Master's Thesis

Title

A Capacity Dimensioning Method for Efficient and Reliable Communication in Power–Law Networks

Supervisor

Professor Masayuki Murata

Author

Nobutaka Makino

February 15th, 2006

Department of Information Networking
Graduate School of Information Science and Technology
Osaka University

Master's Thesis

A Capacity Dimensioning Method for Efficient and Reliable Communication
in Power–Law Networks

Nobutaka Makino

Abstract

Measurement studies on the Internet topology show that connectivity of nodes exhibit power–law attribute. That is, the probability $p(k)$ that a node is connected to k other nodes follows $k^{-\gamma}$ (γ is a constant). Most researches on power–law networks have focused on investigating how to model the topology of the Internet, but it is apparent that only the degree distribution does not determine the network structure. For example, the structures of the router–level topologies using the working ISP networks are highly clustered; a node connects two or more nodes that also connected each other, while not in the AS topologies and existing modeling approaches. When we study the network–related control like routing control, the most important part is the network structure, so does the link capacity since the capacity dimensioning determine the cost of ISP networks. In this thesis, we study the link capacity in power–law networks. We first investigate that requirements for link capacity in several power–law networks. Among several class of power–law networks, topologies based on BA model require much less capacity than the randomly connected topology, however this is not true for ISP topologies. We next evaluate the link capacity by applying over-provisioning method, and observe that distribution of link capacity in power–law networks also exhibits power–law attribute. That is, power–law networks have a structural property such that large number of links requires low link capacity, while small number of links requires high link capacity. We therefore proposed a capacity dimensioning method that simply utilizes the structural properties by calculating the increase of traffic in case of single failures for each link. Evaluation results show that our proposed method reduces 40% of the amount of link capacity compared to the over–provisioning method.

Keywords

Power–law

Scale–free

Capacity dimensioning

Reliability

Internet topology

Betweenness centrality

Contents

List of Figures

List of Tables

1 Introduction

Researches on the network control in the Internet have evaluated their validity on mesh–like network that have relatively a small number of nodes or random networks in which the number of link connected to a node has a Poisson distribution. It has also shown that the network topology can have a significant effect on the performance of network control as well as network planning in ISP networks. However, measurement studies on Internet topology show that the connectivity of nodes exhibit a power–law attribute (e.g., see [1], [2]). That is, the probability $p(k)$ that a node is connected to k other nodes follows $p(k) \sim k^{-\gamma}$. The fact that the Internet topology exhibits the power–law attribute has much impact on network researches because it has believed that the topology would not show power–law attribute since the Internet is highly engineered.

In recent years, considerable numbers of studies have investigated power–law networks whose degree distributions follow the power–law [3, 4, 5, 6, 7, 8]. Here, the degree is defined as the number of out–going links at a node. The theoretical foundation for the power–law network is introduced in Ref. [9] where they also presents the Barabashi–Albert (BA) model in which the topology increases incrementally and links are placed based on the connectivity of topologies in order to form power–law networks. More precisely, Barabasi and Albert presents a BA model in which the topology grows 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. The resulting power–law networks have two main characteristics: (1) a small number of links are connected with numerous nodes, while a large number of links are connected with a few nodes, and (2) the number of hop–counts between nodes is small (*small–world* property). The characteristic of topologies attained with the BA model is further investigated by other researchers [6]. Bu and Towsley [10] compares the structure of the BA model with AS–level topology. Their results show that 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 increase the preferential probability for high–degree nodes.

In addition to topological modeling for AS–level topologies, several researches focus on flow–level behavior. Goh et. al [6] pointed out that, under minimum hop routing, the distribution in the number of node–pairs that pass through node i, l_i, also follows the power–law, $P_L(l_i) \sim l^{-\sigma}$. Gkantsidis et. al [5] derives the lower bound of "congestion", which is defined as the maximum number of demands that pass through a link in a power–law network. They show that when an approximate multicommodity max–flow min–cut theorem is used, the congestion scales as $O(n \log^2 n)$ where n is the number of nodes. Akella et. al [3] shows how the congestion scales as n increases when single shortest path routing is used. The simulation and analytical results revealed that the congestion scales as $\Omega(n^{(1+\Omega(1))})$, which implies that the congestion increases linearly as the number of nodes n increases. Fabrikant et al. [11] presents an FKP model for generating a power law graph. The model uses the incremental growth model, but the cost for link attachment is different to that for the BA model. The researchers introduce two distance–related metrics for the attachment: the physical distance of nodes, d_{ij}, and the hop–distance to an initial or "root" node. The cost of attachment is the sum of these two metrics, but the physical distance is weighted by α. Depending on the value of α, the resulting topology creates phase transition between the star, exponential, and power–law graphs. The FKP model is further generalized in [12] so that AS–like topologies can be generated. These studies demonstrate that even if the degree distributions of some topologies are the same, more detailed characteristics are often quite different.

There are relatively few studies on router–level Internet topology. Actually, different to AS–level topology, each ISP constructs its own router–level topology based on strategies such as minimizing of the mileage of links, redundancies, and traffic demands. Heckman et al. [13] present parameter settings for topology generator tools, such as BRITE, TIERS, and GT–ITM, to construct ISP topologies. However, the topology they examined is a POP (point–of–presence) level topology. A pioneering work by Li et al. [14] has enumerated various topologies with the same degree distributions, and has shown the relation between the characteristics and performances of these topologies. With the technology constraints imposed by routers, the degree of nodes limits the capacity of links that are connected to. Li et al. also point out that higher–degree nodes tend to be located at the edges of a network, and they then demonstrate in an Abilene–based topology where the power–law network can actually be constructed by maximizing the throughput of the network with the technology constraints imposed by routers. Their modeling method in [14] provides a new insight in that the location of higher–degree nodes are not always located at the core of networks. Although Li et al.'s approach is significant, the Abilene network used in Ref. [14], which is one of scientific networks, is different to other ISP networks as will be discussed in more detail in Sec. 2. The main difference may come from the fact that scientific networks like Abilene provide fewer opportunities to enhance their network equipment because of budgetary constraints, while ISPs make their efforts on enhancement of networks based on their strategies. We therefore focus on realistic ISP topologies such as the Sprint topology and AT&T topology.

Although studies on flow behavior in the AS–level topology and BA topology have been made, it is not studied in the router–level Internet topology. ISPs assign higher link capacity than the minimum of it for transporting current traffic volume to prevent over flow from traffic growth and instantaneous traffic change. It has been observed in [15, 16] that the structural difference much affect the maximum link utilization. Therefore, structural property much impacts on the capacity dimensioning approaches, which is especially important on ISP topologies since cost of link capacity is dominant in ISP networks.

In this thesis, we explore the capacity dimensioning approaches to offer efficient and reliable communications in power–law networks. Currently, ISP simply over-estimate requirements of link capacities (over-provisioning), but if we utilize the structural properties of power–law networks, we can expect that much less capacity is required for some links. As we will discuss in section 3, large number of links requires low link capacity, while small number of links requires high link capacity.

Our next concern is reliability. A work in [17] demonstrates that the power–law structure of BA topology easily makes the topology being disconnected when intentional attack occurs. Here, the intentional attack means that nodes / links are broken down in an ascending order of the number of connection that they pass through. The work also demonstrates that because there are lots of nodes having low degree, the power–law structure is robust against random failures where nodes / links are broken down randomly. As we previously discussed, the structure of ISP topology is much different from AS and BA topologies. We therefore evaluate reliability of ISP topologies that have power–law attribute. Surprisingly, our evaluation shows that ISP topologies are more vulnerable than the BA topology, and increases requirements for link capacities in order to accommodate the traffic detoured from the failed nodes/links. Thus, we propose a capacity dimensioning method to achieve the efficient and reliable communication in ISP networks. It is also shown that in power–law network, large number of links requires low link capacity, while small number of links requires high link capacity. That is, power–law networks have a structural property such that large number of links requires low link capacity, while small number of links requires high link capacity. We therefore proposed a capacity dimensioning method that simply utilizes the structural properties by calculating the increase of traffic in case of single failures for each link. Evaluation results show that our proposed method reduces 40% of the amount of link capacity compared to the over–provisioning method.

This thesis is organized as follows. Section 2 presents related works for modeling the Internet topology and shows some fundamental properties of power–law networks. Section 3 evaluate the reliability in ISP topologies that have power–law attribute. We also evaluate the capacity dimensioning approaches used in the current Internet, and reveal the characteristics when the approach is applied to the topologies. Based on these results, we propose a new capacity dimensioning approach in Section 4. Finally Section 5 concludes the thesis.

2 Related works

2.1 Power–Law networks

It has been observed that the degree distribution of Internet topology exhibit power–law attribute [18]. Here, the power–law attribute of the degree distribution means that the probability $p(k)$ that a node is connected to k other nodes follows $p(k) \sim k^{-\gamma}$. A theoretical foundation for the power–law network is introduced in Ref. [9] where they also presents the Barabashi–Albert (BA) model to generate power–law networks. However, more recent studies on Internet topology show that more detailed characteristics are often quite different [14]. In this section, we describe about the typical topology models that have power–law attributes, and show some fundamental properties of power–law networks.

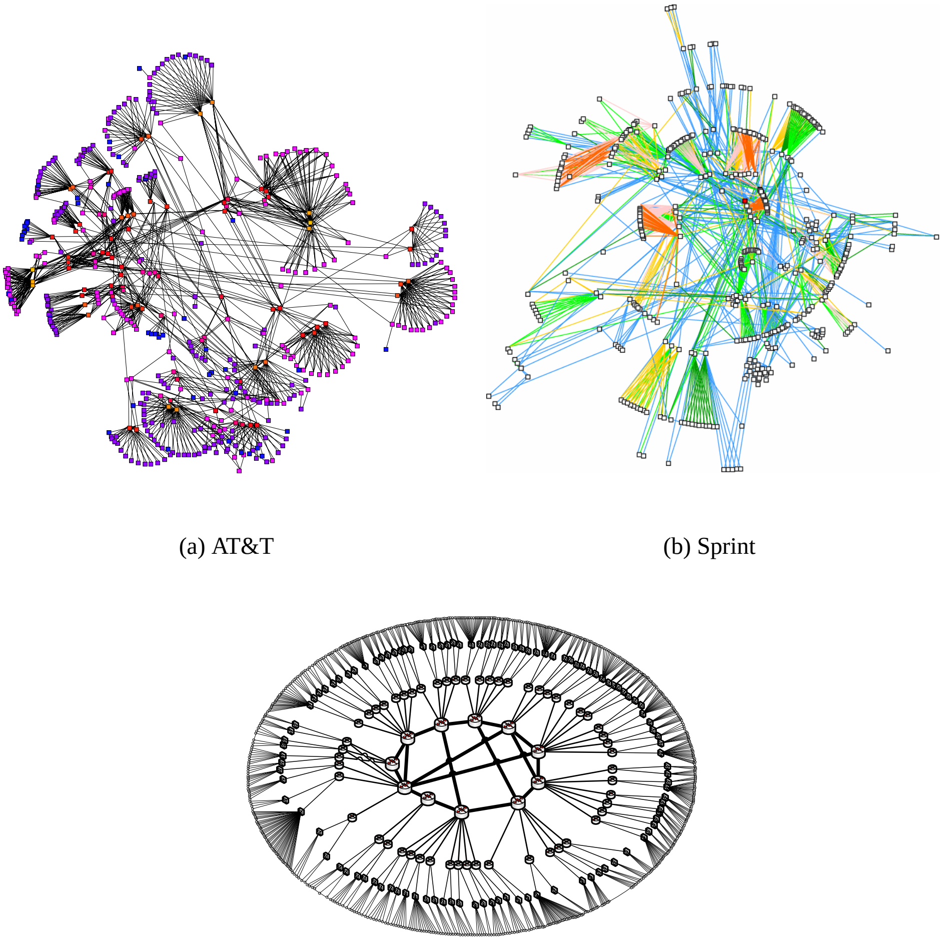
2.1.1 Topologies based on modeling methods

There are many studies that focus on modeling methods for Internet topology. In this section, we first describe the ER (Erdos–Renyi) model in which links are randomly placed between nodes. We next introduce the BA (Barabasi–Albert) model in which the topology grows incrementally and links are placed based on the connectivities of the topologies to form power–law networks. We then clarify the fundamental property of power–law networks generated by BA–model.

ER (Erdos–Renyi) model: The ER model was designed by Erdös and Rényi to describe communication networks. They assumed that such systems could be modeled with connected nodes of randomly placed links usually called random networks. ER model uses two parameters for generating a topology; the number of nodes N is given at first, and every two nodes are connected with the fixed probability p. Thus, the ER model generates a random network that does not have the power–law property. Using the above parameters, ER model generate a random topology by following steps.

