Attack Resiliency of Network Topologies*

Heejo Lee[1] and Jong Kim[2]

[1] Korea University, Seoul 136-701, South Korea
heejo@korea.ac.kr
[2] POSTECH, Pohang 790-784, South Korea
jkim@postech.ac.kr

Abstract. Network topology has no direct effect on the correctness of network protocols, however, it influences on the performance of networks and the survivability of the networks under attacks. In this paper, we examines the attack resiliency of network topologies and shows that the topological structure has direct impact on the robustness of a network under attacks.

1 Introduction

One research direction on Internet topology is to analyze the robustness of the Internet under network attacks [1–5]. One important nature of an attack is target-oriented and that nature can cause catastrophic failures on Internet connectivities [2, 3]. From the analysis of susceptibility to attacks as well as faults, Internet connectivities are more susceptible to malicious attacks than random failures [3], and failures on only a part of components of the Internet can break down the overall Internet infrastructure [2, 4]. On the other hand, the Internet has threads of connection with properties such as small vertex cover [1], which can be a potential "choke point" of the Internet. Thus, exploring topological characteristics of the Internet can be a springboard to enhance the robustness of the Internet infrastructure under malicious attacks.

In this paper, we analyze the resiliency of network topologies under various attacking scenarios. Given a graph G that represents a network topology, the target of an attack can be a set of "nodes", "edges" or "paths", where a path is a series of consecutive edges. Failures caused by an attack influence on the connectivity among nodes, which is represented by deleting the target elements on a graph G. The debilitating effects by attacks are measured for different types of topologies.

2 System Model

A network topology represents the connectivity structure among nodes. Fig. 1 shows three topologies with 10 nodes and 10 edges. Average distances among nodes decrease from the left graph to the right graph, while the dependencies on a single node increases.

* This work was supported in part by the ITRC program of the Korea Ministry of Information & Communications, the BK21 program of the Korea Ministry of Education.

K.-M. Liew et al. (Eds.): PDCAT 2004, LNCS 3320, pp. 638–641, 2004.

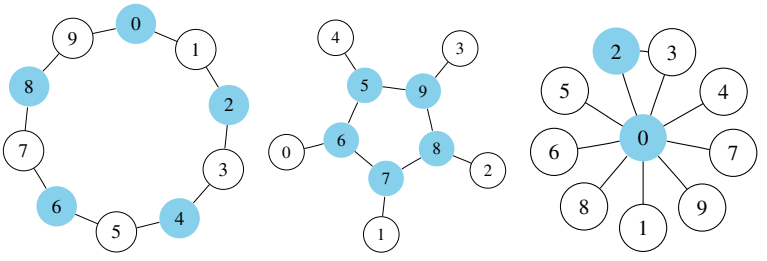

Fig. 1. Network topologies with 10 nodes and 10 edges

One node failure in the left graph does not disrupt the connectivity of other nodes, whereas the failure of the node 0 in the right graph significantly disconnects other nodes. Thus, the topology of a network gives impact on the networking performance and the robustness under attacks.

A network topology is given as 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 of deleting a subgraph T from G such that

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

Deletion of a node or an edge in a graph G is a well-defined operation as described in [6]. Deletion of a path is analogous to the deletion of every edge belonging to the 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. It implies that the failure by an attack could be larger than the target of the attack, i.e., $\mathcal{F}(\mathcal{A}) \supseteq T$.

There are three attacking types according to their targets: 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 shows three attack types: node attack with $T = \{3\}$, edge attack with $T = \{(3, 4)\}$ and 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 no attack so that $T = \{\}$, whereas $\alpha = 1$ means $T = G$. Thus, α implies the severity of an attack.

Attacks and their effects are separated by "cause" and "effect" such that an attack is a cause and the failure is its effect. The following failure metrics are used for measuring the effect of an attack. Node failure ratio is defined by $f_n = n_f/n$ where n_f is the number of failed nodes. Path failure ratio is defined by $f_p = 2 \cdot p_f/n(n-1)$ where p_f is the number of failed paths.

3 Resiliency Evaluation

To evaluate the attack resiliency, we use both AS-level Internet topologies and artificial graphs. We use AS connectivity graphs archived by NLANR from Oregon RouteView

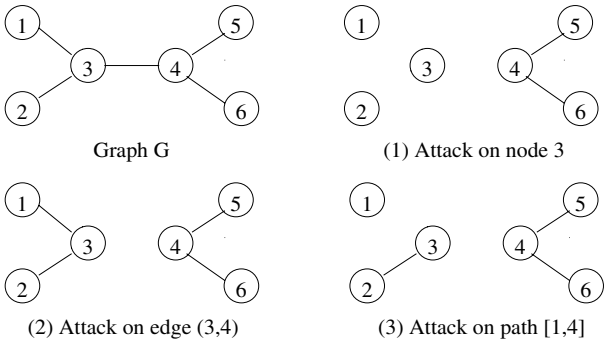

Fig. 2. Three attack types: (1) node attack, (2) edge attack, and (3) path attack

Project [7], which is the most widely used and publicly available data set for studying the Internet topologies. Random graph is generated by connecting two nodes with the linking probability corresponding to the AS connectivity at year 1997, which is $p = 0.001135$ from $p = 2e/n(n-1)$. Internet-like artificial graphs are created by using well-known topology generators such as Brite2.1 [8] and Inet3.0 [9]. Node distributions in the descending order of degree ranks are shown in Fig. 3 (Left), for the AS graphs and the artificial graphs, respectively. These figures show how far from the power-law distributions.

