the connectivity of the topologies after failures occur.

4.1 Structure in ISP topologies

As discussed in Ref. [4], the network's design principles greatly

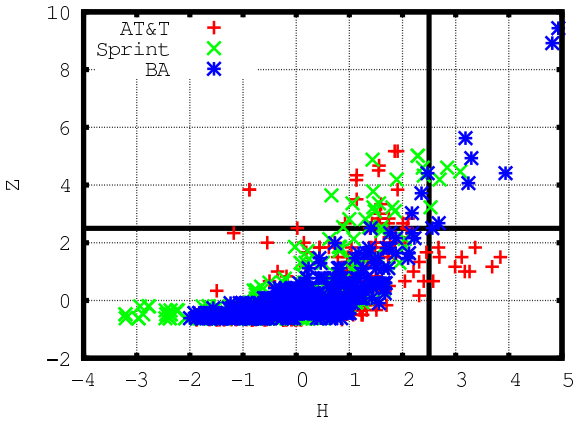


Fig. 6 Node functionality

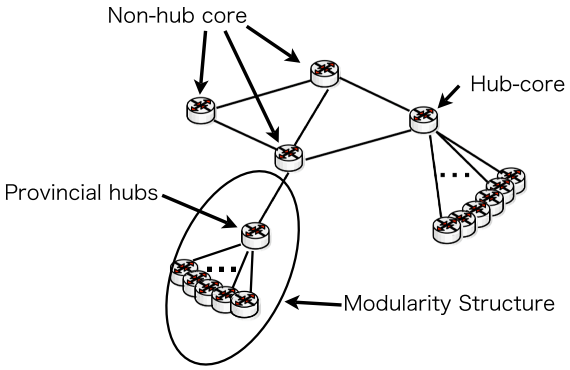


Fig. 7 Illustration Example of node functionalities

affect the structure of ISP topologies. Design principles determine a node functionality, which in turn determines the linking of nodes. In this paper, we consider the location of nodes in the topology. Here, the location does not mean the physical location, but the logical (in terms of hop counts) location. For each node (denoted as i), we define the following two metrics to identify the node functionality.

$$Z_i = \frac{k_i - < k >}{\sigma_k}, \tag{2}$$

where k_i is the degree of nodes, $< k >$ represents the average degree in the topology, and σ_k is the variance of the degree distribution. We also define the location-related metric H as follows.

$$H_i = \frac{d_i - < d >}{-\sigma_d}, \tag{3}$$

where d_i is the average of the hop-count distance starting from node i to the other nodes, $< d >$ is the average of d_i, and σ_d is the variance of d_i. We classify the node functionality according to the value of Z and H as Figure 5.

We then define the node functionality in Table 1. base on the fact that we can consider that the nodes whose Z is greater than 2.5 to be high-degree (hub) nodes, while the nodes whose H is greater than 2.5 are considered to be located at the "center" of the networks.

Figure 6 plots the node functionality in each topology. The BA topology has few number of "hub-core" nodes, i.e., some nodes have lots of out going links and are located at the center of the topology. As Ref. [3] discusses, a random failure of nodes will mostly remove low-degree nodes, with little effect on the network

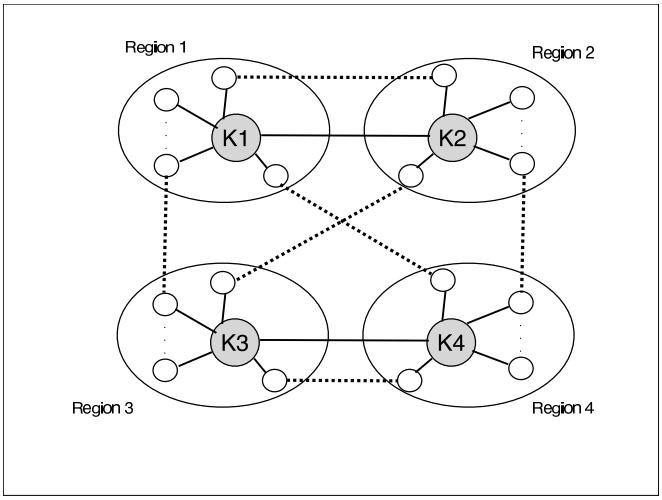


Fig. 11 Modularity-reserved rewiring; the case when rewiring edge (k1,k2) and edge (k3,k4). Accept the rewiring only if there are links (dashed-lines in the figure) that connect other regions.

connectivity. ISP topologies have several "provincial hub" nodes. A "provincial hub" node and its neighbor nodes make a modularity structure. However, the modularity structure has lower failure-tolerant characteristics because the failures of the upstream nodes lose their connectivity around the "provincial hub" nodes.