Step 1: The node of N piece is arranged

Step 2: The link is put at probability p between all node pairs

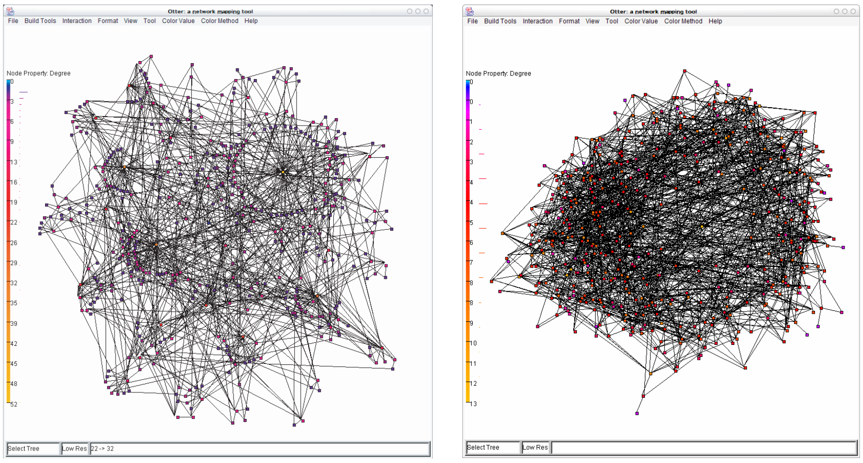


(a) AT&T

(b) Sprint

(c) Abiliene

Figure 1: Visualizations of ISP topologies: AT&T, Sprint and Abiliene topology


Otter: a network mapping tool
File Build Tools Interaction Format View Tool Color Value Color Method Help
Node Property: Degree
0
3
6
9
13
16
19
22
26
29
32
35
39
42
45
48
52
Select Tree
Low Res
22 -> 32
Otter: a network mapping tool
File Build Tools Interaction Format View Tool Color Value Color Method Help
Node Property: Degree
0
0
1
2
3
4
4
5
6
7
8
8
9
10
11
12
13
Select Tree
Low Res

(a) BA Model

(b) ER Model

Figure 2: Network topologies obtained from modeling methods

The probability $P(k)$ that a node has degree (number of links) k is given as

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

In addition, with large N and small p, Eq. (1) becomes

$$P(k) = \lambda^k e^{-\lambda}/k!, \tag{2}$$

where $\lambda = pN$. From Eq. (2), the distribution of the degrees of the nodes in a random network generated by the ER model follows a Poisson distribution [19].

BA Model: Barabasi and Albert designed their model to emulate the growth of such large–scaled networks as the Internet. The BA model is characterized by two features that the ER model does not have: *Incremental Growth* and *Preferential Attachment*. Generating a topology is started with a small number of nodes m_0.

(1) *Incremental Growth*: Add a new node at each time step.

(2) *Preferential Attachment*: Connect the new node with two other different nodes, which are chosen with the probability P_i (k_i is the degree of node i).

$$\Pi(k_i) = k_i / \sum_j k_j. \tag{3}$$

Theoretical foundations have been investigated in [9, 8]. Reference [9] demonstrates that the BA topology has a characteristic that a small number of links are connected with numerous nodes, while a large number of links are connected with a few nodes (*scale–free* property.) Reference [8] shows that the number of hop–counts between nodes are small (*small–world* property.)

2.1.2 AS topologies

In the Internet, the degree distribution has been shown to follow the power–law at the AS–level [1, 2, 20]. Bu and Towsley [10] compares the structure of the BA model with AS–level topology. Their results show that 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 increase the preferential probability for high–degree nodes.

2.1.3 ISP topologies

Li et al. [14] enumerated various topologies with the same degree distributions, and showed the relation between their structure and performances of those topologies. They pointed out that because of a technology constraint of commercial routers, high–degree nodes [1] accommodate low–bandwidth access lines while lower–degree nodes accommodate high–bandwidth core lines because of technology constraints with commercial routers. Due to technology constraints, the hub node is located at the edges of the network, while in the AS–level topology the hub node is located at the core of the network. With a three–level hierarchical structure based on the Abilene network and the previously mentioned link capacity constraints, Li et al. show that there exists a topology such that the throughput of the topology is maximized while the degree distribution follows a power–law. In the Abilene–based topology presented in Fig. 6 (e) of Ref. [14], there are no redundant links between nodes (except in network cores), and a single node/ link failure will easily split the network, while the ISP topologies presented in Ref. [21] clearly include redundant links (see Fig. 1). Therefore, we cannot apply their modeling method to traffic flow level researches like routing control.

[1] We call several nodes with a much larger number of outgoing links than other node as “hub nodes” without clear definition.

ISP topologies used in this thesis is obtained by trace–route based measurement [21]. Figure 4(a) and figure 4(b) shows degree distribution of AT&T and Sprint topologies, respectively. We observe that in either network, the degree distribution exhibit power–law with slope $\gamma = -1.7$.

2.2 Structural properties of network topologies

Structural properties of ISP topologies To compare how structure for router–level topology affects the basic properties of networks, we prepare three topologies that have the same number of nodes and links. For the router–level topology, we use topologies generated by the BA model and the ER topology generated by the ER model. The degree distributions for these topologies are shown in Figs. We can confirm that the degree distribution for the Sprint topology and AT&T topology follows a power–law. We use the following metrics for node i to investigate the characteristics of topologies:

$A(i)$, $D(i)$: Average and maximum number of hop–counts from node i to all other nodes. Hereafter, we will call the maximum hop–counts as diameters.

$C_e(i)$: Cluster coefficient [22] for a node, which is defined as

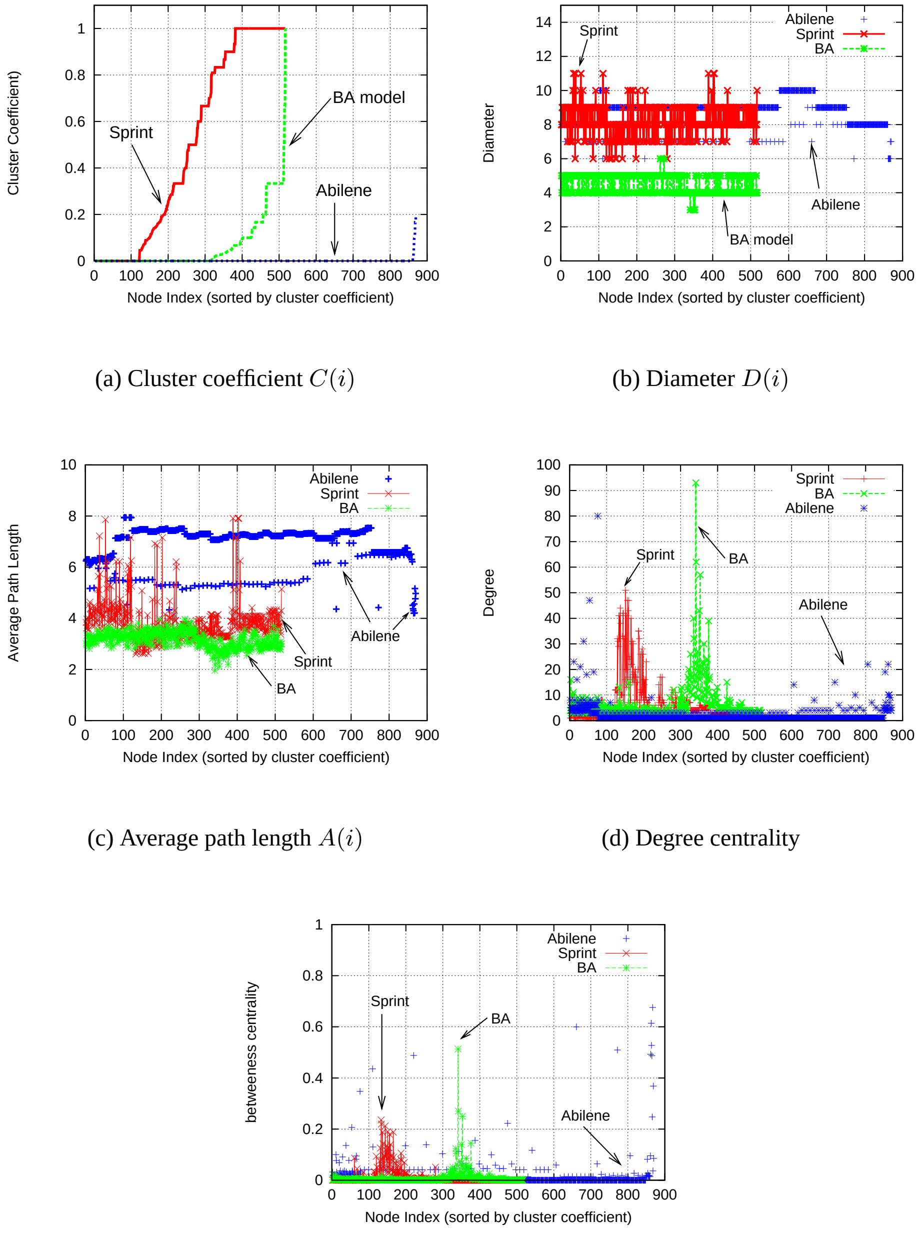
$$C_e(i) = \frac{2E_i}{d_i(d_i - 1)}, \tag{4}$$

where d_i is the degree of node i, and E_i is the number of links connected between node i's neighbor nodes.

We also consider two centrality measures; degree centrality and betweenness centrality [19]. For each node i, degree centrality is defined as the degree of node i, and betweenness centrality is defined as the number of node–pairs that pass through node i. The cluster coefficient for each node is ranked in ascending order in Fig. 3(a). In the figure, the results of the Abilene topology are also presented. We can see that the cluster coefficient for the Sprint topology is much larger than that for the BA topology that is generated from BA model. Furthermore, the results in Figs. 3(a) and 3(d) show that lower–degree nodes are more highly clustered with the Sprint topology; a node with two out–going links always forms a cluster, while higher–degree nodes do not always have a high cluster coefficient. Other interesting observations can be seen in Figs. 3(b) and 3(c), which show the diameter $D(i)$ and average distance $A(i)$ from each node; both with the Sprint topology are larger than those with the BA topology. A node in the BA model tends to be connected to higher–degree nodes, and therefore any two nodes communicate with smaller hop–counts via the higher–degree nodes. However, the results for the router–level topology do not exhibit this effect. Since the average distance with the Sprint topology is larger than that with the BA topology, the small world property no longer hold with the router–level topology.

The Abilene topology shows quite different characteristics in Fig. 3(a). With the Abilene topology, the cluster coefficient is even lower than the BA topology, and the average path length is much longer than the Sprint topology and the BA topology. The reason for this is apparent in that the Abilene topology is three–level hierarchical topology. As previously discussed, the structure of router–level, especially ISP–level topologies, is very different from the BA and Abilene topologies. In the next section, we evaluate how these structural differences affect the performance of networks.

Fundamental properties of ER and BA models Figure 5(a) and figure 5(b) show complementary cumulative distribution functions $F(d)$ of node degrees d in the topologies generated by the BA and ER models. There are 1,000 nodes. In the ER model, the connected probability p to 0.002, which generates 2,066 links. In the BA model, the number of initial nodes m_0 is 2, and the number of additional links for each node growth, we add 2 links for the topology. The resulting topology has 1,997 links where the number of links is almost the same to the ER topology. Figure 5(a) is the results for BA model and Figure 5(b) is the results for ER model. Figure 5(b) shows that the distribution of node degrees of the random network approximately follows a Poisson distribution. On the other hand, in Figure 5(a), distribution of the degrees of the power–law network is approximately aligned on a log–log plot, which indicates the distribution follows the power–law.



(a) Cluster coefficient $C(i)$

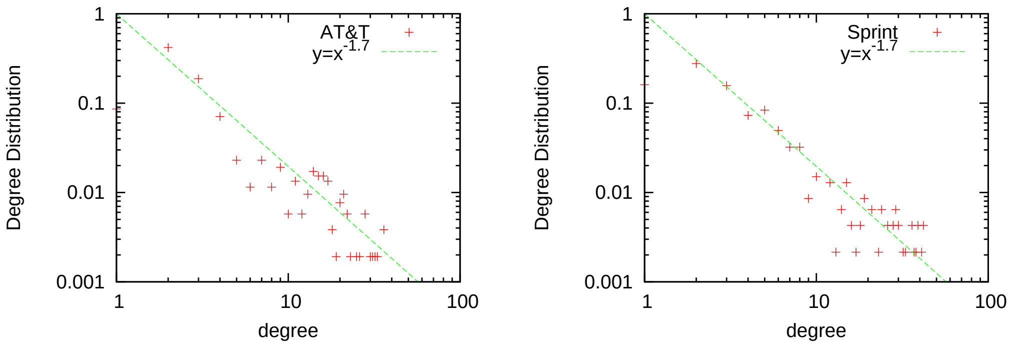
(b) Diameter $D(i)$

(c) Average path length $A(i)$

(d) Degree centrality

(e) Betweenness centrality

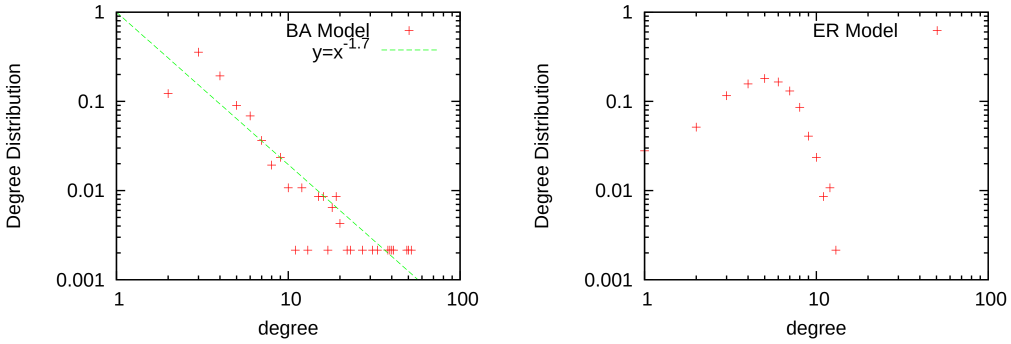
Figure 3: The basic properties of the router–level topology: Comparison among Sprint, BA and Abilene topologies



(a) AT&T

(b) Sprint

Figure 4: Degree distribution of ISP topologies



(a) BA Model

(b) ER Model

Figure 5: Degree distribution of model–based topologies

3 Capacity dimensioning in Power–Law networks

In this section, we apply the over–provisioning approach as conventional capacity dimensioning method, and then evaluate requirements of link capacity in power–law networks. In the over–provisioning approach, we give a higher link capacity than the minimum of its requirements to convey the traffic. Here after, we will call over–provisioning approach as conventional capacity dimensioning method. In conventional capacity dimensioning method, we give a residual capacity on a link with the stable fraction for the amount of traffic on the link. The fraction of the residual capacity is selected based on a experience. Usually, the residual capacity is added such that the link utilization would be within the range of 30% to 50%. In this approach, there is a possibility that we can decrease the amount of traffic in case of failures and the cost of link capacity by evaluating the amount of traffic that is increased by a failure, or by exploiting the structural property of power–law networks.

