Improving Resiliency of Network Topology with Enhanced Evolving Strategies

Soo Kim[†], Heejo Lee[†*], Wan Yeon Lee[‡]
[†]Korea University [‡]Hallym University
heejo@korea.ac.kr

***Abstract*— Recent studies have shown that many real networks follow the power-law distribution of node degrees. Instead of random connectivity, however, power-law connectivity suffers from the vulnerability of targeted attacks, since its interconnection is heavily relying on a very few nodes. In addition, the connectivity of power-law networks becomes more concentrated on the small group of nodes as time goes by, which can be explained by Barabasi and Albert's rich-get-richer model. The rich-get-richer model is known as the most widely accepted generative model and follows the rule of preferential attachment to high-degree nodes. Thus, the preference of high-degree nodes to connect a newly created node renders the network less resilient as evolves. In this paper, we propose three different evolving strategies which can be applicable to the Internet topologies and the resiliency of evolving networks are measured by two resiliency metrics. From the experiments, we show that choosing an appropriate evolving strategy is more effective to increase the resiliency of network topology, rather than simply adding more links. Also, we show the possibility of improving the attack resiliency of Internet topology by adapting only a part of networks, e.g. 20–40%, to a new evolving strategy, such as change from the max-degree preference to the average-degree preference, which can be considered as a practical range of deployment.**

***Keywords*— Evolving strategy, attack resiliency, power-law distribution, network topology.**

I. Introduction

The Internet can be represented as a huge topology which is composed of innumerable computers and links between them. Previous studies have shown that the Internet expands its topology over time, and the distribution of the number of connections per node follows a *power-law* distribution. The power-law distribution also expresses the relation between degree, rank and frequency of a node [1], [2]. It was suggested that the probability of attachment between existing nodes and a newly generated node is proportional to the degree of existing nodes, *i.e.preferential attachment* [3], [4], then the resulting network leads to the power-law distribution. Recent studies found that network topologies evolving with the strategy of preferential attachment, including the Internet, are getting less resilient to network attacks [5], [6].

In this paper, we present a topological and degree-based approach to measure the attack resiliency of a network topology. Power-law networks like the Internet are vulnerable to the attack on high-degree nodes, which can give serious damage to a network. We suggest two metrics which reflect the attack resiliency. One metric, ν, is a vertex cover ratio which have been used in previous studies [5], [6]. Three evolving strategies are also suggested to expand a network topology. *Max* strategy let a newly generated node attach to a high-degree node. *Avg* strategy makes a newly generated node has higher probability of being connected to average-degree nodes. *Min* strategy has probability distribution that prefers minimum-degree nodes. Evaluation shows the effectiveness of suggested evolving strategies under various network environments.

The main contribution of this paper consists of four parts. First, we propose three evolving strategies and the resiliency of growing networks are measured by two resiliency metrics. One metric is the ratio of vertex covering nodes, and the other metric is the connectivity of the remaining network after the occurrence of an attack. Second, we show that the current Internet topology becomes weaker and weaker over time, using the resiliency metrics. Third, we show that it is possible to increase the resiliency of network topology by altering the current evolving strategy to another one. Furthermore, the increment of attack resiliency can be achievable in a practical range, such as 20–40% of deployment of new strategies. Finally, it is shown that the best strategy can be found for designing newborn networks as well as existing power-law networks.

II. System model

In this section, we set resiliency metrics, topological graphs and preferential attachment strategies as system model.

A. Resiliency metrics

Previous studies on network resiliency have used the ratio of vertex covering nodes as one resiliency metric [5], [6]. Let ν denote the ratio of vertex cover as the primary metric in this paper, such that

$$\nu = \frac{|VC|}{n} \tag{1}$$

where $|VC|$ is the cardinality of the minimum vertex cover of a graph and n is the number of nodes in the graph. ν represents the attack resiliency of network topologies, such as a graph which has small ν can be seriously demolished by attacking the small number of vertex covering nodes. This metric also represents the balance of degree distribution.

Since ν is a static property of a graph and does not necessarily carry the dynamic property under attack, we propose

This work was supported in part by the ITRC program of the Korea Ministry of Information & Communications under the grant IITA-2005-(C1090-0502-0020) and the BK21 program of the Korea Ministry of Education.

