PAPER

Resiliency of Network Topologies under Path-Based Attacks*

Heejo LEE†, *Member*, **Jong KIM**††, *Nonmember*, *and* **Wan Yeon LEE**†††, *Member*

SUMMARY

Network topology has no direct effect on the correctness of network protocols, however, it influences the performance of networks and their survivability when they are under attack. Recent studies have analyzed the robustness of the Internet in the face of faults or attacks which may cause node failures. However, the effect of link failure or a series of link failures has not been extensively examined, even though such a situation is more likely to occur in the current Internet environment. In this paper, we propose an attack-and-failure graph model and practical techniques for attacking strategies against nodes, edges or paths in order to reflect real-life attack scenarios. The resiliency of Internet topologies is examined under the attacking strategies, with various metrics including path-failure ratio and "attack power", which is defined as the ratio of the failure to attack. The experiments reveal that "path-based" attacks can result in greater damage to the connectivity of a network than the other types of attack. Nonetheless, the effectiveness of an attack depends on the objective that the attacker wants to achieve through the attack. The proposed simple but formalized approach can be a springboard for developing more resilient Internet topologies in a variety of aspects.

key words: *Network topology, attack resiliency, connectivity, graph theory.*

1. Introduction

1.1 Background

Network topology has no direct effect on the correctness of network protocols. However, it influences the performance of networks [2], [3], and the survivability of the networks under attack [4], [5]. Much work has been conducted for finding the topological characteristics of the Internet [3], [6]–[8]. In addition, researchers have developed topology generators to construct network graphs similar to the Internet [9], [10]. However, additional study is required for generating graphs identical to the current Internet topology [2], [3], [7].

One research direction regarding Internet topology involves the analysis of the robustness of the Internet faced with network attacks [2], [4], [5], [11], [12]. An important characteristic of these attacks is that they are target-oriented, and can therefore result in catastrophic failures in terms of Internet connectivity [4], [5]. From analysis of susceptibility to attacks and faults, it has been found that Internet connectivity is more susceptible to malicious attacks than to random failures [5]. Moreover, failures involving only a part of the components of the Internet can break down the overall Internet infrastructure [4], [11]. On the other hand, the Internet has threads of connection with properties such as a small vertex cover [2], which can be a potential "choke point" on the Internet. Exploring the topological characteristics of the Internet can thus provide a springboard from which to enhance the robustness of the Internet infrastructure against malicious attacks.

Previous research has focused on the impact of node failures, while link failures are more likely to occur in current network environments [11], [13], [14]. This insufficiency in the study of attacks and failures motivated us to study the resiliency of the Internet faced with various types of attack.

1.2 Failures on Networks

Internet connections can suffer from several types of failure, resulting from hardware faults, human errors or malicious attacks. These failures can be classified into three categories: node failure, link failure and path failure.

1. **Node failure:** Hardware faults or human errors may cause node failures, where the nodes involved can be networking devices such as routers or ASes (autonomous systems), depending on the granularity of the attack and failure. Malicious attacks can also cause node failures, and the effect of such an attack can be identical to that produced by faults and errors.
2. **Link failure:** Link-based attacks may cause link failure on the Internet. Physical or electronic attacks may result in loosing network connectivity. Physical attacks include fiber cuts and damage to switching equipment. Electronic attacks include DNS hacking, routing table poisoning attacks, packet mistreating attacks, denial-of-service (DoS) attacks and so forth [11], [15], [16].
3. **Path failure:** Certain types of attacks or faults can cause the failure of consecutive links, which is referred to as "path failure". DoS attacks or routing loops are good examples of this type of attack, because they have impact on more than one link. In case of DoS attacks, an overwhelming number of packets floods all or part

†The author is with the Department of Computer Science and Engineering, Korea University, Seoul 136-713, South KOREA.

††The author is with the Department of Computer Science and Engineering, POSTECH, Pohang 790-784, South KOREA.

†††The author is with the Division of Information Engineering and Telecommunications, Hallym University, Chunchon 200-702, South KOREA.