First of all, we evaluate the amount of investment and the resilience of the network against failures in the conventional capacity dimensioning method, and clarify the relationship between the required link capacity and reliability against network failures. Moreover we investigate the distribution of the bandwidth determined by the conventional capacity dimensioning method. In section 3.1, we examine the characteristics of the rerouted traffic by failures to clarify the property of the power–law network. In section 3.2, we discuss about the overview of conventional capacity dimensioning method and simulation models for evaluation. In section 3.3, we investigate what kind of the failures, and how many failures the network can tolerable by the conventional dimensioning method. We finally discuss about its relationship to the cost of capacity equipment.

3.1 Propoerties of power–law networks against failures

In this section, we clarify the behavior of the power–law network when a failure occurred. We evaluate the number of shortest paths on the link. In this case we consider the shortest paths between all node pairs. The shortest paths detour in case of failures. In such case, the number of node pairs on the link changes. A number of detoured paths may concentrate on a certain link. This number of paths are considered as the amount of traffic when the uniform traffic matrix are given in a network. We can explore the characteristics of the link load when failure occurred, by evaluating the distribution and the increase of the number of shortest paths.

We describe about the way to calculate the number of node pairs. The node pair is assumed to be the all node pairs, and the paths are consists of shortest paths. We count the number of there shortest paths over a link. The target topologies are AT&T topology, Sprint topology, the topology based on BA model and the topology based on ER model.

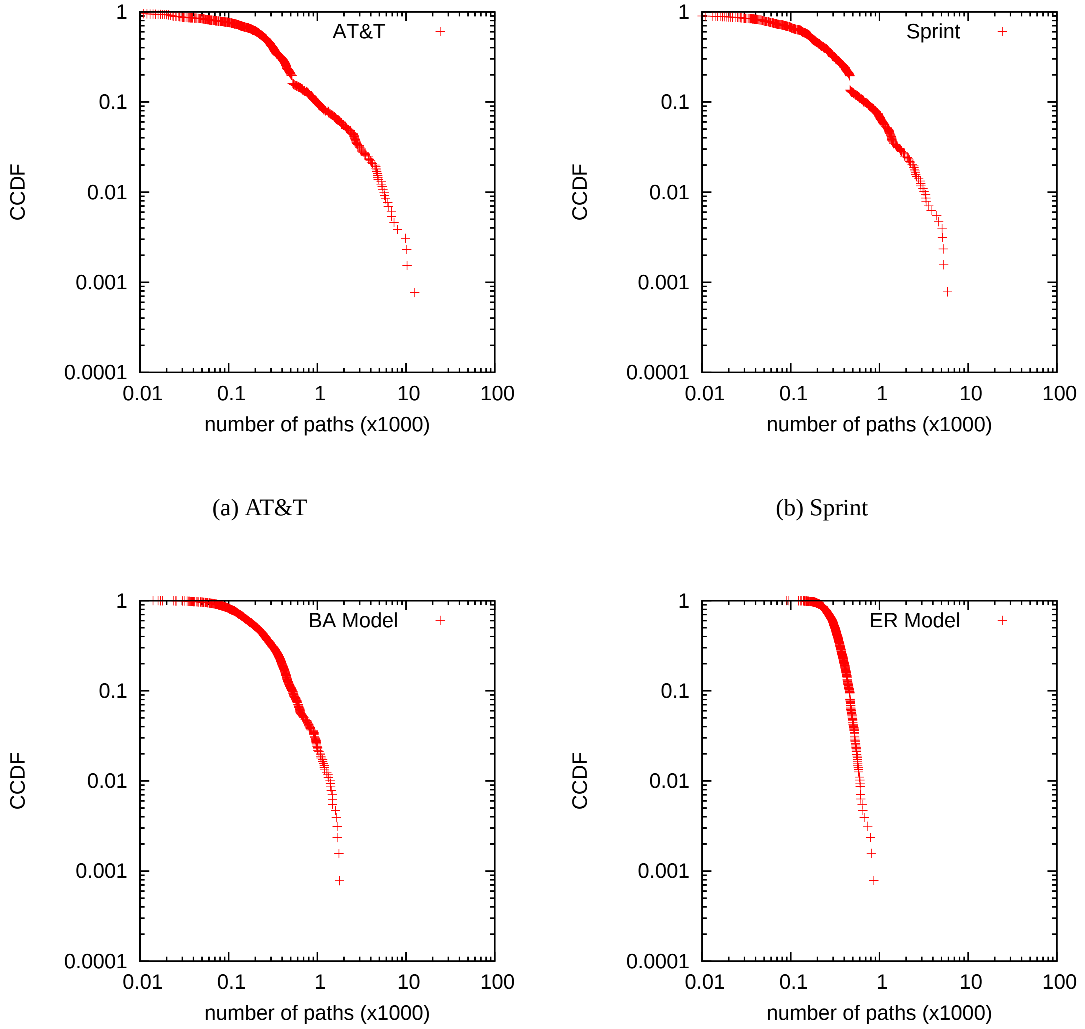
3.2 Property on load concentralion

Figure 6 shows the distribution of number of shortest paths that passes through the link on the network when no failure occurs. The horizontal axis represents the number of node pairs that passes the link, and the vertical axis represents the complementary cumulative distribution function in terms of the number of shortest paths. This figure shows that the number of paths are widely distributed from the small number of paths to the large number of paths in the topology of AT&T and Sprint. On the other hand, in the ER topology, the number of shortest paths is narrowly distributed, and we observe that the number of shortest paths on the link is small. In topology generated by BA model, the distribution of the number of shortest paths that pass on the link also narrowly distributed like ER topology though it has the similar distribution of degrees to the one of ISP topologies.

We can say that ISP topologies have more a tendency that traffic concentrate on certain links than the case of BA topology. Therefore it is expected that if we increase capacities on links that traffic concentrate, the resilience of networks increases. The ER topology has a narrow distribution of the number of shortest paths, the resilience will be increase by simply increasing the capacity of links uniformly. In the BA topology, since it has narrower distribution of number of shortest paths, relative uniform increase of link capacity will make the network adaptive to the failures. unlike the case of ISP topologies, BA topology has many links that connects two nodes far apart because the length of links are not constrained by the physical length. This makes BA topology have a lot of long distance detouring paths, which decreases the concentration of the number of shortest paths on a link than ISP topologies.

3.3 Overview of conventional capacity dimensioning method

In this section we describes about the simple mechanism of conventional capacity dimensioning method used in the current ISP networks. Then we state about the simulation model to evaluate



(a) AT&T

(b) Sprint

(c) BA Model

(d) ER Model

Figure 6: Complementary cumulative distribution of number of paths that pass through a link

the conventional capacity dimensioning method. We evaluate this capacity dimensioning method to clarify the relationship between tolerance and amount of link capacity allocated on the links.

In conventional method, we introduce the over provisioning ratio R. R is a ratio of the residual link capacity to the amount of traffic that flows on a link. If a link has a certain amount of traffic, say X bps, and over provisioning ratio R is given, the room of the capacity is configured as $X \cdot R$ bps, and amount of the capacity of the link is set to $X(1 + R)$.

Next we state about the simulation conditions for evaluation. To make things simpler, we use the number of shortest paths that pass on a link as the substitute for the amount of traffic on that link in this simulation. We consider all the shortest paths between all node pairs. The amount of traffic on a link as above can be considered to the amount of traffic generated by the uniform traffic matrix in the same topology.

If the amount of traffic and over provisioning ratio R are given, the required capacity is determined as $X(1 + R)$. Next we introduce the following eight kinds of discrete bandwidth: respectively 100Mbps, OC–3 (150Mbps), OC–12 (600Mbps), OC–24 (1.2Gbps), OC–48 (2.4Gbps), OC–96 (4.8Gbps), OC–192 (9.6Gbps), and 19.6 Gpbs. The one starts by ”OC” is a name of the communication standard of SONET. For each links, one of the bandwidth that is larger than the required capacity $X(1 + R)$ is selected. In order to allocate 9.6Gbps to the link with the highest capacity, we introduced a conversion ratio k as $1/5$ Mbps per a path. With this ratio k we convert the number of shortest paths on a link into the corresponding link capacity or bandwidth.

In our evaluation, we choose three over provisioning ratio R as 1.0, 2.0, 4.0. We use the topologies shown in Fig. 4 and Fig. 5, and we evaluate when link failures occur. The failure is simulated by simply deleting the link or the node on the network. After the deletion of link or node, we recalculate the number of shortest paths over each links and evaluate the amount of traffic.

We evaluate the conventional capacity dimensioning method in two measures. One is the amount of traffic exceeded the configured bandwidth as the tolerance to the failure. The other is the sum of the configured bandwidths for all links as the cost of investment. At last we clarify the relationship between the amount of exceeded traffic and the cost of investment that we evaluated above.

Table 1: Topologies used in evaluation and its fundamental properties

name	number of nodes	number of links	type	gamma of power–law
AT&T	522	1079	measurement	1.7
Sprint	466	1029	measurement	1.7
BA	466	1028	model based	1.7
ER	466	1028	model based	–

3.3.1 Topologies

We describe about the topologies used in this evaluation. We focus on the four topologies of the topologies introduced in section 2.1: AT&T topology and Sprint topology as the measured ISP topologies, the topology based on BA model which has the power–law properties in its degree distribution and the topology based on ER model which has the exponential distribution in its degree distribution.

The number of nodes and links in each topologies are follows. The AT&T topology consists of 522 node 1079 links that is based on the result of the topology measurement project in ref. [21]. The Sprint topology is also obtained from topology measurement [21] and consists of 466 nodes 1029 links.

We generated the model–based topologies based on BA or ER models that have the same number of links and nodes to Sprint topology to compare them easily. In BA model, there are three parameters: the number of initial nodes m_0 , the number of links added per node m, the total number of nodes N. Once we choose the number of node N, the number of the initial nodes m_0, the number of links added per node m then the number of links is calculated to $m_0(m_0 - 1)/2 + m(N - m_0))$. We adjusted the number of added links per node m with probability in order to get desired number of links and got the topology consists of 466 nodes and 1028 links. In ER model, we choose the probability p moderately with which probability the links between two nodes, and we got the topology consists of 466 nodes and 1028 links.

Table 1 summarizes the fundamental properties of four topologies. Figure 4, figure 5 and figure 6 already showed the distribution of degrees and the distribution of link loads respectively. In next section, we describe about the failures we consider on these topologies.

3.3.2 Failure model

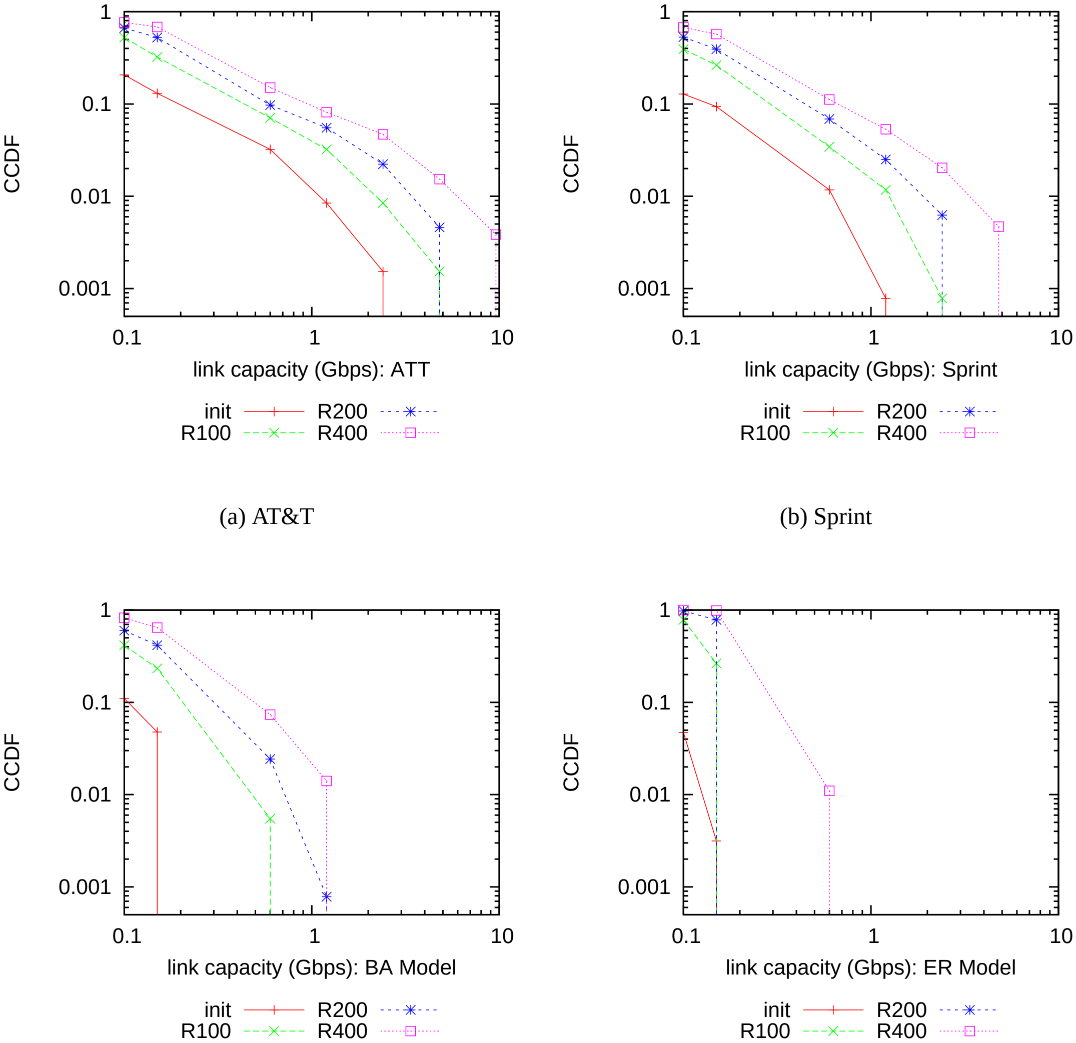
We describes about the failure model used in evaluation. We consider two failures. One is a random failure to a link that assumes the case that a link become unavailable by a failure of a part of a network equipment or the miss configuration of route settings. The other is an intentional attack to specific link that assumes the case that someone attacks the link to be failed or the worst case of random failure.