* To whom all correspondence should be addressed.

another metric based on the connectivity of the remaining network after the occurrence of an attack. The secondary metric also represents attack resiliency of a network topology. The difference between this metric and ν is that this metric shows the subgraph distribution *after* attacks. We show

$$\tau(i) = \frac{\sum_{j=1}^{s_i} n_j(n_j - 1)}{n(n-1)} \tag{2}$$

where s_i is number of subgraphs after i node attacks, n is number of nodes in a graph and n_j is number of nodes in the jth subgraph after i node attacks. We remark that i varies from 0 to n in Eq. (2) and τ is difficult to compare resiliency between topological graphs with different node size when i is a fixed value. $K(\alpha)$ is a normalized function of τ using α $(0 < \alpha \leq 1)$, the ratio of the total node size n. Namely, we show

$$K(\alpha) = \tau([\alpha \cdot n_{init}]) \tag{3}$$

where n_{init} is a constant node size of an initial graph which is not influenced by node increment. $[\alpha \cdot n_{init}]$ is an integer value since this parameter is the number of attacked nodes. Priority of attacked nodes is decided by the degree of nodes for maximizing attack influence. K is proportional to the size of the biggest subgraph by Fig. 3. For example, two subgraphs of node size 8 and 2 make K higher than two subgraphs of node size 5 and 5. This metric is significant since graph size of the majority subgraph represents attack resiliency. K also represents connectivity of minor subgraphs unlike the metrics used in [7] and [8]. This property is critical to distinguish the resiliency of these two subgraph groups: {5, 4} and {5, 2, 2}. Numbers in the brackets are node sizes of subgraphs. It is obvious that the former subgraph group has better connectivity than the latter. K distinguishes the connectivity of two groups, while the metric used in [7] and [8] is same in both groups.

B. Topological graphs

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 [5]. We use two power-law graphs *i.e.*AS full connectivity graph of 1997 and 2006 (will be expressed as AS-1997 and AS-2006 from now on) for resiliency evaluation of the Internet [10], [11]. In addition, three 200-node graphs *i.e.*a ring-shaped graph, a star-shaped graph and a power-law graph are used to evaluate how the resiliency metrics change by the shape of a base graph. We also use a 2-node graph to measure resiliency of a newly emerging network.

C. Modeling evolving strategies

In many real networks, edges are not created independently at random, but rather seem to follow some preferential attachment rule [3]. Preferential attachment is modeled by assuming that the probability that a newly created vertex v is connected to an existing vertex w is proportional to the degree $k_w(t)$ of w, so that the corresponding probability of attachment is given by $k_w / \sum_r k_r$ [4]. However, it is known that nonlinear forms of preferential attachment do not lead to stationary power-law distribution [3]. We use three basic evolving strategies by degree-based probability distribution which are:

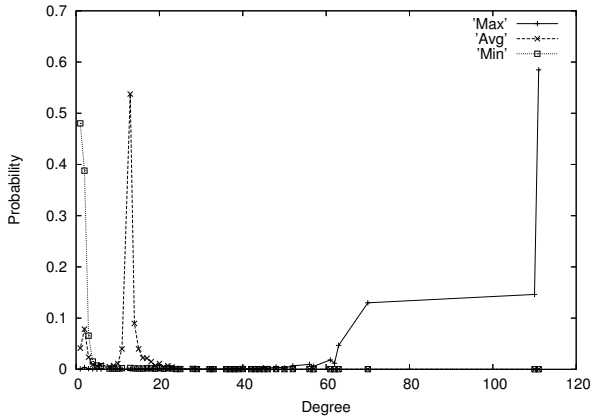

Fig. 1. Probability distribution of three evolving strategies.

- ***Max* strategy:** A newly generated node has a tendency to be connected to higher degree nodes. This strategy follows the power-law 1 in [1], i.e., $d_v \propto r_v^R$, to expand a topology.
- ***Avg* strategy:** A newly generated node has a tendency to be connected to average-degree nodes, with higher probability than to other nodes.
- ***Min* strategy:** A newly generated node has a tendency to be connected to minimum-degree nodes, with higher probability than to other nodes.