*A preliminary version of this paper was presented at PDCAT 2004 [1]. This work was supported in part by the ITRC program of the Korea Ministry of Information & Communications under grant IITA-2005-(C1090-0502-0020), the BK21 program of the Korea Ministry of Education.

of the network, consuming all of the resources on a particular server and further clogging the network between the attacking source and destination. Routing loops between two nodes can also cause path failure. The misconfiguration of routing policies or unexpected corruption caused by route oscillations can give rise to routing loops [13], [14]. A routing loop can result in packet loss if the packets trapped in the routing loop cannot exit the loop but be discarded after their TTL field reaches zero. Thus, routing loops can break connectivity among networks.

One case of "path failures" can be caused by a DoS attack with packet flooding [17], and rate limiting of a certain class of packets has been proposed as a solution for mitigating such flooding attacks [18], [19]. However, its application is bounded by only a few obvious attack patterns such as using TCP SYN or ICMP. In addition, without universal deployment, various paths remain vulnerable to flooding attacks. Thus, it is feasible for an entire path between two nodes to fail, furthermore, such failure will disturb other paths overlapping with a part of the failed path. Moreover, while parts of the path may not exhaust entire bandwidth, significant reduction of network service quality can be considered as a logical failure of the communication path.

1.3 Contributions

This study is motivated by the question: "How vulnerable is the Internet topology to the latest methods of attack?" First, we propose a graph model for representing various attacking scenarios and their failures. Then, we evaluate the resiliency of network topologies under various attack scenarios. From the evaluation, path attacks demonstrate more debilitating effects on network connectivity than node and edge attacks. The most effective mechanism, nonetheless, depends on the objective of an attacker.

The main contribution of this paper is to introduce the concept of path failure with a concise graph model, which helps to provide a more realistic evaluation of the network status in the case of an attack. We also evaluate the resiliency of Internet topologies, based on the principle of "cause-and-effect" between attacks and failures. From the evaluation, it is shown that the Internet in its current form is susceptible to path-based attacks. This implies that a small portion of a network can initiate disastrous failure by launching a path-based attack. In other words, the judicious placement of attacking sources and their targets under a DDoS attack or an Internet worm epidemic can give more serious *amplification effect* on network failure.

2. Graph Model for Attack Resiliency

2.1 Network Topology

A network topology represents the connectivity structure among nodes. Fig. 1 presents three topologies with 10 nodes and 10 edges. The average distance among the nodes decreases from the left-hand graph (2.78) to the right-hand graph (1.78), while the dependency on a single node increases. The failure of a single node in the left-hand graph does not disrupt the connectivity of the other nodes, whereas the failure of node 0 in the right-hand graph significantly affects the connectivity of other nodes. Thus, the topology of a network has an impact on the robustness against attack.

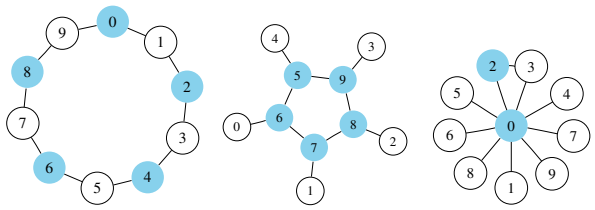

Fig. 1 Network topologies with 10 nodes and 10 edges.

A network topology can be represented by an undirected graph $G = (V, E)$, where V is the set of nodes and E is the set of edges. Let T denote the target of an attack, where T is a subset of G, i.e. $T \subseteq G$. T can be a set of nodes, edges or paths. A path $\mathcal{P}[x, y]$ is a set of consecutive edges from a source x to a destination y such that $[x, y] = \{x, v_1, v_2, ..., v_{d-1}, y\}$ where $(v_i, v_{i+1}) \in E$ for all $i = 0 \;..\; d-1$ with $x = v_0$ and $y = v_d$. Let $\mathcal{A}$ denote an *attack* which represents an operation resulting in the deletion of a subgraph T from G such that

$$\mathcal{A}(T) : G - T.$$

The deletion of a node or an edge in graph G is a well-defined operation[†]. And, the deletion of a path is analogous to the deletion of every edge belonging to that path. As a result of an attack $\mathcal{A}$, the failure can be measured by $\mathcal{F}(\mathcal{A}) = T \cup D$, where D is a set of nodes in $G-T$ that have no remaining edges. This implies that the failure caused by an attack could be larger than the target of the attack, i.e. $\mathcal{F}(\mathcal{A}) \supseteq T$ when $D \neq \{\}$.