The failure is imitated by excluding the selected links from the network topology. In a random failure to the link, some links are selected from each topology at random. In the intentional attack to the link, the link with the number of node pairs that passes the link are selected sequentially. The number of links that break down is assumed to be from 1% to 10% of the number of links in the networks. We evaluated the number of failures from 5 to 90 at intervals of 5.

3.4 Evaluation of conventional method

3.4.1 Distribution of link capacity

To investigate the feature of a conventional capacity dimensioning method, we examine the distribution of the bandwidth allocated by the conventional method. Figure 7 shows the result. The horizontal axis is a value of bandwidth, vertical axis is a complementally cumulative distribution. We evaluated the cases of over provisioning ratio R is 1.0, 2.0 and 4.0. Fig. 7 shows that the bandwidths are distributed widely in the topology of AT&T and Sprint. It also shows that the higher over provisioning ratio R makes wider distribution of the bandwidth. In the topology based on ER model, there are smaller bandwidths in narrow range compared to the topologies of AT&T and Sprint. Moreover in ER topology, large bandwidth are rarely required when the over provisioning ratio R becomes higher. In the topology by the BA model, the configured bandwidths are not too large though it has the similar distribution of degrees as the topologies of AT&T and Sprint. These characteristics in distribution of the bandwidth are similar to the one of the number of shortest paths described in Figure 6 of previous section. In the next section, we evaluate the relationship between tolerance to the failures and a cost of investments in conventional capacity dimensioning.



(a) AT&T

(b) Sprint

(c) BA Model

(d) ER Model

Figure 7: Complementary cumulative distribution of link capacity

3.4.2 Effects of over–provisioning against failures

In this section we examine the characteristic of the conventional capacity dimensioning method in case of random failures and intentional attack that described in section 3.3.2.

If a failure occurs in a network, the traffic that flows on the link detours and the amount of traffic of the specific link increases. In this section, at first, we evaluate the amount of traffic that exceeds the bandwidth of the link as the tolerance of conventional method against the failures. Next we evaluate the sum of the configured bandwidth on links as the investment amount. The number of failures is set to 3% of the 1028 links. Over provisioning ratio R of the conventional method is set to 0.0, 1.0, 2.0 and 4.0.

Tolerance to random failures Figure 8 shows the relationship between the number of random failures and the amount of traffic that exceeds the allocated bandwidth. The horizontal axis indicates the number of failed links. The vertical axis is the amount of traffic that exceeds the allocated bandwidths in all links. The lines corresponds to each over provisioning ratio R.

This figure shows that if random failures occur, the amount of detoured traffic do not exceed the allocated bandwidth on each link in the topology of AT&T, the BA model and the ER model. In the topology of Sprint there is a little amount of traffic exceeds the allocated bandwidth with the over provisioning ratio is set to 0.0 or 1.0 though there is no traffic exceeds the link capacity with other ratio ($R = 2.0, 4.0$).

Figure 9 shows the sum of the bandwidth allocated on all links in the network when the random failure occurred. The horizontal axis shows the number of failures and the vertical axis shows the sum of the amount of bandwidth and amount of traffic that exceeded the bandwidth. The value when the number of failures equals zero is the sum of the bandwidth allocated by the capacity dimensioning method. If this is small, the investment amount to the bandwidth is small. The other values are the summation of bandwidth and amount of traffic exceeds the bandwidth (e.g. shown in fig. 8), that is the sum of the required bandwidth by the failure.

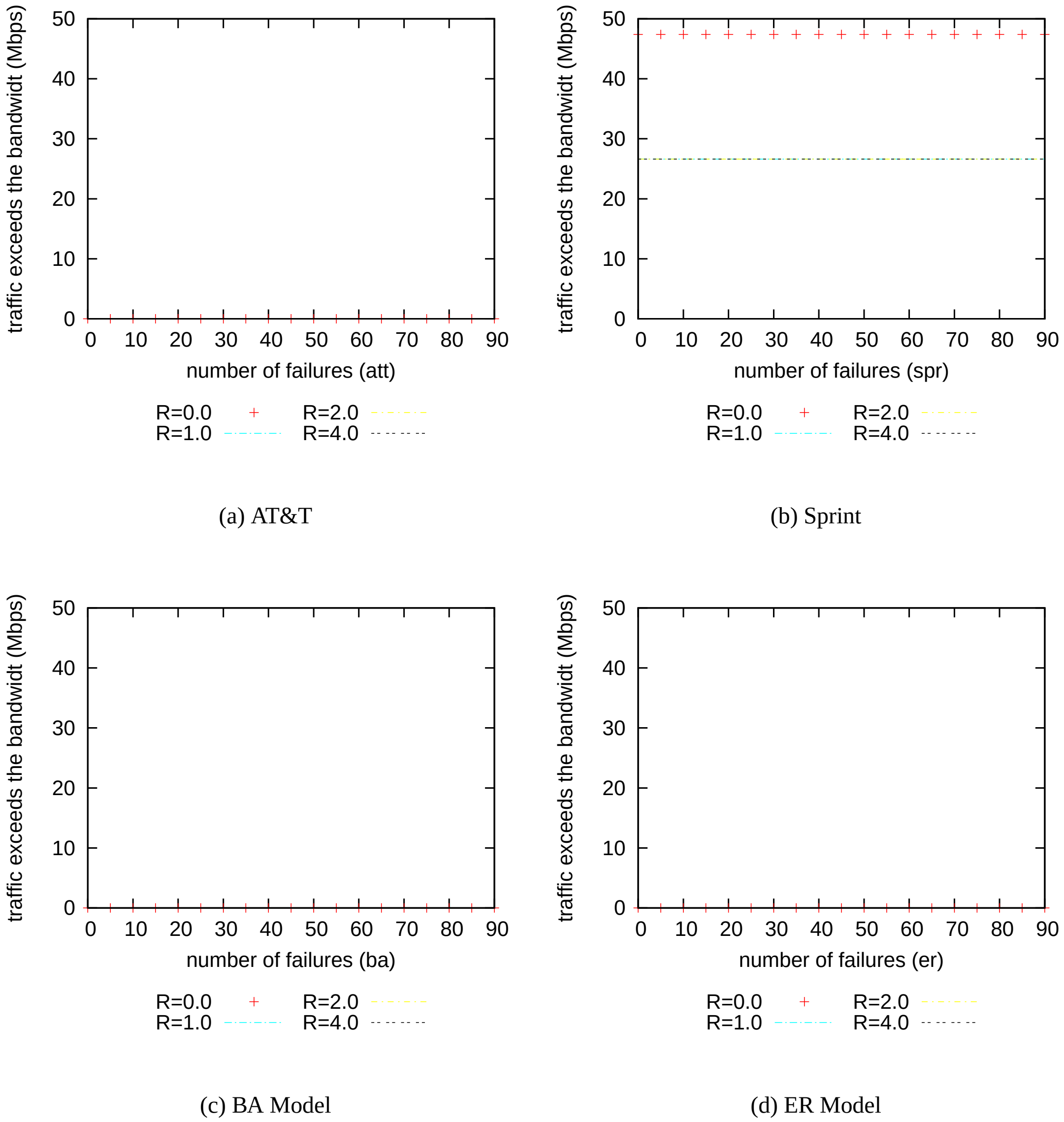
This figure shows that the smaller over provisioning ratio R makes the amount of bandwidth required in the network smaller. Because the required bandwidth are flat in all topologies, we can say that the increase of traffic caused by this scale of random failure is smaller than over provisioned bandwidth. These results show that we can decrease the investment amount and enable the cost efficient capacity dimensioning by lowering the over provisioning ratio R in case of this scale of random failures.

Tolerance to intentional attacks Next, we evaluate the tolerance to the intentional attack of the conventional capacity dimensioning method.

Figure 10 shows the relation of the number of failures and the amount of traffic that exceeds the link bandwidths when intentional attacks are performed in the networks configured by conventional capacity dimensioning method. In contrast to the random failures, there are large amount of traffic that exceeds the link capacity. In the topologies of AT&T and Sprint network, the amount of traffic that run over the bandwidth largely increases as the increase of the number of failures. On the other hand, in the topology based on BA model and ER model, there is little traffic exceeds the bandwidth when the over provisioning ratio R is larger than 1.0. This shows that ER and BA topology is more tolerance to intentional attack than other ISP measured topologies. Although ref. [17] insists that BA topologies are less tolerant to ER model, the ISP topologies are much less tolerant than BA topologies.

Next we focus on the result when number of failures is around 30, which is a 3% of the number of links in each topologies. In AT&T and Sprint topologies, there are more than 40 Gbps of exceeding bandwidth on the network. This indicates the conventional method cannot assign the appropriate link capacity the links against traffic increase. On the other hand in BA model, there is little amount of exceeding traffic at the number of failures is 2% of all links when the over provisioning ratio $R = 1.0$. If we choose the ratio $R = 2.0$, over provisioning method works well as far as the 3% of all links fails. This indicates that conventional method works well in BA topology.

Figure 11 shows the sum of the required link capacity when the same intentional attacks are performed as in Fig.10. This shows that the smaller over provisioning ratio R makes the sum of the bandwidth allocated in the network smaller. In this figure it is found that the amount of allocated bandwith are almost the same in Sprint, BA and ER topologies. It is interesting that the similar investment amount makes different amount of traffic exceeds the configured bandwidth. It is also found that AT&T topology required double of investment amount with the same over provisioning ratio R compared to the Sprint topology.



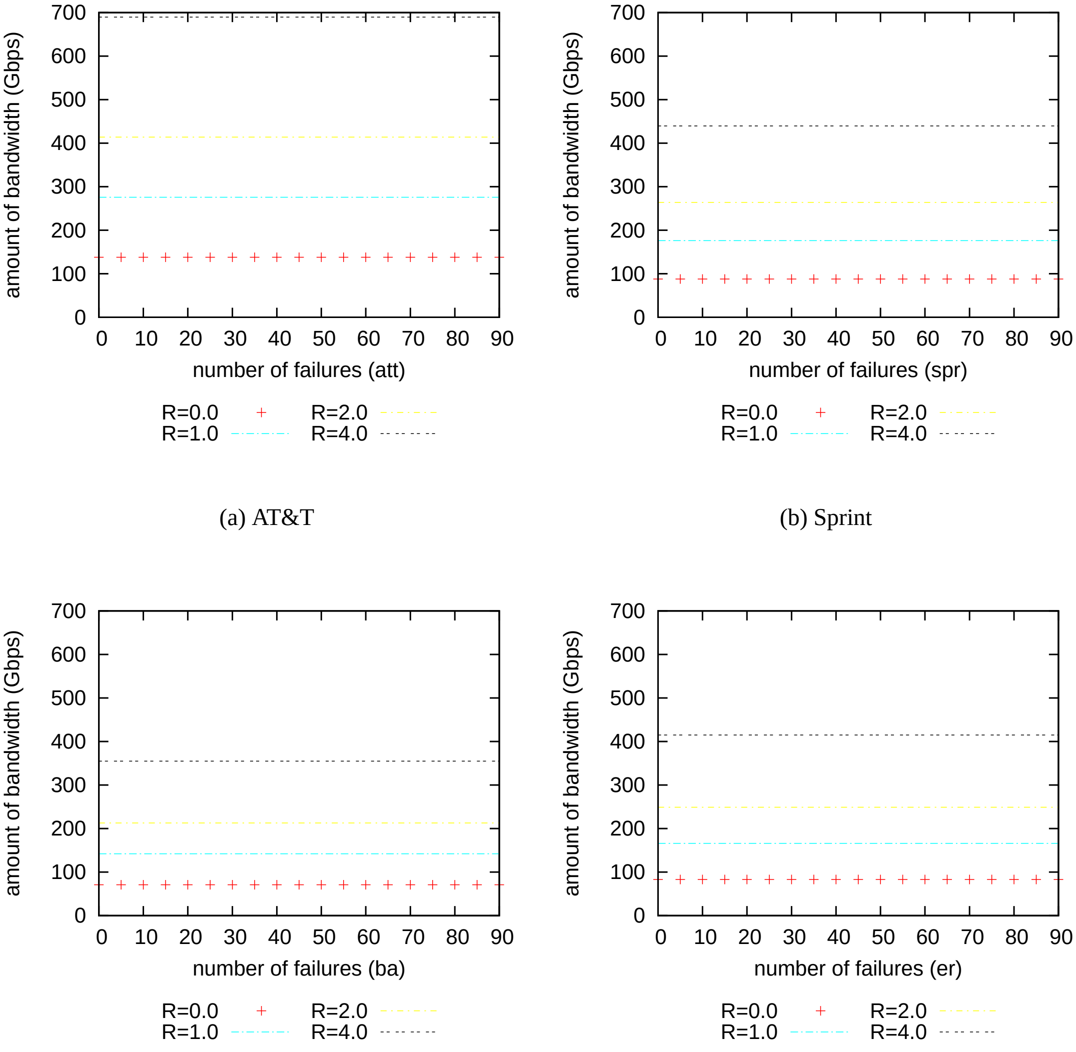
(a) AT&T

(b) Sprint

(c) BA Model

(d) ER Model

Figure 8: Amount of additional link capacity required when multiple failures occur: over–provisioning and random failures