Let $P_{max}(d)$ denote the probability of *Max* strategy at degree d such that

$$P_{max}(d) = f_d \cdot {r_d}^R \cdot \Big(\sum_j f_j \cdot {r_j}^R \Big)^{-1} \tag{4}$$

where f_d is the frequency of a degree d, r_d is the rank of a degree d, R is the rank exponent in [1] and j is the number of different degrees. This probability distribution function has similar characteristics with the previous topology generator Inet [9], which also obeys the *power-law*. Modified rank ω for *Avg* strategy is expressed as

$$\omega = 1 + |d_{avg} - d| \tag{5}$$

where d_{avg} is the rounded integer of the average degree. Using Eq. 5, we briefly show that the probability distribution function of *Avg* strategy is

$$P_{avg}(d) = f_d \cdot {\omega_d}^W \cdot \Big(\sum_j f_j \cdot {\omega_j}^W \Big)^{-1} \tag{6}$$

where W is the modified rank exponent. Finally, the probability distribution of *Min* strategy is shown to be

$$P_{min}(d) = f_d \cdot d^D \cdot \Big(\sum_j f_j \cdot {d_j}^D \Big)^{-1} \tag{7}$$

where D is the degree exponent [1]. Fig. 1 shows probability distribution of three evolving strategies at the 200-node subgraph extracted from the AS-2006 graph with exponents $R = -2$, $W = -2$ and $D = -1$. *Max* strategy has the highest probability at the maximum-degree ($d = 111$) node. Likewise, *Avg* strategy has the highest probability at the average-degree ($d = 13$) node and *Min* strategy has the highest probability at the minimum-degree ($d = 1$) node. A small peak of P_{avg}

shown in $1 \leq d \leq 3$ is due to relatively high frequency of low-degree nodes.

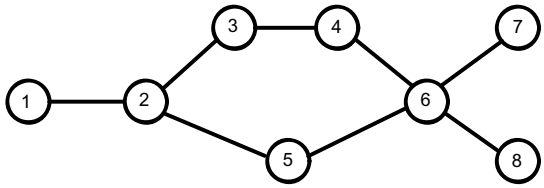

Fig. 2. A sample graph of network topology

Probability distribution in Fig. 2 for each strategy is calculated as follows. Let n be the number of nodes that $1 \leq n \leq 8$. Degrees of each node are: $d_1 = 1$, $d_2 = 3$, $d_3 = 2$, $d_4 = 2$, $d_5 = 2$, $d_6 = 4$, $d_7 = 1$ and $d_8 = 1$. Next step is to calculate r_d, f_d and ω_d for $1 \leq d \leq 4$ to use Eqs. 4, 6 and 7. Calculated probabilities of three evolving strategies are shown in Table I.

TABLE I

PROBABILITY OF EVOLVING STRATEGIES IN FIG. 2

d	r_d	f_d	ω_d	$P_{max}(d)$	$P_{avg}(d)$	$P_{min}(d)$
1	6	3	2	0.05	0.1824	0.5902
2	3	3	1	0.2	0.7297	0.2951
3	2	1	2	0.15	0.0608	0.0655
4	1	1	3	0.6	0.0271	0.0492

There are three strategies if $d_{new} = 1$, where d_{new} is the degree of newly generated nodes: *Max, Avg* and *Min*. *Max* strategy is that a newly generated node has probability P_{max} to make a connection with existing nodes, which means a new node tends to be connected with the maximum-degree node of a graph. Similarly, *Avg* strategy gives P_{avg} and *Min* gives P_{min} to newly generated nodes. In case of $d_{new} = 2$, six strategies can be made by combining the three basic strategies: *Max-Max, Avg-Avg, Min-Min, Max-Avg, Max-Min* and *Avg-Min*. *Max-Min* strategy, for example, gives P_{max} and P_{min} to newly generated nodes; a new node with degree 2 tends to make connection with one high-degree node and one low-degree node.

III. EXPERIMENTAL RESULTS

In this section, we take various experiments for measuring the attack resiliency of growing networks via the evolving strategies. The simulator is developed for modeling attacks and network connectivities, which is implemented by the Java programming language [12]. Each simulation run is performed on a connected and undirected graph as follows. Given a set of nodes and edges, a node is added to the graph with d_{new} uniform number of edges. Attack targets to the graph are a set of nodes, which are decided by the degree of nodes. We set d_{new} to 1 in every simulation since that assumption makes the resiliency of a network worst. Exceptionally, simulations using $d_{new} = 2$ and $d_{new} = 3$ are performed in the fourth subsection, *Varying* d_{new}.