2.2 Attack Types

Three types of attack can be defined using the graph model, depending on the target. They are node attacks, edge attacks and path attacks. Hardware faults and human errors are not considered as separate items since they can be modeled as "random" attacks. Fig. 2 presents the three types of attack, viz. a node attack with $T = \{3\}$, an edge attack with $T = \{(3, 4)\}$ and a path attack with $T = \{[1, 4]\}$. We use α to represent the attack ratio where $0 \leq \alpha \leq 1$. For instance, $\alpha = 0$ means that there is no attack so that $T = \{\}$, whereas $\alpha = 1$ means $T = G$. Thus, α indicates the severity of the attack.

Node attacks target a set of nodes. Node attacks also delete all edges connected to the target nodes, which are

[†]In a graph G, edge deletion is $V_{G-e} = V_G$ and $E_{G-e} = E_G - \{e\}$. Also, vertex deletion is $V_{G-v} = V_G - \{v\}$ and $E_{G-v} = \{e \in E_G | v \notin endpts(e)\}$.

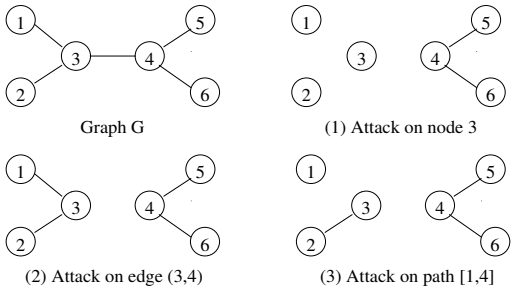

Fig. 2 Three types of attack: (1) node attack, (2) edge attack and (3) path attack.

represented by the deletion of nodes in T from G. The attack ratio α is defined as the fraction of nodes under attack. More formally,

$$\alpha_n = \frac{|V(T)|}{n}$$

where $V(T)$ is a set of nodes in T and $n = |V|$. Note that node attacks imply $V(T) \neq \{\}$ but $E(T) = \{\}$.

Edge attacks target a set of edges. The attack ratio α on an edge attack is defined by $\alpha_e = |E(T)|/e$ where $E(T)$ is a set of edges in T and $e = |E|$. Note that edge attacks also imply $E(T) \neq \{\}$ but $V(T) = \{\}$.

Path attacks target a set of paths. Attacking a path between two nodes is analogous to attacking a set of consecutive edges belonging to the path. The attack ratio α of a path attack is defined by $\alpha_p = |P(T)|/n(n-1)$ where $P(T)$ is a set of paths in T. A path from s to t is determined by routing policies

2.3 Failure Metrics

Failures can be measured separately from attack types. A node failure is identical to failures of all edges connected to the node. When there is no alternative path available between two nodes in a graph, we call it the "path failure" between the two nodes. Consequently, one edge attack could result in the failure of multiple paths.

Attacks and their effects are separated by the principle of "cause" and "effect" such that an attack is a cause and the failure is its effect. Here, in order to measure the effect of an attack, the failure metrics are defined as the ratio of failed components. The node failure ratio is defined as $f_n = n_f/n$ where n_f is the number of failed nodes. The path failure ratio is defined as

$$f_p = \frac{p_f}{n(n-1)}$$

where p_f is the number of failed paths.