4.2 Modularity-reserved rewiring

The d2-randomization method and the d3-randomization method do not represent the failure-tolerant characteristics of ISP topologies. In this section, we introduce another kind of rewiring technique: modularity-reserved rewiring. We demonstrate that the topologies obtained from this modularity-reserved rewiring represent the failure-tolerant characteristics more than the d2 and d3-randomization methods. To see why d2 and d3-randomization methods fail to represent the failure-tolerant characteristics, we present the node functionality after these methods are applied (Figs. 8 – 10). Figure 9 shows that "non-hub core" nodes and "provincial hub" nodes are eliminated; thus, the modularity structure disappears from the topology. The d3-randomization method seems to have less impact on the node functionality (Fig. 10), but the cover rate is still different from the cover rate of the original topology.

We therefore introduce a modularity-reserved rewiring method to keep the modularity structure in the ISP topologies. Figure 11 explains the modularity-reserved rewiring method for rewiring edge ($K1$, $K2$) and edge ($K3$, $K4$). Note that the degree of $K2$ and $K4$ is the same in this exampleu (since we used d2-reserved rewiring). Our method considers a region, with nodes one-hop-away from node $K1$-$K4$. Then, we simply check the connectivity between regions, and accept the rewiring only if there is a connectivity between regions. By doing this, the rewiring of edge ($K1$, $K2$) and edge ($K3$, $K4$) does not add/delete the connectivity between the region; thus, it is expected to keep the structure in the topology. Figures 12 and 13 show the cover rate and node functionality when we apply the modularity-reserved rewiring method to the AT&T topology. As we can see from the figure, the cover rate of the modularity-reserved

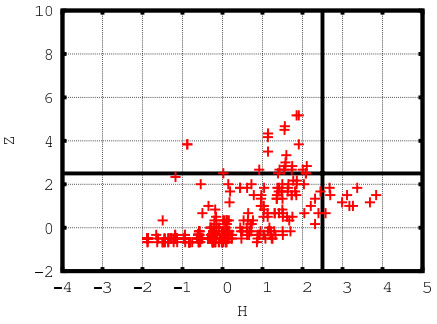


Fig. 8 Node functionality: AT&T topology (original)

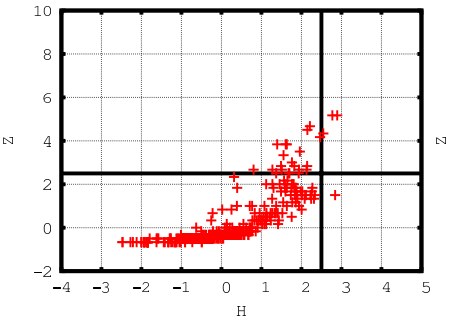


Fig. 9 Node functionality: D2 randomization

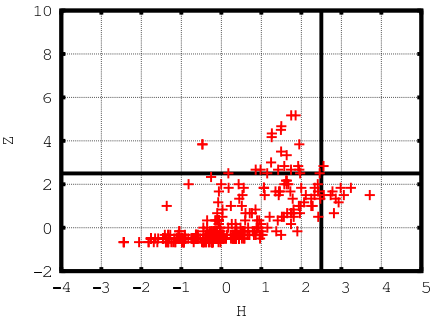


Fig. 10 Node functionality: D3 randomization

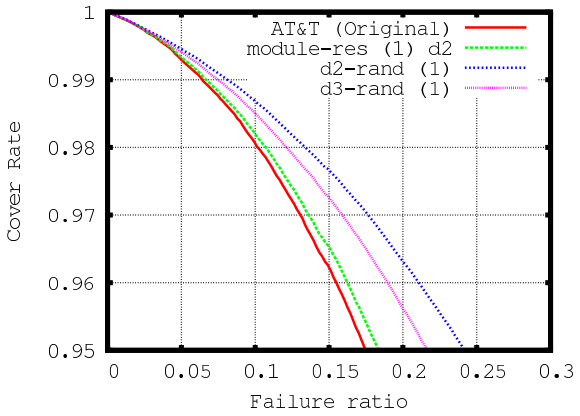


Fig. 12 The cover rate (Modularity-reserved rewiring)