A. Power-law internet

The node size of the Internet topology has been increasing rapidly; AS-2006 graph has 22035 nodes, while AS-1997 graph has 3015 nodes. Resiliency metrics of AS-1997 graph are $\nu \approx 0.1914$ and $K(0.001) \approx 0.2827$. However, the metrics have been decreased to $\nu \approx 0.1451$ and $K(0.001) \approx 0.1809$ in AS-2006 graph. It means that the Internet is getting less resilient to attacks.

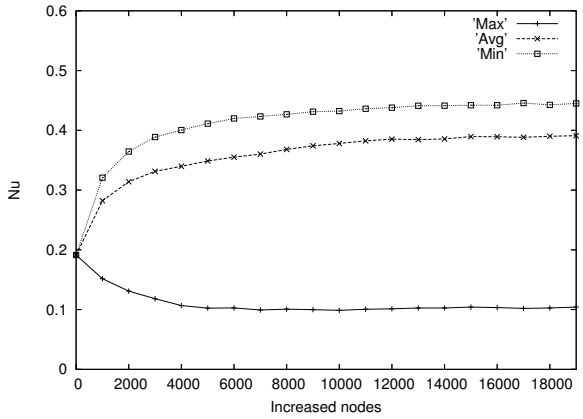

Fig. 3. ν vs. increased nodes in AS-1997 graph

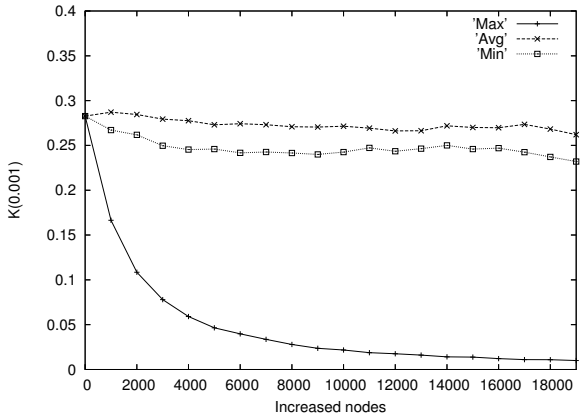

Fig. 4. $K(0.001)$ vs. increased nodes in AS-1997 graph

We add 19000 nodes to AS-1997 graph by three evolving strategies, where new nodes are connected with degree one, *i.e.*, $d_{new} = 1$. Using the two resiliency metrics, we measure the resiliency of evolving networks. Fig. 3 shows how ν changes in three evolving strategies. *Max* strategy decreases ν, while *Avg* and *Min* strategies increase the metric higher than 0.3. We can see that *Min* strategy is the best strategy to increase ν. On the other hand, *Avg* strategy is the best strategy for metric K, although it cannot increase the metric higher than the initial value. The decline of $K(0.001)$ in all three strategies, shown in Fig. 4, is caused by d_{new}, which is always set to 1 for all newly generated nodes. Metrics difference between AS-2006 graph and *Max* strategy result is caused by rank exponent R in Eq. 4. R is -2 in the experiment, which makes the preference to maximum degree node more strict than -0.75, previously computed rank exponent in AS level [9].

B. Regular graphs

In this part, we discuss the impact of a base graph on the resiliency of evolving networks. We use three graphs with 200 nodes as a base graph: a ring graph, a star graph and a power-law graph. We add 1200 nodes to each initial graph since we