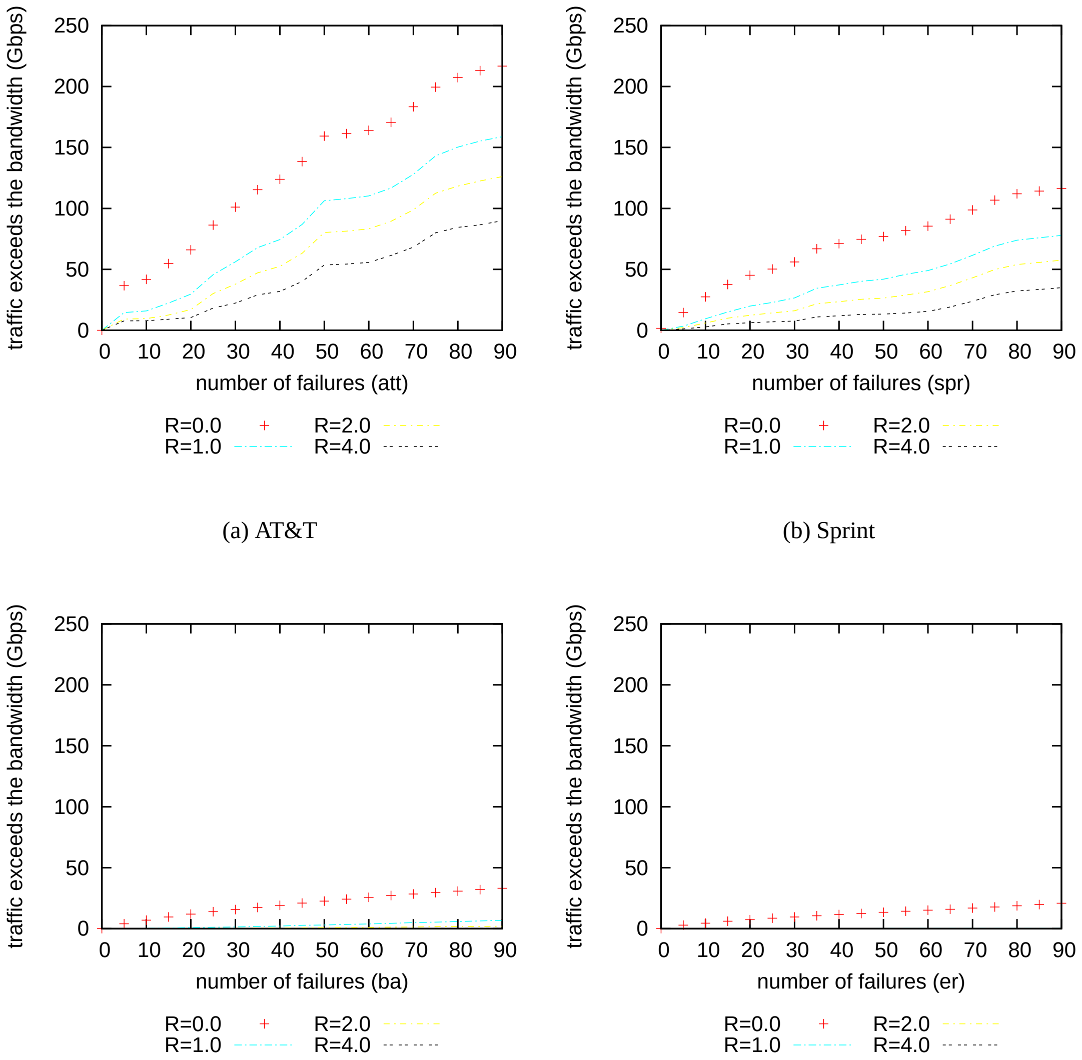
(a) AT&T

(b) Sprint

(c) BA Model

(d) ER Model

Figure 9: Amount of total link capacity required when multiple failures occur: over–provisioning and random failures



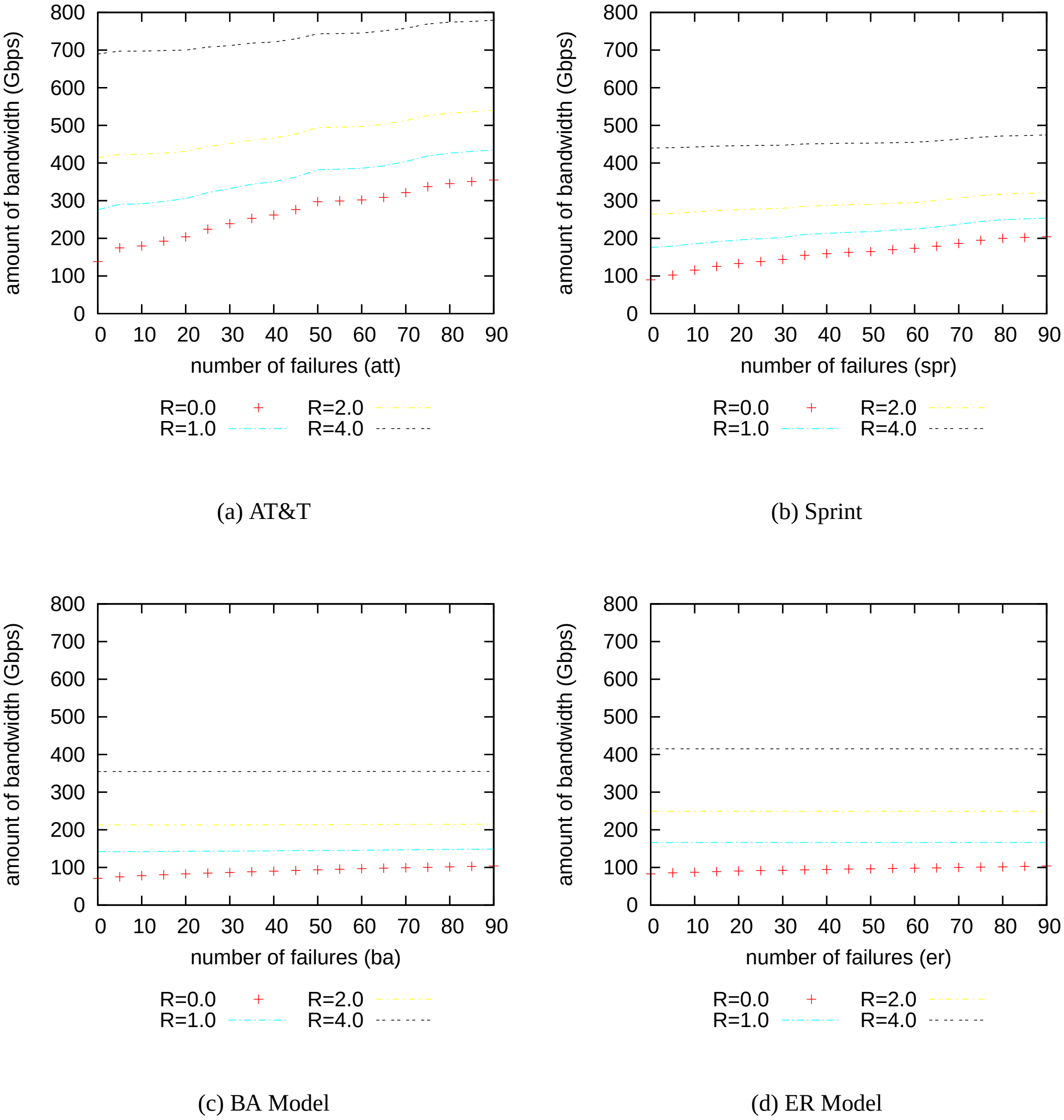
(a) AT&T

(b) Sprint

(c) BA Model

(d) ER Model

Figure 10: Amount of additional link capacity required when multiple failures occur: over–provisioning and intentional attacks



(a) AT&T

(b) Sprint

(c) BA Model

(d) ER Model

Figure 11: Amount of total link capacity required when multiple failures occur: over–provisioning and intentional attacks

4 New capacity dimensioning method for power–law networks

In previous section, we evaluated the conventional capacity dimensioning method in ISP topologies and model–based topologies. Conventional method is much tolerant to the random failure, for example, the breakdown of 10% of links causes no traffic that exceeds the configured bandwidth in AT&T, BA and ER topologies. On the other hand, conventional method has large amount of traffic that exceeds the allocated bandwidth in case of intentional attack to the 1% of the links in ISP topologies. That is, the conventional method didn't assign the appropriate bandwidth for links against intentional attacks in ISP topologies. We also found that if we allocate the optimal bandwidth, the amount of the bandwidth allocated on the network will be improved by 50%. There is a room of improvement to lower the investment amount and adapt to intentional attacks by allocating bandwidth with a thought of intentional attacks.

In this section, we propose the capacity dimensioning method that has tolerance to the intentional attacks and lowers the investment amount. Our method aim to fully decrease the traffic exceeds over the allocated bandwidth with the breakdown of the 1% of links and to lower the sum of the allocated bandwidth on the network by intelligent capacity dimensioning.

4.1 Overview of proposed method

The conventional capacity dimensioning method has less tolerance to intentional attacks that have different characteristics compared to the that of random failures though conventional method has a tolerance to the random failures which leads the small increase of traffic that exceeds the allocated bandwidth. In order to work well with intentional attacks, we have to consider the peculiar characteristics in the distribution of its increase of traffics. In this section, we propose a new capacity dimensioning method that predicts the distribution of increasing traffic generated by intentional attacks, by overlapping the distribution of all intentional attacks to single link. The outline is shown as follows.

First of all, we focus on the number of the detoured shortest path that passes over the link when single failure occurs in a network, and we calculate the basic distribution of the increase of traffic. Let init(l) to be the number of shortest paths that passes the link l when there is no failures, load(l, x) to be the number of shortest paths that passes over the link l when another link x went down. Then let max_diff(l) to be the maximum number of shortest paths increased by a single failure as equation 5.

$$\mathrm{max\_diff}(l) \quad := \quad \max_{x \subset L} (\mathrm{load}(l, x)) - \mathrm{init}(l) \tag{5}$$

In proposed method A, we simply assume the amount of traffic increased by the failure of N links is the same to N times of a case of single failure. We define cap1(l) as the number of shortest paths that each link will receive in worst case, as equation 6. Here N is the number of failures to be assumed to occur.

$$\mathrm{cap1}(l) = \mathrm{max\_diff}(l) \times N + \mathrm{init}(l) \tag{6}$$

In proposed method B, we assume the amount of traffic increased by N link failures is the same to a summation of largest N cases of single failure. Let topsum(l,N) to be a summation of largest N values of load(l,x) for changing x, and we set cap2(l) as the number of shortest paths that link(l) would receives as equation 7.

$$\mathrm{cap2}(l) = \mathrm{topsum}(l, N) + \mathrm{init}(l) \tag{7}$$

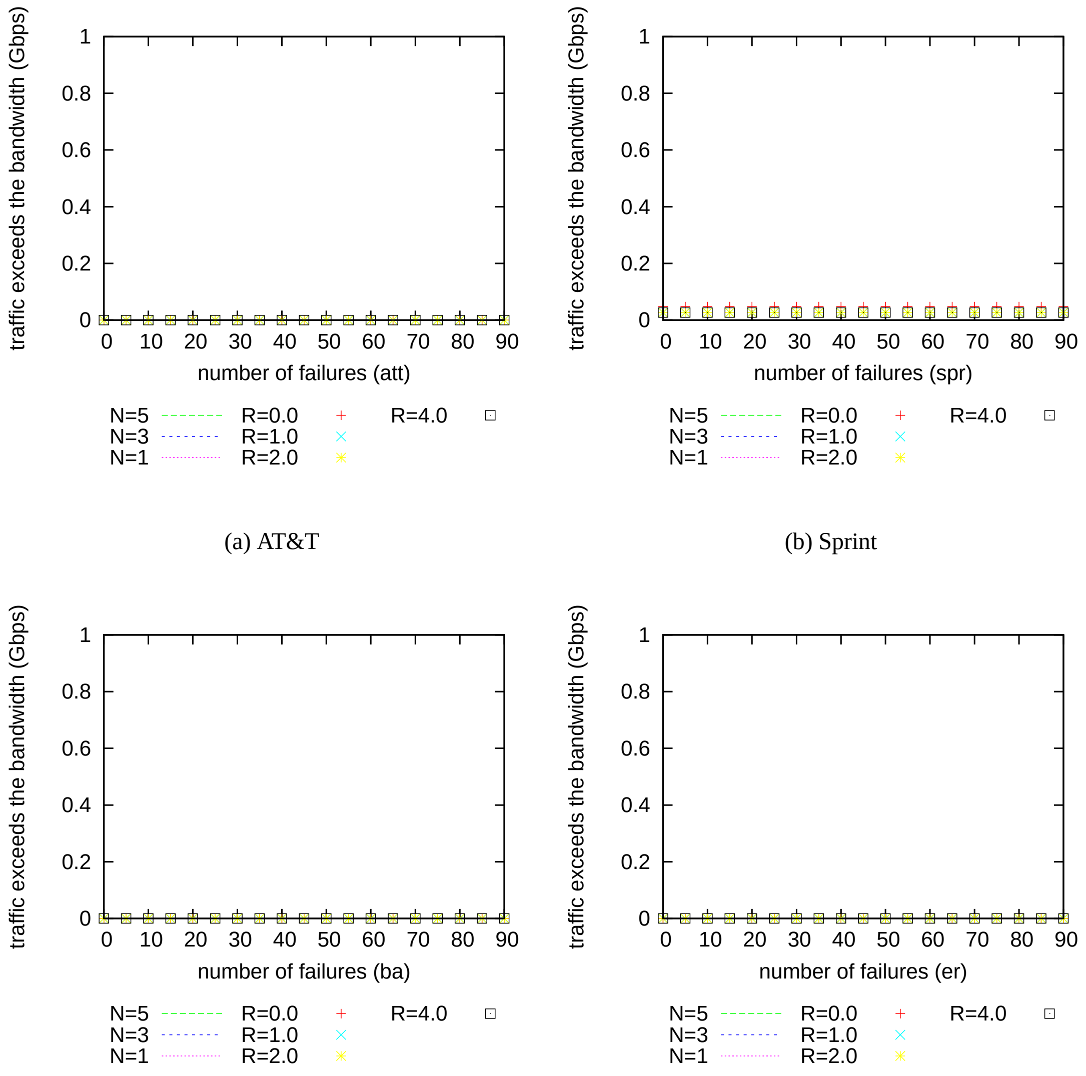
The bandwidth allocated on links are chosen based on cap1(l) and cap2(l) by the same way used in section 3.3, that is we use proportional constant k as $1/5$ Mbps/path and select the bandwidth larger than $k \cdot \mathrm{cap1}(l)$, $k \cdot \mathrm{cap2}(l)$ respectively.