Let us consider graph properties for the purpose of observing the dynamics of attacks. In addition to node degrees and path lengths, an interesting graph property is the "minimum vertex cover" of a graph [20]. A vertex cover (VC) of an undirected graph $G = (V, E)$ is a subset of $VC \subseteq V$ such that, for any $(u, v) \in E$, $u \in VC$ or $v \in VC$. In other words, $T \subseteq V$ is a vertex cover of G if every edge in E is incident on some node in T. A minimum vertex cover is a vertex cover with the least number of vertices. Let $|VC|$ denote the cardinality of a minimum vertex cover. For instance, $|VC| = 1$ in a star graph, $|VC| = n/2$ in a ring, and $|VC| = n - 1$ in a fully connected graph. A vertex cover or VC represents a minimum vertex cover hereafter. The failure of VC nodes renders a graph G completely disconnected. The VC ratio $|VC|/n$ represents the deconcentration of a graph. The value of a fully connected graph is the closest to 1 for a given n, whereas a highly centralized "star" graph has $|VC|/n = 1/n$. The $|VC|/n$ values of the Internet are smaller than 0.2, while those of randomly connected graphs are larger than 0.5, as presented in [2]. This confirms that the connectivity of the Internet heavily relies on a few high degree nodes, which forms the power-law relationships [6]. Such a small VC can be a "choke point" of the Internet.

Here we propose a new metric, Φ, referred to as the "attack power," to measure the destructive impact of an individual attack. The attack power, Φ, is defined as

$$\Phi(\alpha) = \frac{f(\alpha)}{\alpha}$$

where α is the attack ratio and $f(\alpha)$ is the failure ratio due to the attack with attack ratio α. The lower the attack power, the more resilient the network topology is to the attack. While the connectivity metric is a static value of network status, the attack power is used to measure the relative impact of an attack in a given network topology.

3. Resiliency Evaluation

3.1 Attacking Strategies

The attacking strategy of an attack is to select the target elements on a network, which gives great impact on the resulting damage caused by the attack [12]. Target elements can be chosen by the importance of each element to maximize the attack impact. In case of equal importance among elements, such an attack – categorized as a "random attack", can be taken by an attacker since aim is taken at random targets. Attacking the highest degree node first [4], [5], [12], is the use of node degrees as the importance of a node. In addition, attacking the minimum degree node first, even if it is not likely to occur, is included for comparing attack strengths.

Regarding node attacks, there are four possible strategies to build a target T. A node attack starts with $T = \{\}$ and finishes when $|V(T)| \geq \alpha n$.

- **Random node attack:**
  While $|V(T)| < \alpha n$, choose a node v_i randomly in $G - T$, and $T = T \cup \{v_i\}$.
- **Min-degree node attack:**
  While $|V(T)| < \alpha n$, choose v_i with $deg(v_i) = \min_{u \in G-T}\{deg(u)\}$, and $T = T \cup \{v_i\}$.

- **Max-degree node attack:**
  While $|V(T)| < \alpha n$, choose v_i with $deg(v_i) = \max_{u \in G-T}\{deg(u)\}$, and $T = T \cup \{v_i\}$.
- **Max-weight node attack:**
  While $|V(T)| < \alpha n$, choose v_i with $W_n(v_i) = \max_{u \in G-T}\{W_n(u)\}$, and $T = T \cup \{v_i\}$.

The weight of a node u, $W_n(u)$, is the sum of the weights of all edges adjacent to u. It is described by

$$W_n(v_i) = \sum_{e_j \in E(v_i)} W_e(e_j)$$

where $E(v_i) = \{\, e_j \in E \,|\, v_i \in endpts(e_j) \,\}$ and $W_e(e_j)$ is the weight of an edge e_j. The edge weight $W_e(e_j)$ is the number of paths holding e_j. It satisfies that $W_e(e_j) \leq n(n-1)$ for any $e_j \in E$, where $n(n-1)$ is the number of paths [†]. For instance, the max-degree node attack removes the highest degree node on the remaining network until the number of removed nodes reaches αn.

With regard to edge attacks, there are three edge attack types: random edge attack, min-weight edge attack, and max-weight edge attack. They can be defined in a similar way to the node attacks. We omit the details due to lack of space.