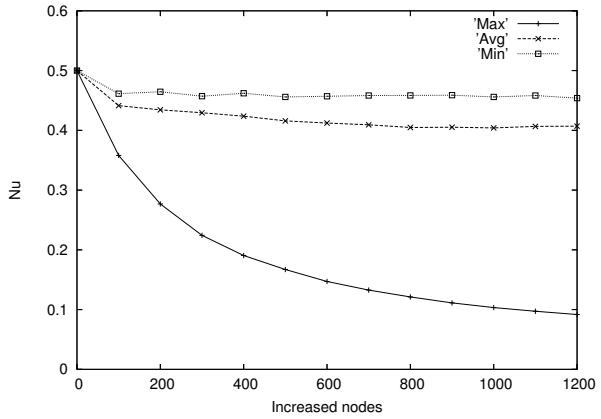

Fig. 5. ν vs. increased nodes in 200-node ring-shaped graph

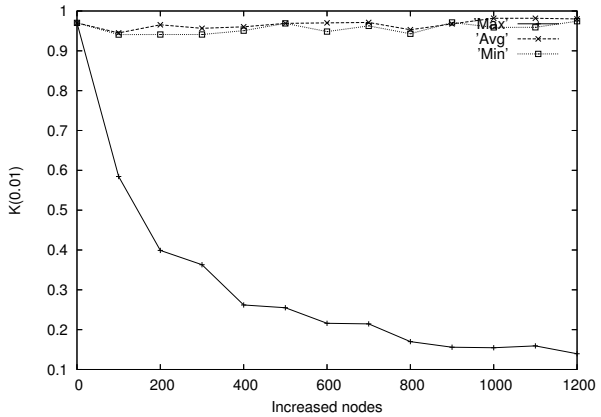

Fig. 6. $K(0.01)$ vs. increased nodes in 200-node ring-shaped graph

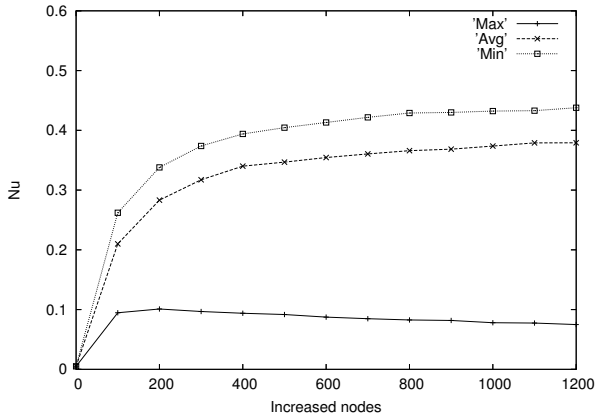

Fig. 7. ν vs. increased nodes in 200-node star-shaped graph

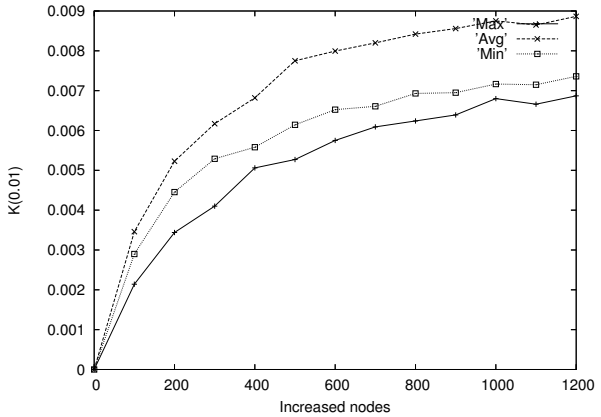

Fig. 8. $K(0.01)$ vs. increased nodes in 200-node star-shaped graph

septupled the node size of the former experiment for power-law internets.

The first regular graph used in the experiment is a ring-shaped graph. In *Max* strategy, ν decreased from 0.5 to 0.1, while *Avg* and *Min* strategies showed relatively low decline between 0.4 and 0.5 as shown in Fig. 5. All of the strategies cannot increase ν more than the initial value, since an initial ring-shaped graph is resilient enough to have higher ν than the real internet graph. Therefore we can measure the resiliency of each strategy by the slope of ν decline. The result of $K(0.01)$, shown in Fig. 6 is similar to ν that *Max* strategy shows lower value than *Avg* and *Min* strategies. It is also shown that K transition of *Avg* strategy and *Min* strategy are almost same while *Min* strategy has higher values than *Avg* strategy in ν transition.

A star-shaped graph, the second regular graph used in the experiment, has extremely low ν and $K(\alpha)$ since an attack to the central node gives critical damage to the entire graph. It also means the properties of this graph is contrary to a ring-shaped graph. In the experiment, both initial metrics are close to zero as shown in in Fig. 7 and Fig. 8. Transition of ν is *Min* $>$ *Avg* $>$ *Max*, which is different from transition of $K(0.01)$: *Avg* $>$ *Min* $>$ *Max*. ν transition in *Max* strategy in Fig. 5 shows that the metric increases until 200 nodes are added, but slightly decreases afterwards. Another characteristic in a star-shaped graph is that the gap of K between *Max* strategy and *non-Max* strategies is not so big as other graphs used in the experiment.