4.2 Evaluation of proposed method

In this section we evaluate the amount of traffic that exceeds the bandwidth of the link as the tolerance of conventional method against the failures, the sum of the configured bandwidth on links as the investment amount, that are same measures used in section 3.4. Our proposed method aim to decrease the exceeding traffic over the bandwidth and reduce the investment amount for bandwidth in the network when 1% of the links are broken by intentional attack.

4.2.1 Tolerance to random failures

Figure 12 and figure 13 show the evaluation result of proposed method 1 when random failures are performed in the network. Figure 14 and figure 14 are the evaluation results of proposal method 2. In both cases proposed method can decrease the exceeding traffic though the amount of allocated bandwidth is larger than conventional methods.



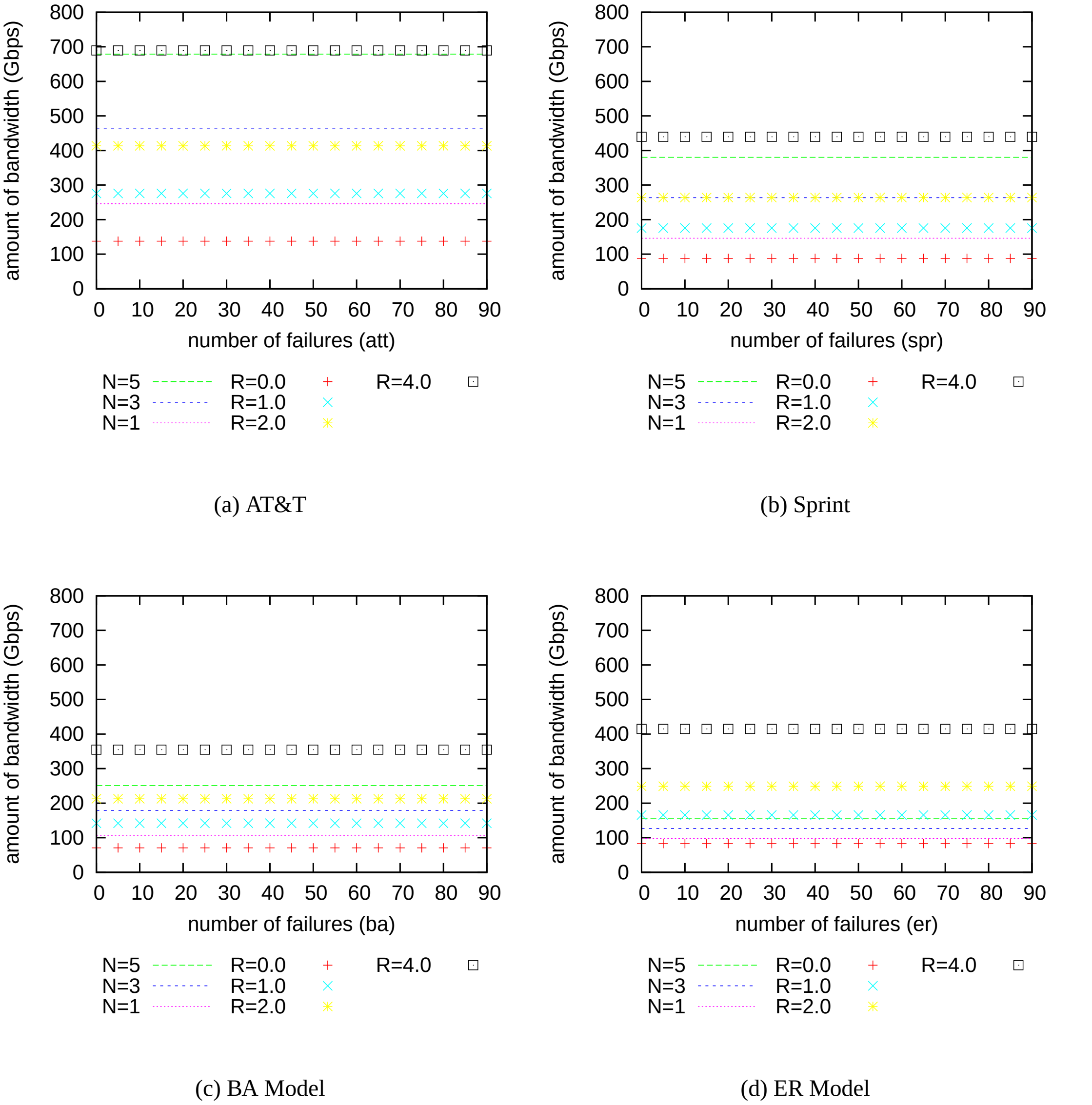
(a) AT&T

(b) Sprint

(c) BA Model

(d) ER Model

Figure 12: Amount of additional link capacity required when multiple failures occur: proposed method A and random failures



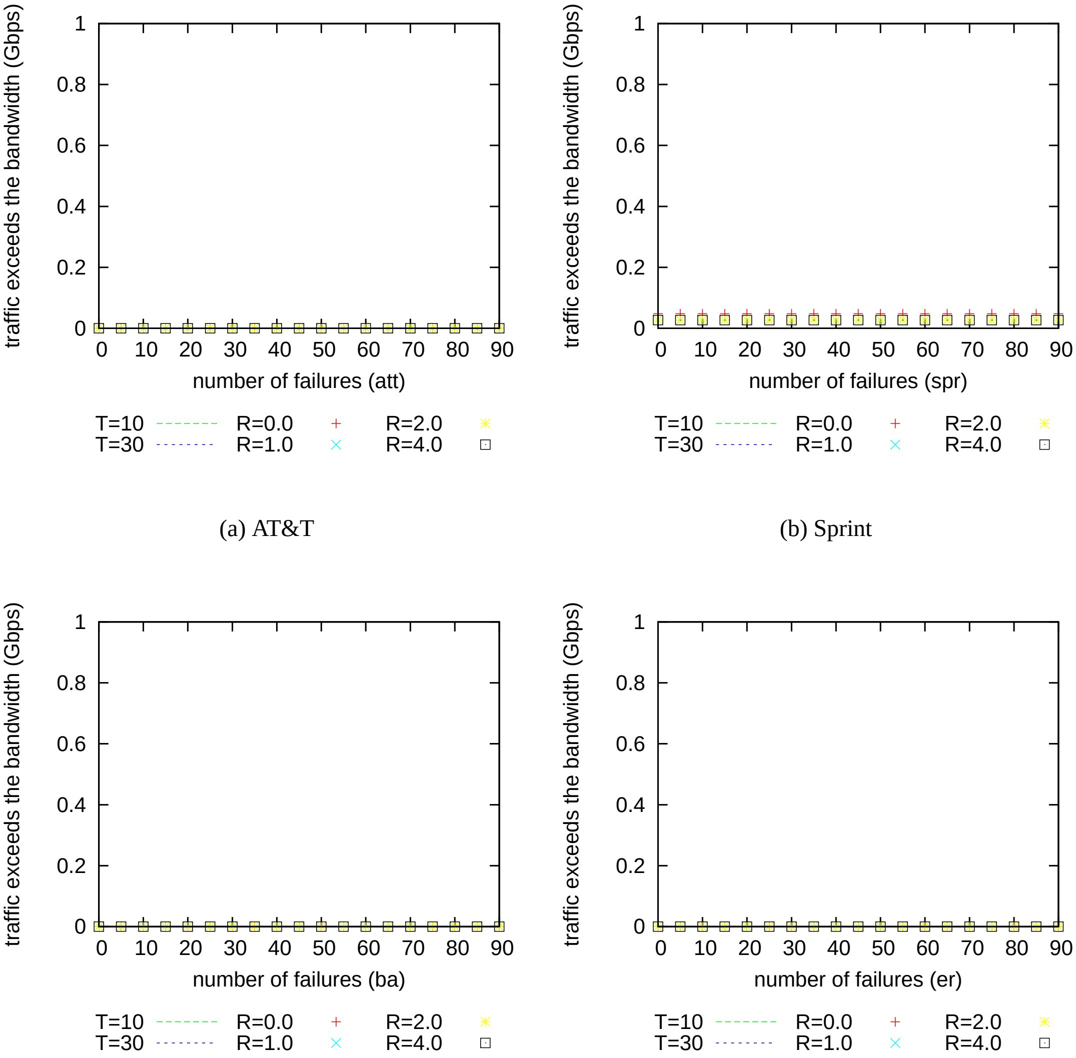
(a) AT&T

(b) Sprint

(c) BA Model

(d) ER Model

Figure 13: Amount of total link capacity required when multiple failures occur: proposed method A and random failures



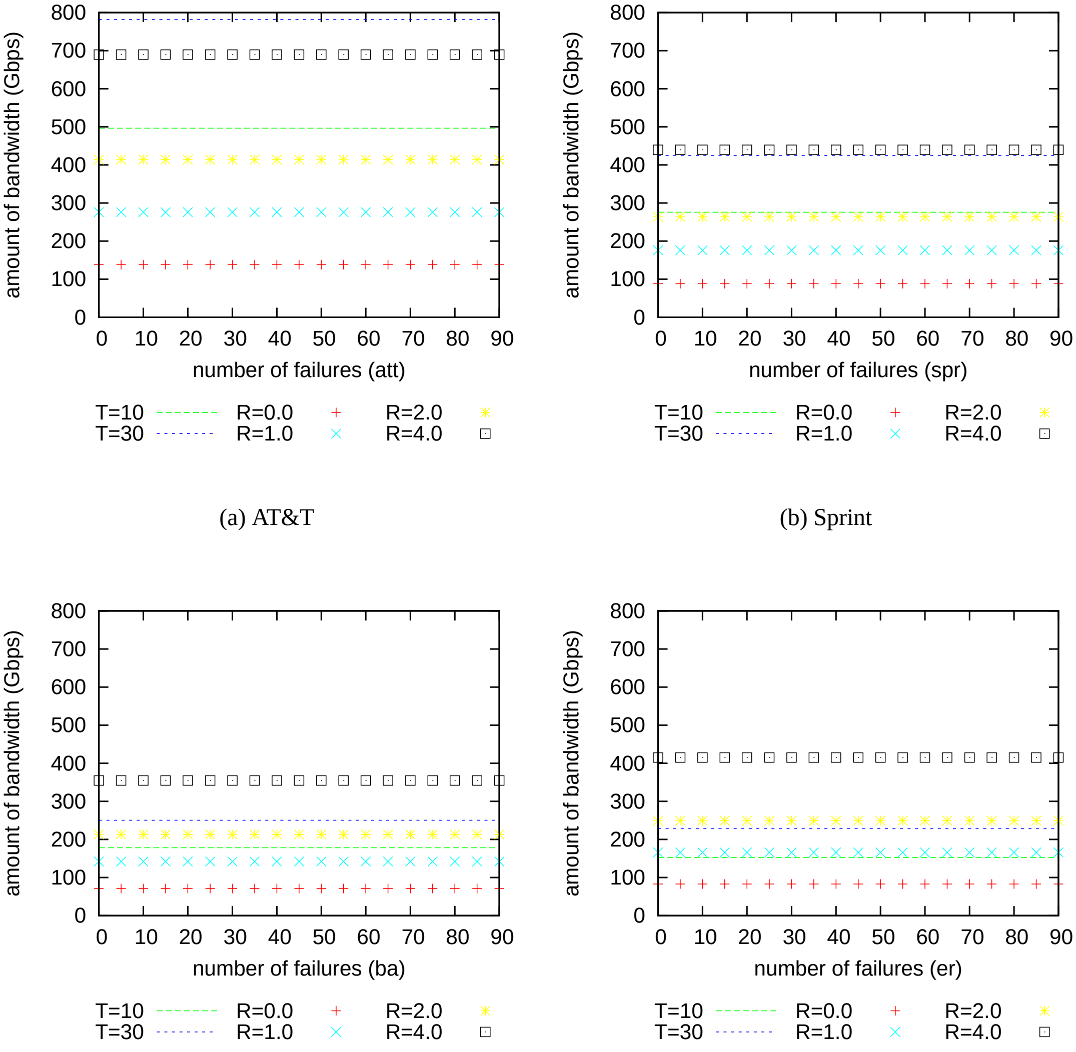
(a) AT&T

(b) Sprint

(c) BA Model

(d) ER Model

Figure 14: Amount of additional link capacity required when multiple failures occur: proposed method B and random failures



(a) AT&T

(b) Sprint

(c) BA Model

(d) ER Model

Figure 15: Amount of total link capacity required when multiple failures occur: proposed method B and random failures