With regard to path attacks, there are three path attack types, which can be described as follows.

- **Random path attack:**
  While $|P(T)| < \alpha n(n-1)$, choose a path p_k randomly in $G - T$, and $T = T \cup \{p_k\}$.
- **Max-length path attack:**
  While $|P(T)| < \alpha n(n-1)$, choose the longest path p_k in $G - T$, and $T = T \cup \{p_k\}$.
- **Max-weight path attack:**
  While $|P(T)| < \alpha n(n-1)$, choose p_k with the maximum weight in $G - T$, and $T = T \cup \{p_k\}$.

The weight of a path is defined by the sum of all edge weights in the path. An effective attack must be an attack on the most popular links which have a heavy weight.

3.2 Effects of Network Topologies

In order to evaluate the resiliency of a network topology against attack, we use both AS-level Internet topologies and artificial graphs. We use the AS connectivity graphs archived by NLANR from the Oregon RouteView Project [22], which is the most widely used and publicly available data set used for studying Internet topologies. Random graphs are generated by connecting two nodes with linking probability (p) corresponding to the AS connectivity from the equation $p = 2e/n(n-1)$. Internet-like artificial graphs are created using well-known topology generators, such as Brite2.1 [10] and Inet3.0 [9].

The effects of the network topologies are measured for both AS connectivities and router connectivities. Fig. 3 shows the distribution of f_n as a function of α for the max-weight node attack. The AS graph used is the connectivity at Nov. 8, 1997, which consists of 3015 nodes and 5156 edges. The Random, Brite, Inet graphs are generated equally with the number of nodes and/or edges in the AS graph. In Fig. 3, it is shown that AS graph, Brite and Inet are weaker than Random, when faced with a node attack. This confirms that the robustness of the Internet is not better than that of the random topology. The node failure ratio, f_n, increases, reaching $f_n = 1.0$ at $\alpha = 0.18$, which is the ratio of the vertex covering nodes in the Internet topologies. This relationship holds true for all other graphs. While the result is exactly the same as Albert *et al.* [4], it is found that the critical point of network failure is related to the size of vertex cover.

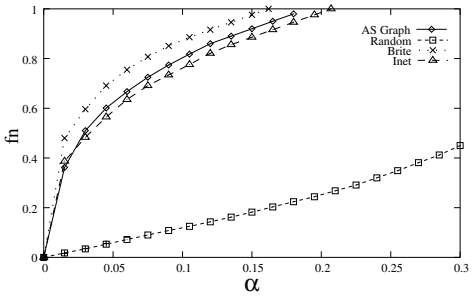

Fig. 3 Distribution of f_n on the node attack.

While real router-level topologies are not publicly available, we can obtain the high quality router maps measured by Rocketfuel [23]. Among the 10 topologies provided by Rocketfuel, 4 topologies are selected based on the diversity of graph properties. These are AS 1221 (Telstra, AU), AS 1755 (Ebone, EU), AS 3356 (Level3, US), and AS 3967 (Exodus, US). While many properties of the AS-level topologies are similar, the router-level topologies are reasonably diverse and provide good sampling spaces. For instance, while the vertex covers in the AS graphs are all approximately 18%, the router-level topologies have vertex covers with different sizes, i.e. $11.7\% \sim 47.9\%$.

Fig. 4 shows the distribution of f_p as a function of α for router topologies under the max-weight path attack. The Telstra network has the weakest structure faced with the path attack, and Ebone (AS 1775) is the strongest under the path attack. Level3 (AS 3356) has the largest number of links per node with $d = 8.32$, however, this network is the second weakest when faced with an attack. This implies that possessing more links does not necessarily provide greater resiliency against attack. However, the robustness of a network relies heavily on its underlying topology. Furthermore,

[†] In case of symmetric routing, the number of distinct paths can be reduced to $n(n-1)/2$. However, routing asymmetry is considerable portion in the Internet [21], thus we used $n(n-1)$ without loss of generality.