The third regular graph is a power-law graph, *i.e.*a 200-node subgraph of AS-2006 graph. ν of a power-law graph, shown in Fig. 9, shows the inefficiency of *Max* strategy in terms of resiliency. Compared with that *Avg* and *Min* strategies increases ν, *Max* strategy decreases ν from 0.2 to 0.1. In addition, *Max* strategy brings $K(0.01)$ the worst in Fig. 10 (*Avg* $>$ *Min* $>$ *Max*). We can also see that this subgraph of the Internet graph has similar properties to the original internet graph by comparing Fig. 3 and Fig. 9. The difference between Fig. 4 and Fig. 10 is due to the node number of its initial graph, which is crucial factor to transit K.

C. Constructing a new network

Unlike the Internet, the topology of a newborn network like local-area network(LAN) can be optimally designed considering the attack resiliency. It is also flexible to apply and modify various strategies to find the optimal evolving strategy in a newborn network environment. Fig. 11 and Fig. 12 show ν and $K(0.05)$ increasing 1200 nodes in the 2-node graph ($d_{new} = 1$). *Max* strategy makes both ν and K worst of the three strategies. We can see that both *Avg* and *Min* strategies are much more effective than *Max* strategy for attack resiliency, though they cannot increase ν higher than the initial value. It is shown that the best strategy for ν is *Min* strategy, which is uniformly better than *Avg* strategy.

Like the Internet graph, a star-shaped graph and a power-law subgraph, *Avg* strategy is the best strategy for increasing

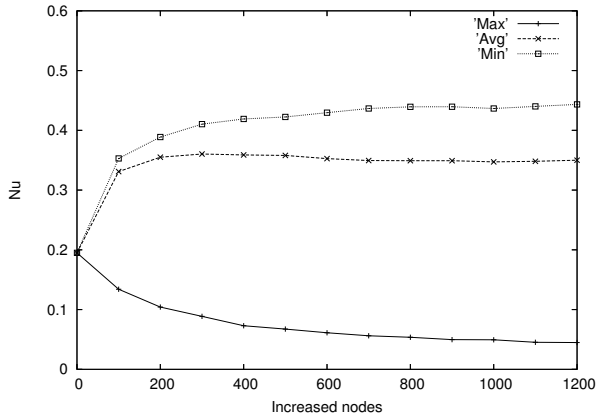

Fig. 9. ν vs. increased nodes in 200-node power-law graph

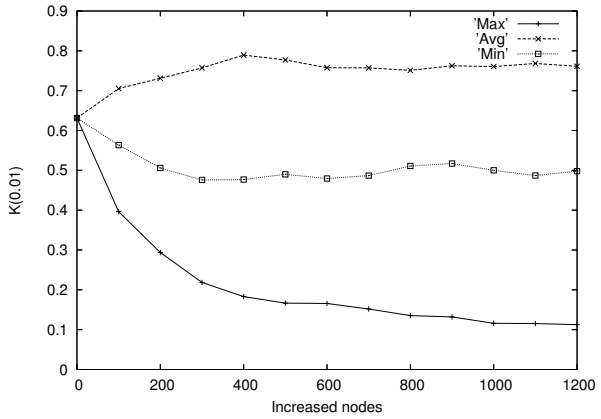

Fig. 10. $K(0.01)$ vs. increased nodes in 200-node power-law graph

$K(0.01)$ as shown in Fig. 12. We can see that *Min* strategy is the best strategy to increase ν and *Avg* strategy is the best to increase $K(\alpha)$ via the former experiment results. It is also revealed that ν converges to uniform scope by strategy after n-node expansion; $\nu_{max} \sim 0.1$, $\nu_{avg} \sim 0.4$ and $\nu_{min} \sim 0.45$. This means the resiliency is influenced by evolving strategy more than by the shape of a base graph.

D. Varying d_{new}

In this part, we evaluate the resiliency effectiveness of d_{new} in the 2-node graph. We add new nodes to an initial graph using three different d_{new} (1, 2 and 3). In addition we compare d_{new} variation result and strategy variation result to discover the better method for increasing attack resiliency.