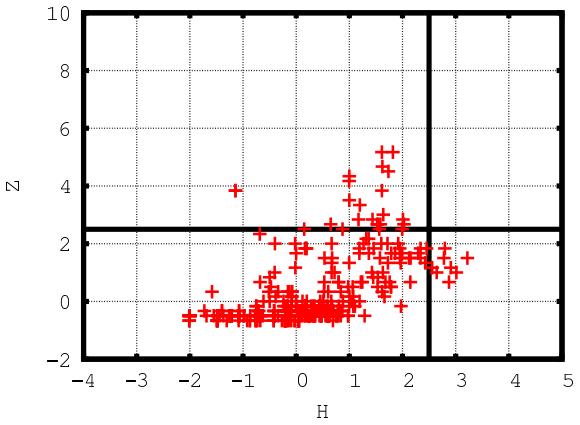


Fig. 13 Node functionality: Modularity-reserved rewiring

rewiring method is close to the original topology.

In summary, the degree correlation between nodes does not determine the failure-tolerant characteristics in the ISPs router-level topologies. This is mainly because the failure-tolerant characteristics are determined by the modularity structure, as we demonstrate in Fig. 12.

5. Conclusion

It is shown that the degree distribution of Internet topologies obey a power-law attribute. However, only the degree distribution does not determine the topological properties of the Internet. This paper presented the failure-tolerant characteristics of ISP's router-level topologies and revealed what topological properties determine the failure-tolerant characteristics. Our results indicate the degree correlation between three nodes does not determine the failure-tolerant characteristics, but the modularity structure of topologies is important for the failure-tolerant characteristics of router-level topologies.

In this work, we focused on topological characteristics due to random failures. However, the attack tolerance is another concern in the power-law networks. We will consider cases involving attack failures in the future.

Acknowledgment

This work was partly supported by Grant-in-Aid for Scientific Research (A) 21240004 of the Japan Society for the Promotion of Science (JSPS) in Japan.

References

[1] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On power–law relationships of the Internet topology," in *Proceedings of ACM SIGCOMM*, pp. 251–262, Oct. 1999.

[2] A. Barabasi and R. Albert, "Emergence of scaling in random networks," *Science*, vol. 286, pp. 509–512, Oct. 1999.

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

[4] L. Li, D. Alderson, W. Willinger, and J. Doyle, "A first–principles approach to understanding the Internet's router–level topology," *ACM SIGCOMM Computer Communication Review*, vol. 34, pp. 3–14, Oct. 2004.

[5] P. Machadevan, D. Krioukov, K. Fall, and A. Vahdat, "Systematic topology analysis and generation using degree correlation," in *Proceedings of SIGCOM 2006*, Aug. 2006.

[6] R. Guimera and L. N. Amaral, "Functional cartography of complex metabolic networks," *Nature*, vol. 433, pp. 895–900, Feb. 2005.

[7] T. Bu and D. Towsley, "On distinguishing between Internet power law topology generators," in *Proceedings of INFOCOM*, pp. 1587–1596, June 2002.

[8] A. Fabrikant, E. Koutsoupias, and C. H. Papadimitriou, "Heuristically optimized trade–offs: A new paradigm for power law in the Internet," in *Proceedings of the 29th International Colloquium on Automata, Languages and Programming*, pp. 110–122, July 2002.

[9] N. Berger, B. Bollobás, C. Borgs, J. Chayes, and O. Riordan, "Degree distribution of the FKP network model," in *Proceedings of International Colloquium on Automata, Languages and Programming (ICALP)*, pp. 725–738, July 2003.

[10] R. Fukumoto, S. Arakawa, T. Takine, and M. Murata, "Analyzing and modeling router-level Internet topology," in *Proceedings of ICOIN 2007*, Jan. 2007.

[11] N. Sprint, R. Mahajan, D. Wetherall, and T. Anderson, "Measuring ISP topologies with rocketfuel," *IEEE/ACM Transactions on Networking*, vol. 12, pp. 2–16, Feb. 2004.

[12] V. Paxson, "End-to-end routing behavior in the Internet," *IEEE/ACM Transactions on Networking*, 1998.