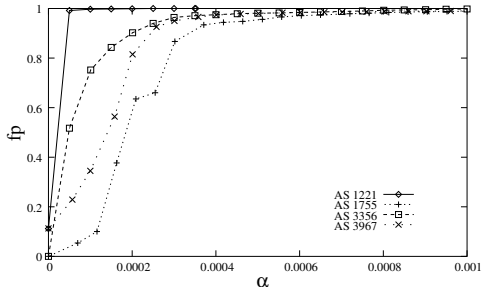

Fig. 4 Distribution of f_p for router-level connectivity.

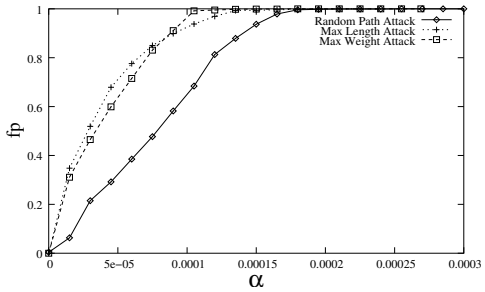

Fig. 6 Path failure ratio f_p as a function of attack ratio α.

it was found that simply adding more links does not always enhance the resiliency against network attacks. Therefore, when designing a network, the network topology in terms of its attack resiliency must be considered.

3.3 Effects of Attack Types

The effect of an attack strategy is measured on the AS graph. Since the AS connectivity has shown similar properties over different years, the smallest graph, year 1997, was selected for the sake of complexity.

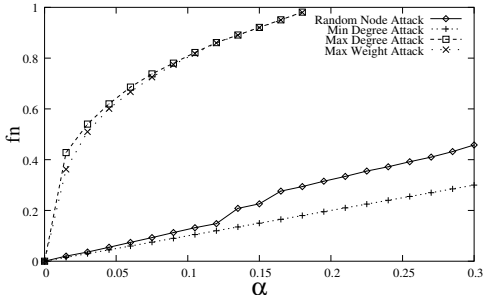

Fig. 5 Node failure ratio f_n as a function of attack ratio α.

Fig. 5 shows the distribution of the node failure ratio f_n under four node-attack strategies. For the majority of cases, except for the min-degree attack, the number of failed nodes becomes larger than that of attacked nodes. We call this impact as attack-failure amplification, and it is represented by attack power Φ. The two most significant attacks are max-degree and max-weight node attacks. These two attacks are very similar and reach $f_n = 1.0$ at $\alpha = 0.18$, which is the VC size. This implies that max-degree or max-weight nodes correspond to the majority of VC nodes in Internet topologies and the associated failures completely destroy the network connectivity.

As a function of α, path failures grow more rapidly than node failures, as presented in Fig. 6. Among three types of path attacks, the max-weight path attack is the more effective one to achieve 90% paths to fail, i.e. $f_p(\alpha) > 0.9$. Thus, the choice of an attacking strategy depends on the objective of the attack.

From the experiments with various attacking strategies, path-based attacks are more destructive than the other types of attacks. However, it is shown that the effectiveness of an attack relies on the attack objective.

3.4 Attack Power as a Failure Metric

In order to measure the connectivity of a network under attack, Albert [4] and Magoni [12] used the largest component size, S, of the graph. Park *et al.* [5] proposed another metric, K, to describe the overall network connectivity, since S considers only the largest connected component. The metric, K, is defined as $K = |\Pi|/|\Psi|$ where Ψ is the set of all distinct node pairs, i.e. $|\Psi| = n(n-1)$. Π is the set of connected node pairs. It is worth noting that the failure metric, f_p, is closely related to K, such that $1 - f_p = K$. While K represents the probability of the connectedness between two arbitrary nodes, f_p represents the probability of the disconnectedness caused by an attack.