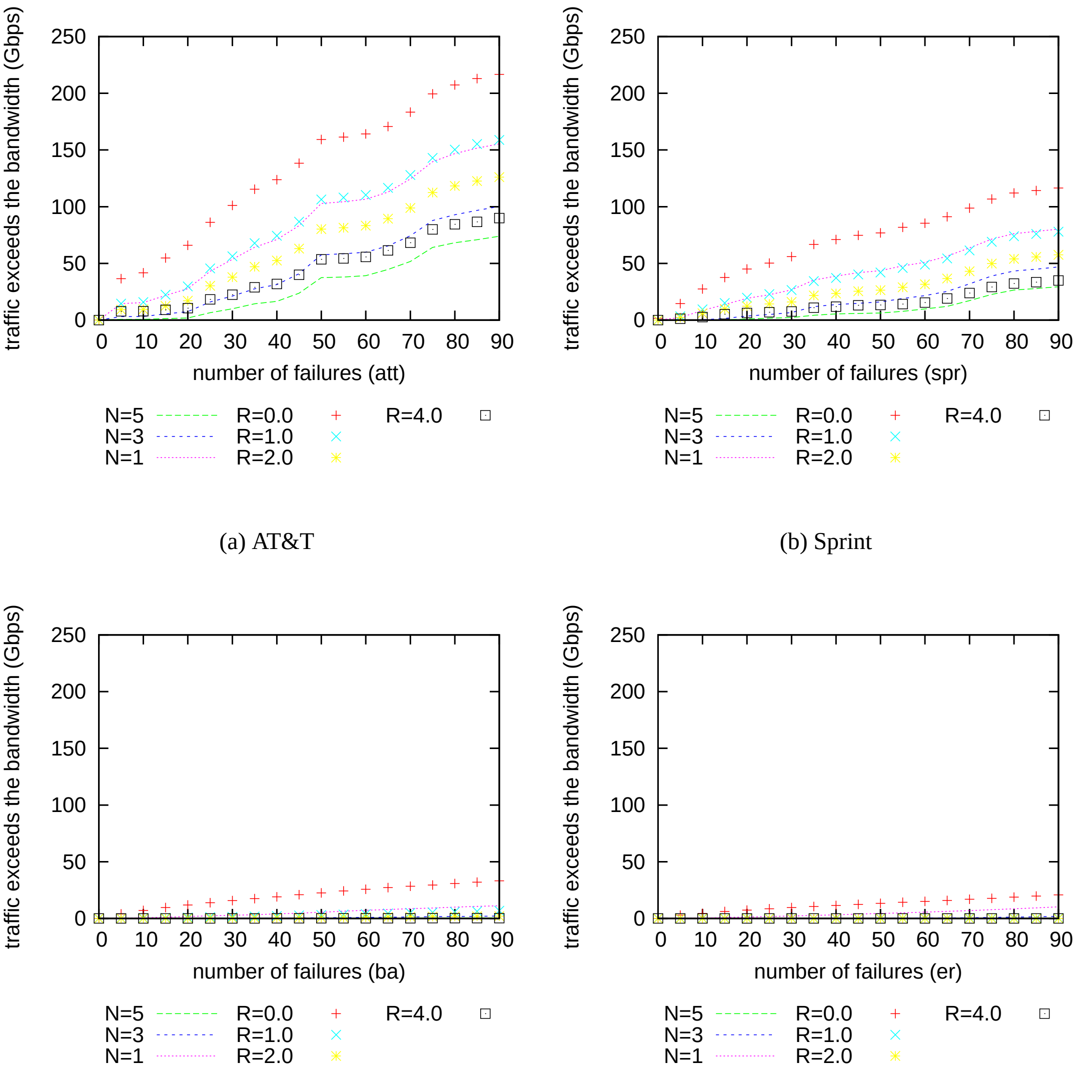
4.2.2 Tolerance to intentional attack

Figure 16 shows the relations of the number of links broken by intentional attack and the amount of traffic exceeding the bandwidth on links. The supposed number of failures N which is a parameter of the proposed method is set to 1, 3 and 5. The over provisioning ratio in conventional method is set to 1.0, 2.0 and 4.0. Figure 17 also shows the amount of the bandwidth allocated by the each method at that time.

In the topology of Sprint network, proposed method with $N = 3$ lower the amount of exceeding traffic and uses amount of allocated bandwidth in the network at 260 Gbps at the 10 link failures. The conventional method with over provisioning ratio $R = 4.0$ reduces the similar amount of exceeding traffic and allocates 440 Gbps. Proposed method decreases the same amount of exceeding traffic and reduces the amount of allocated bandwidth by 40% than that of conventional method. In AT&T topology, our method decreases the amount of allocated bandwidth by 33% than that of conventional method. On the other hand, in BA topology, our proposed method with $N = 3$ only reduces the amount of allocated bandwidth by 24% though it decreases all the exceeding traffic at 10 failures. In ER topology, proposed method with $N = 3$ only reduces the amount of allocated bandwidth by 18% than that of conventional method tough it decreases all the exceeding traffics at 10 failures.

There results show that our proposed method is effective in the topologies with power–law distribution of degrees such as AT%T or Sprint network. In contrast, our proposed method doesn ’ t work well in topology based on ER model, which has non power–law degree distribution and narrow range of bandwidth. Our method performed worked middle between Sprint and ER topology. This is because BA topology has the middle range of bandwidth distribution between Sprint and ER topology, shown in fig. 7.

Figure 18 and figure 19 shows the evaluation results of proposed method B. This method with $N = 10$ decreases at most of exceeding traffic when 10 failures occurred. But that figure shows proposed method A with adjusted parameter N decreases can lower the amount of exceeding traffic than proposed method B.



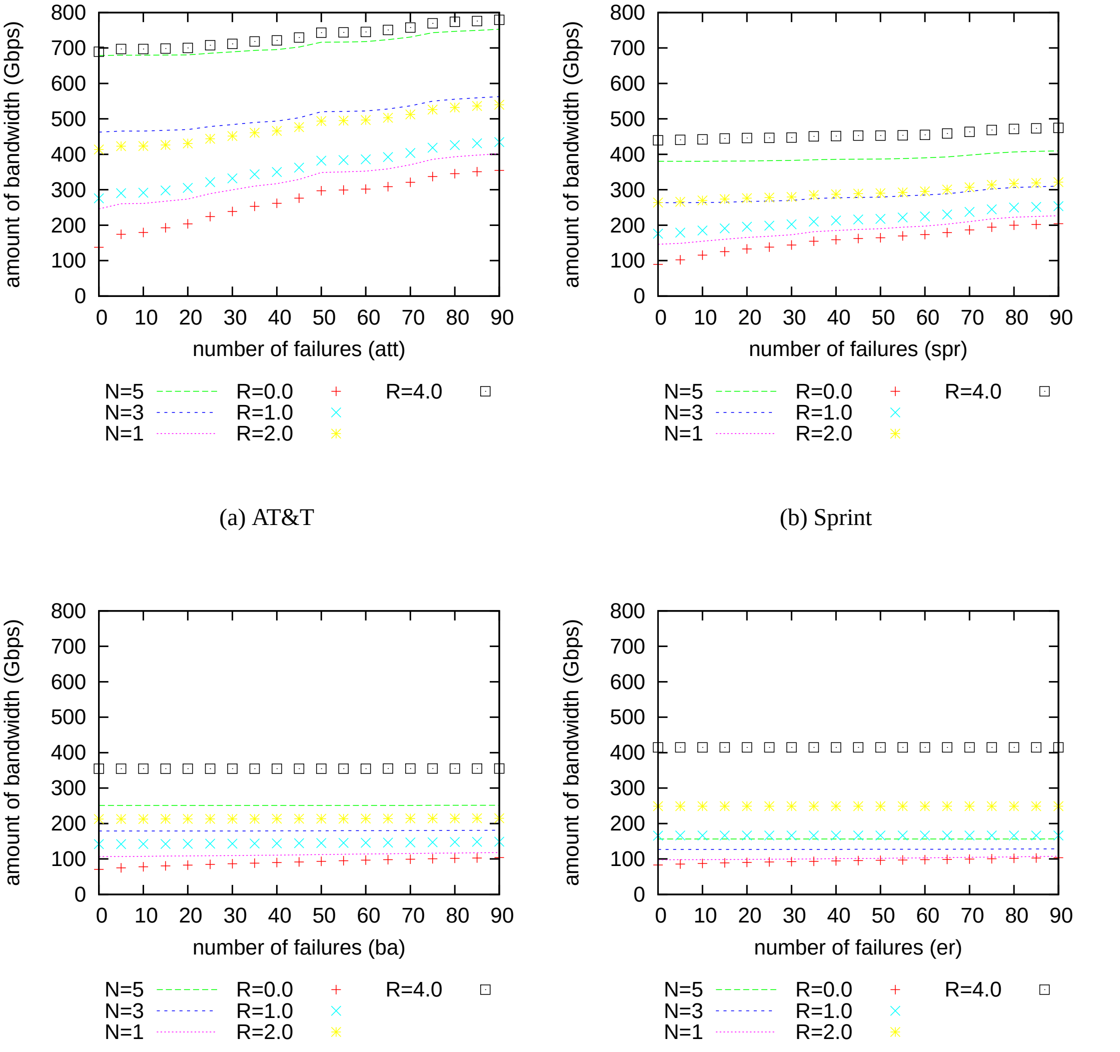
(a) AT&T

(b) Sprint

(c) BA Model

(d) ER Model

Figure 16: Amount of additional link capacity required when multiple failures occur: proposed method A and intentional attacks



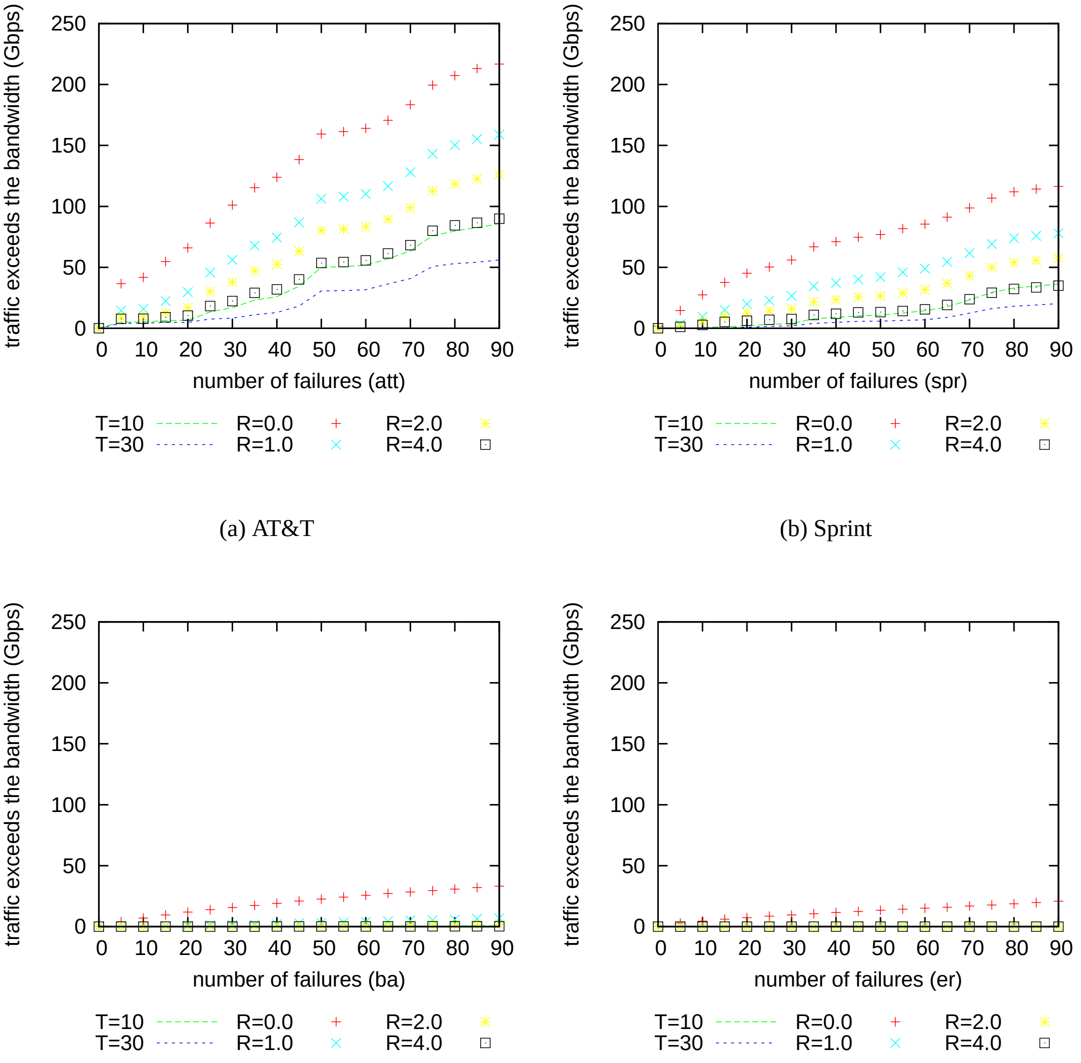
(a) AT&T

(b) Sprint

(c) BA Model

(d) ER Model

Figure 17: Amount of total link capacity required when multiple failures occur: proposed method A and intentional attacks