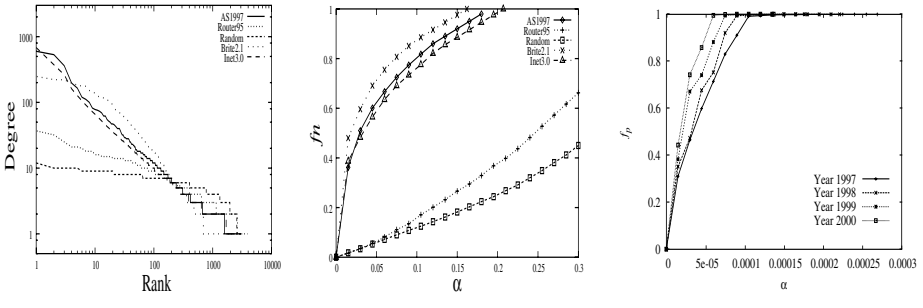

Fig. 3. (Left) Rank-degree distribution of network topologies. (Middle) Distribution of f_n on the node attack. (Right) Distribution of f_p on the path attack

The effects of network topologies are measured with both AS connectivities and router connectivities. Figure 3 (Middle) shows the distribution of f_n as a function of α on the node attack. This shows that AS1997, Brite2.1 and Inet3.0 are weaker than Random and Router95 under the node attack. This confirms that the robustness of the Internet is not better than the random topology.

The node failure ratio f_n jumps up to reach $f_n = 1.0$ at $\alpha = 0.18$, which is the ratio of vertex covering nodes in the Internet topologies [1]. This shows that an attack on vertex covering nodes significantly disconnects the network so that $\alpha = |VC|/n$ can make $f_n = 1$.

Experimental results on the Internet connectivities are shown in Figure 3 (Right). The distributions of f_p under the path attack show similar behaviors for the periods of year 1997 $\sim$ 2000. From the experiments, we can see that the Internet becomes more vulnerable as time goes on.

4 Conclusions

We have proposed several new techniques to model attacks on the Internet, as well as new failure metrics to evaluate the resiliency of the network. Path-based attacks could result in more severe damage on the connectivity of a network. From the comparison of topologies, the Internet is more vulnerable than random graphs, and even becomes worse as time goes on. The purpose of this study is to provide a foundation for finding protection mechanisms. Recent study argued that breakdown of the Internet by attacking nodes is not feasible due to the high connectivity of concentrated nodes. However, judicious placement of attacking sources and their well-targeting could render the whole network disability.

From the fact that performing different types of attacks requires different amount of resources and different degree of controls, we will study on attack costs required to mount attacks and their effectiveness. Also the goal of an attacker can be represented as partitioning a network instead of disconnecting an entire network. Network partitioning can be effective if it isolates some section of a network from desired destinations, particularly from crucial resources such as high-level name servers. Thus, evaluation of attack cost and effectiveness is the future work of this study. As well, this work will continue to find evolving strategies for making networks more resilient to attacks.

References

1. Park, K., Lee, H.: On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. ACM SIGCOMM. (2001) 15–26
2. Albert, R., Jeong, H., Barabasi, A.L.: Error and attack tolerance of complex networks. Nature (2000) 378–382
3. Park, S.T., Khrabrov, A., Pennock, D.M., Lawrence, S., Giles, C.L., Ungar, L.H.: Static and dynamic analysis of the internet's susceptibility to faults and attacks. IEEE INFOCOM. (2003)
4. Chakrabarti, A., Manimaran, G.: Internet infrastructure security: A taxonomy. IEEE Network (2002) 13–21
5. Magoni, D.: Tearing down the internet. IEEE JSAC (2003)
6. Gross, J., Yellen, J.: Graph Theory and Its Applications. CRC Press (1998)
7. Nat'l Lab. for Applied Network Research: Routing data (2001) Supported by NFS, http://moat.nlanr.net/Routing/rawdata/
8. Medina, A., Lakhina, A., Matta, I., Byers, J.: Brite: Universal topology generation from a user's perspective. BUCS-TR-2001-003, Boston University (2001)
9. Winick, J., Jamin, S.: Inet-3.0: Internet Topology Generator. CSE-TR-456-02, University of Michigan (2002)