While there are several other metrics to measure the resiliency of a graph G such as its connectivity and toughness, these measures are inappropriate for Internet topologies. The connectivity of G is measured by finding the weakest points (subset of nodes or edges) of the graph G so that the failure of the points will disconnect the graph. More formally, a graph G is said to be k-connected if there does not exist a set of $k-1$ nodes whose removal disconnects the graph, i.e., the node connectivity of G is $\geq k$ where k is the size of minimum vertex cut. In addition, the edge connectivity of G is defined as the size of the minimum edge cut. The power-law Internet topologies have plenty of degree 1 nodes [7], therefore, node connectivity and edge connectivity is always 1. This monotony proves insufficiency as a metric of Internet topologies. As another metric, the toughness of a graph was introduced by Chvátal [24]. G is t-tough if $|S| \geq t \cdot w(G-S)$ for every subset S of $V(G)$ with $w(G-S) > 1$, where $w(G)$ is the number of components of G. Then, the toughness of Internet topologies is always 0 in the existence of degree 1 nodes. Therefore, these conventional metrics are not sufficient for measuring the resiliency of Internet topologies.

Attack power is proposed as a new metric for measuring the effect of an attack as the ratio of the failure to attack. Attack power is sensitive to the type of attack, which are presented in Fig. 7. The topology used in Fig. 7 is the same as the AS graph in Fig. 5 and Fig. 6. Node attacks can increase their power by 30 times by carefully selecting

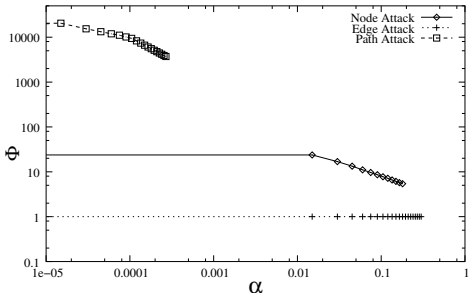

Fig. 7 Comparison of Φ for three types of attack: max-weight node attack, max-weight edge attack, max-weight path attack.

target nodes. However, the number of edge failures caused by edge attacks is only equal to the number of target edges, i.e. $\Phi = 1$. Path attacks have the most significant effect, with the damage being multiplied by four orders of magnitude. For instance, an attack on one path can destroy more than 20,000 paths, i.e. $\Phi = 20,000$. The failure of the most popular path gives impact on 20,000 other paths which share one or more edges with the failed path. Given a n-node network, there exist $(n^2 - n)$ distinct paths on the network. This establishes the fact that path-based attacks have an effect on $O(n^2)$ paths at maximum, whereas node-based attacks have an effect on $O(n)$ nodes at maximum. It also implies that attack power is dependent on network size.

Each curve in Fig. 7 can be seen to be decreasing toward $\Phi = 1.0$ as α increases, which shows the convergence of $f \to \alpha$. From the experiments, it is demonstrated that attack power Φ, as the ratio of the failure to attack, is an effective metric for measuring the impact of different attacks on a given topology in a quantitative way.

3.5 Applying Results

The proposed attack-and-failure model can be useful to analyze the resiliency of network topologies under attack. It is valuable to check the weakness of a newly-designed network and find a method to strengthen the network. In addition, we can rate candidate networks in terms of robustness, this assists in selecting the best topology.

Another application of this study is to find an evolving strategy for better topological structure in the future. In the Internet, edges are not created randomly but rather seem to follow a preferential attachment rule [8]. This implies that the rich get richer and the Internet will continue to concentrate on a small set of nodes. Instead of connecting every new link to one of the highest degree nodes, a better strategy needs to be found, making the Internet more robust.

4. Conclusion

We proposed an attack-and-failure model for the Internet with regard to link-based attacks and path-based attacks. Based on the experimental results, it is concluded that path-based attacks are likely to inflict greater damage to the connectivity of a network than other types of attack. Through the experiments, it is also shown that the Internet is more vulnerable than a random topology, and becomes more vulnerable as time passes.

Based on the fact that performing different types of attacks requires different amounts of resources and different degrees of control, we will investigate the cost required to mount each type of attack and its effectiveness. In addition, the goal of an attacker can be considered as an attempt to partition a network rather than complete disconnection. Network partitioning can be effective, if it isolates a section of a network from the desired destinations, particularly from crucial resources such as high-level name servers. Thus, the evaluation of the cost of an attack and its effectiveness will be the objective of future study. In addition, we will continue to create evolving strategies designed to make networks more resilient to attacks.