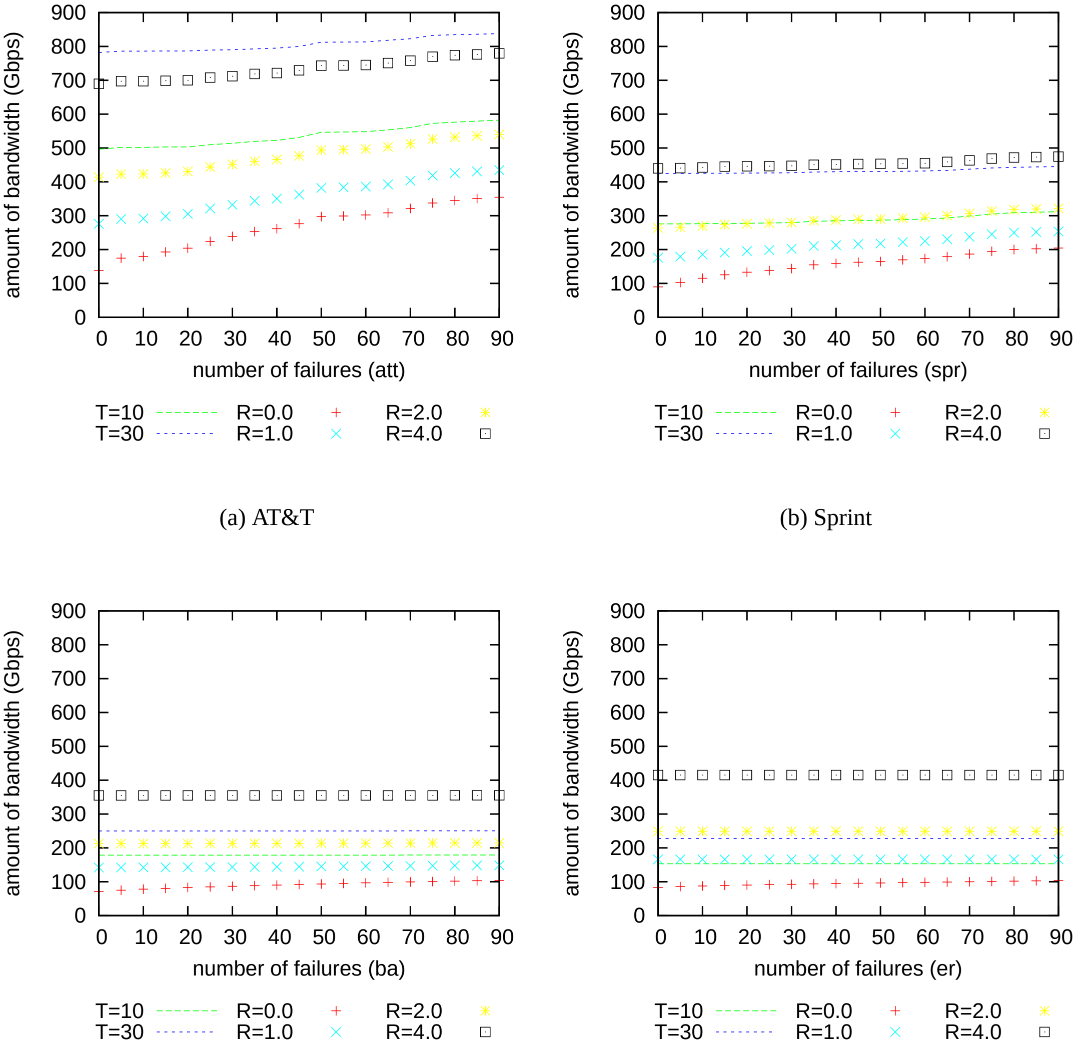
(a) AT&T

(b) Sprint

(c) BA Model

(d) ER Model

Figure 18: Amount of additional link capacity required when multiple failures occur: proposed method B and intentional attacks



(a) AT&T

(b) Sprint

(c) BA Model

(d) ER Model

Figure 19: Amount of total link capacity required when multiple failures occur: proposed method B and intentional attacks

5 Conclusion

In this thesis, the link capacity in power–law networks has investigated. We have evaluated the link capacity by applying over–provisioning method, and have found that distribution of link capacity in power–law networks also exhibits power–law attribute. It has also found that the simple over provisioning method works well in topologies generated by BA model in the case of random link failures. However, in the case of intentional attacks, the over provisioning method causes over–utilization on some links. We have revealed that ISP topologies have a structural property such that large number of links requires low link capacity, while small number of links requires high link capacity. We therefore proposed a capacity dimensioning method that simply utilizes the structural properties by calculating the increase of traffic in case of single failures for each link. Evaluation results showed that our proposed method reduces 40% of the amount of link capacity compared to the over–provisioning method.

Acknowledgements

I would like to express my sincere appreciation to Professor Masayuki Murata of Osaka University. His guidance and inspiration have provided invaluable experiences that have helped me to fulfill this research, and that also taught me the enjoyment and depth of the research.

I would like to express my deepest gratitude to Research Associate Shin'ichi Arakawa of Osaka University, for his appropriate guidance, hearty encouragement, and invaluable firsthand advice. All works of this thesis would not have been possible without his support.

I am most grateful to Professors Koso Murakami, Makoto Imase, Teruo Higashino, Hirotaka Nakano, and Tetsuji Satoh of Osaka University, for their appropriate guidance and invaluable firsthand advice.

I am also indebted to Associate Professors Naoki Wakamiya, Go Hasegawa, and Research associate Hiroyuki Sasabe of Osaka University who gave me helpful comments and feedback.

Finally, I heartily thank my friends and colleagues in the Department of Information Networking, Graduate School of Information Science and Technology of Osaka University for their support.

References

[1] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On power–law relationships of the Internet topology," in *Proceedings of ACM SIGCOMM '99*, pp. 251–262, Oct. 1999.

[2] B. Zhang, R. Liu, D. Massey, and L. Zhang, "Collecting the Internet AS–level topology," *ACM SIGCOMM Computer Communication Review*, vol. 35, pp. 53–61, Jan. 2005.

[3] A. Akella, S. Chawla, A. Kannan, and S. Seshan, "Scaling properties of the Internet graph," in *Proceedings of the Twenty-second Annual Symposium on Principles of Distributed Computing*, pp. 337–346, 2003.

[4] W. Willinger, R. Govindan, S. Jamin, V. Paxson, and S. Shenker, "Scaling phenomena in the Internet: Critically examining criticality," *Self–organized Complexity in the Physical, Biological, and Social Sciences*, Mar. 2001.

[5] C. Gkantsidis, M. Mihail, and A. Saberi, "Conductance and congestion in power law graphs," in *Proceedings of SIGMETRIC*, June 2003.

[6] K. L. Goh, B. Kahng, and D. Kim, "Universal behavior of load distribution in scale–free networks," *Physical Review Letters*, vol. 87, Dec. 2001.

[7] L. Qiu, Y. R. Yang, Y. Zhang, and S. Shenker, "On selfish routing in Internet–like environments," in *Proceecdings of ACM SIGCOMM 2003*, pp. 151–162, Aug. 2003.

[8] R. Cohen, S. Havlin, and D. Avraham, "Structural properties of scale–free networks," in *Handbook of Graphs and Networks – From the Genome to the Internet* (S. Bornholdt and H. G. Schuster, eds.), WILEY-VCH GmbH & Co., 2003.

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

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

[11] 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.

[12] J. I. Alvarez-Hamelin and N. Schabanel, “An Internet graph model based on trade–off optimization,” *European Physical Journal B,* vol. 38, pp. 231–237, Mar. 2004.

[13] O. Heckmann, M. Piringer, J. Schmitt, and R. Steinmetz, “Generating realistic ISP–level network topologies,” *IEEE Communications Letters,* vol. 7, pp. 335–337, July 2003.

[14] 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.

[15] R. Fukumoto, S. Arakawa, and M. Murata, “Proposal and evaluation of routing methods in power–law networks,” *IEICE Tech. Rep.*(IN2005-68), vol. 105, pp. 43–48, Sept. 2005.

[16] S. Arakawa, R. Fukumoto, T. Takine, and M. Murata, “Analyzing and modeling route level Internet topologies,” *submitted to Networking 2006*, 2006.

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

[18] M. Faloutsos, P. Faloutsos, and C. Faloutsos, “On power–law relationships of the Internet topology,” in *Proceedings of ACM SIGCOMM ’99*, pp. 251–262, Oct. 1999.

[19] M. E. J. Newman, *Random graphs as models of networks,* ch. 2, pp. 35–68. WILEY–VCH, 2002, Nov. 2002.

[20] G. Siganos, M. Faloutsos, P. Faloutsos, and C. Faloutsos, “Power laws and the AS–level Internet topology,” *IEEE/ACM Transactions on Networking*, vol. 11, pp. 514–524, Aug. 2003.

[21] 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.

[22] R. Albert and A.-L. Barabási, “Statistical mechanics of complex networks,” *Reviews of mordern physics*, vol. 74, pp. 47–97, Jan. 2002.

[23] C. Labovitz, A. Ahuja, R. Wattenhofer, and V. Srinivasan, “The impact of Internet policy and topology on delayed routing convergence,” in *Proceedings of INFOCOM*, pp. 537–546, Apr. 2001.

[24] P. Erdös and A. Rényi, “On the evolution of random graphs,” *Publications of the Mathematical Institute of the Hungarian Academy of Sciences*, vol. 5, pp. 17–61, 1960.

[25] L. da F Costa, F. A. Rodrigues, G. Travieso, and P. R. V. Boas, “Characterization of complex networks: A survey of measurements,” *ArXiv Condensed Matter e-prints*, May 2005.

[26] W. Aiello, F. Chung, and L. Lu, “A random graph model for massive graphs,” in *ACM Symposium on Theory of Computing (STOC)*, pp. 171–180, 2000.

[27] M. E. J. Newman, “The structure and function of networks,” *SIAM Review*, vol. 45, pp. 167–256, 2003.

[28] M. Kim and M. Medard, “Robustness in large–scale random networks,” *IEEE INFOCOM 2004 - The Conference on Computer Communications*, vol. 4, pp. 2364–2373, Mar. 2004.

[29] B. Shargel, H. Sayama, I. R. Epstein, and Y. Bar-Yam, “Optimization of robustness and connectivity in complex networks,” *Physical Review Letters*, vol. 90, 068701-1-4, no. 068701-1-4, 2003.

[30] A. Beygelzimer, G. Grinstein, R. Linsker, and I. Rish, “Improving network robustness.,” in *Proceedings of 1st International Conference on Autonomic Computing (ICAC 2004), 17-19 May 2004, New York, NY, USA*, pp. 322–323, 2004.

[31] S. Merugu, S. Srinivasan, and E. Zegura, “Adding structure to unstructured peer–to–peer networks: The use of small–world grpahs,” *Journal of Parallel and Distributed Computing*, vol. 65, pp. 142–153, Feb. 2005.

[32] R. Schollmeier and G. Schollmeier, “Why peer-to-peer (p2p) does scale: An analysis of p2p traffic patterns,” in *P2P ’02: Proceedings of the Second International Conference on Peer-to-Peer Computing*, p. 112, IEEE Computer Society, 2002.

[33] M. E. J. Newman, “Random graphs as models of networks,” in *Handbook of Graphs and Networks – From the Genome to the Internet* (S. Bornholdt and H. G. Schuster, eds.), Berlin: WILEY-VCH GmbH & Co., 2003.

[34] J. Kleinberg, *Small–World Phenomena and the Dynamics of Information*, ch. 14. MIT Press, 2002.

[35] R. Guimerà, A. Díaz-Guilera, F. Vega-Redondo, A. Cabrales, and A. Arenas, “Optimal network topologies for local search with congestion,” *Physical Review Letters*, vol. 89, 248701, Dec. 2002.

[36] G. M. Viswanathan, S. V. Buldyrev, S. Havlln, M. G. E. da Luz, E. P. Raposo, and H. E. Stanley, “Optimizing the success of random searches,” *Nature*, vol. 401, pp. 911–914, Oct. 1999.

[37] F. Banaei-Kashani and C. Shahabi, “Criticality–based analysis and design of unstructured peer-to-peer networks as ’complex systems’,” in *Proceedings of Third International Workshop on Global and Peer-to-Peer Computing (GP2PC)*, pp. 22–32, May 2003.

[38] X.-H. Wang, “Directed random walks on directed percolation clusters,” *Physical Review E*, vol. 67, 050101, May 2003.

[39] S. Zhou and R. Mondragón, “Accurately modeling the Internet topology,” *Physical Review E*, vol. 70, no. 066108, 2004.

[40] 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.

[41] J. M. Carlson and J. Doyle, “Highly optimized tolerance: A mechanism for power laws in designed systems,” *Physical Review E*, vol. 60, pp. 1412–1427, Aug. 1999.

[42] P. Erdös and A. Rényi, “On the evolution of random graphs,” *Publications of the Mathematical Institute of the Hungarian Academy of Sciences*, vol. 5, pp. 17–61, 1960.

[43] F. Chung and L.lu, “The average distance in a random graph with given expected degrees,” *Internet Mathematics*, vol. 1, pp. 91–113, 2003.

[44] L. Zhao, K. Park, and Y.-C. Lai, “Attack vulnerability of scale-free networks due to cascading breakdown,” *Physical Review E*, vol. 70, Sept. 2004.

[45] A. E. Motter, “Cascade control and defense in complex networks,” *Physical Review Letter*, vol. 93, Aug. 2004. unreada.

[46] R. Albert, I. Albert, and G. L. Nakarado, “Structural vulnerability of the North Americal power grid,” *Physical Review E*, vol. 69, Feb. 2004.

[47] R. Cohen, K. Erez, D. Avraham, and S. Havlin, “Breakdown of the Internet under intentional attack,” *Physical Review Letters*, vol. 86, Apr. 2001.

[48] S. N. Dorogovtsev and J. F. F. Mendes, “Comment on ”Breakdown of the Internet under intentional attack”,” *Physical Review Letters*, vol. 87, Nov. 2001.

[49] L. Gallos, P. Argyrakis, A. Bunde, R. Cohen, and S. Havlin, “Tolerance of scale–free networks: from friendly to intentional attack strategies,” *Physica A: Statistical Mechanics and its Applications*, vol. 344, pp. 504–509, Dec. 2004.

[50] A. Medina, A. Lakhina, I. Matta, and J. Byers, “BRITE: Universal topology generation from a user’s perspective,” Tech. Rep. BUCS–TR–2001–003, Boston University, Apr. 2001.

[51] V. Latora and M. Marchiori, “A measure of centrality based on the network efficiency,” *Preprint: submitted to Elsevier Science*, Feb. 2004. arXiv:cond-mat/0402050v1.

[52] D. G. Andersen, H. Balakrishnan, M. F. Kaashoek, and R. Morris, “Resilient overlay networks,” in *Proceecdings of ACM SOSP*, 2001.

[53] P. Holme, “Edge overload breakdown in evolving networks,” *Physical Review Letters*, vol. 66, Sept. 2002.

[54] P. Holme and B. J. Kim, “Vertex overload breakdown in evolving networks,” *Physical Review Letters*, vol. 65, June 2002.