References

[1] H. Lee and J. Kim, "Attack resiliency of network topologies," Proc. of PDCAT, pp.609–612, Dec. 2004.
[2] K. Park and H. Lee, "On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets," Proc. of ACM SIGCOMM, pp.15–26, Aug. 2001.
[3] H. Tangmunarunkit, R. Govindan, S. Jamin, S. Shenker, and W. Willinger, "Network topology generators: Degree-based vs. structural," Proc. of ACM SIGCOMM, pp.147–159, Aug. 2002.
[4] R. Albert, H. Jeong, and A.L. Barabasi, "Error and attack tolerance of complex networks," Nature, pp.378–382, July 2000.
[5] S.T. Park, A. Khrabrov, D.M. Pennock, S. Lawrence, C.L. Giles, and L.H. Ungar, "Static and dynamic analysis of the internet's susceptibility to faults and attacks," Proc. of IEEE INFOCOM, 2003.
[6] M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On power-law relationships of the Internet topology," Proc. of ACM SIGCOMM, pp.251–262, 1999.
[7] G. Siganos, M. Faloutsos, P. Faloutsos, and C. Faloutsos, "Power laws and the AS-level internet topology," IEEE/ACM Transactions on Networking (TON), pp.514–524, Aug. 2003.
[8] P. Baldi, P. Frasconi, and P. Smyth, Modeling the Internet and the Web, John Wiley & Sons Ltd, 2003.
[9] J. Winick and S. Jamin, "Inet-3.0: Internet Topology Generator," Tech. Rep. CSE-TR-456-02, Department of EECS, University of Michigan, 2002. http://topology.eecs.umich.edu/.
[10] 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, April 2001.
[11] A. Chakrabarti and G. Manimaran, "Internet infrastructure security: A taxonomy," IEEE Network, pp.13–21, Nov/Dec. 2002.
[12] D. Magoni, "Tearing down the internet," IEEE Journal on Selected Areas in Communications, Aug. 2003.
[13] A. Broido, E. Nemeth, and K. Claffy, "Internet expansion, refinement and churn," European Trans. on Telecommunications, Jan. 2002.
[14] U. Hengarner, S. Moon, R. Mortier, and C. Diot, "Detection and analysis of routing loops in packet traces," Proc. of SIGCOMM IMW, 2002.
[15] R. Perlman, Network Layer Protocols with Byzantine Robustness, Ph.D. thesis, M.I.T., 1988.
[16] S. Kent, C. Lynn, and K. Seo, "Secure border gateway protocol (Secure-BGP)," IEEE Journal on Selected Areas in Communications, April 2000.
[17] L. Garber, "Denial-of-service attacks rip the Internet," Computer, pp.12–17, April 2000.
[18] R. Mahajan, S.M. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and

S. Shenker, “Controlling high bandwidth aggregates in the network,” ACM Computer Communication Review, July 2002.

[19] Cisco, “Strategies to protect against distributed denial of service (DDoS) attacks.” Updated News Flash, April 2003.

[20] J. Gross and J. Yellen, Graph Theory and Its Applications, CRC Press, Dec. 1998.

[21] V. Paxon, “End-to-end routing behavior in the internet,” IEEE/ACM Transactions on Networking (TON), vol.5, no.5, pp.601–615, Oct. 1997.

[22] Nat’l Lab. for Applied Network Research, “Routing data,” 2001. Supported by NFS, http://moat.nlanr.net/Routing/rawdata/.

[23] N. Spring, R. Mahajan, and D. Wetherall, “Measuring ISP topologies with Rocketfuel,” Proc. of ACM SIGCOMM, Aug. 2002.

[24] V. Chvátal, “Tough graphs and hamiltonian circuits,” Discrete Math., pp.215–228, 1973.