We add 1200 nodes to a 2-node graph using *Max* strategy. *Max* strategy with $d_{new} = 2$ is that a newly generated node tends to attach to two distinct high-degree nodes and *Max* strategy with $d_{new} = 3$ is likewise. Fig. 13 shows that increasing d_{new} does not increase ν effectively. Comparing $\nu \sim 0.15$ in *Max* strategy with $d_{new} = 3$ and $\nu \sim 0.4$ in *Avg* strategy with $d_{new} = 1$, we can see that choosing *non-Max* strategy is more effective to increase ν than increasing d_{new}. Choosing *non-Max* strategy is also more effective to increase $K(\alpha)$ than increment of d_{new}, comparing $K(0.01) \sim 0.45$ in *Max* strategy with $d_{new} = 3$ and $K(0.01) \sim 0.8$ in *Min* strategy with $d_{new} = 1$. However, increasing d_{new} is effective to increase K, more than to increase ν.

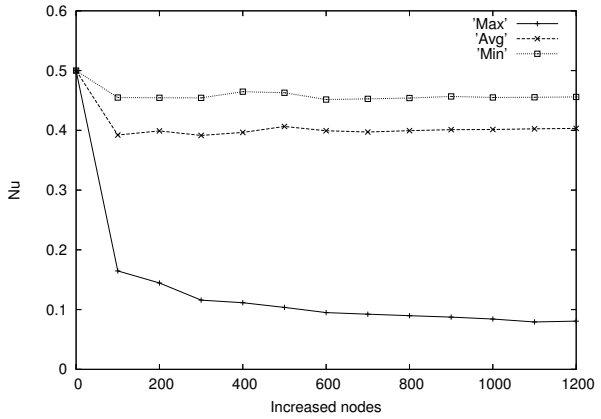

Fig. 11. ν vs. increased nodes in the 2-node graph ($d_{new} = 1$)

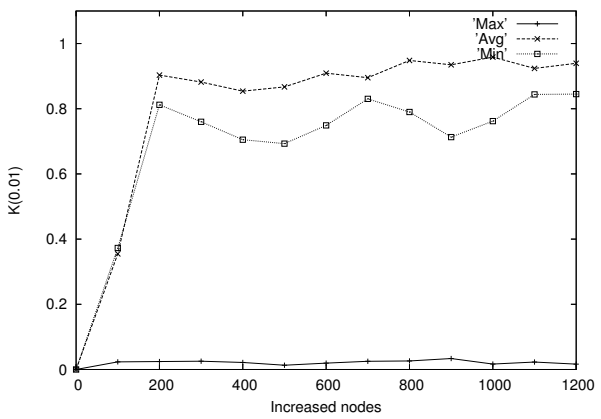

Fig. 12. $K(0.01)$ vs. increased nodes in the 2-node graph ($d_{new} = 1$)

IV. Evaluation and Practical Consideration

It is not difficult to apply the best evolving strategy for attack resiliency to newborn networks or small-sized networks like LAN. We can see that *Min* strategy is the most effective strategy to increase ν, and *Avg* strategy is the best for $K(\alpha)$ via Fig. 11 and 12. In addition, it is obvious that choosing an appropriate strategy is much more effective than increasing d_{new}, comparing Fig. 11 and Fig. 12 with Fig. 13 and Fig. 14 as we mentioned in the previous section.

However, it is difficult to apply the best evolving strategy for attack resiliency to power-law networks, especially large networks like the Internet. Practically low-degree nodes on the Internet have relatively lower bandwidth than high-degree nodes, which let a newly generated node attach to high-degree nodes. There are also commercial problems to connect new nodes with existing nodes. Fig. 15 shows how the resiliency metrics transit by the ratio of *Max* strategy and *Avg* strategy in 200-node power-law graph with $d_{new} = 1$. We take *Avg* strategy for the experiment, not *Min* strategy, since *Avg* strategy has higher possibility to have large bandwidth and attraction to new nodes than *Min* strategy. If more than 60% of newly generated nodes on the graph obey *Avg* strategy, ν can exceed the initial value. Similarly, more than 90% of newly generated nodes should follow *Avg* strategy to increase $K(0.001)$.

We repeat the same experiment varying d_{new} from 2 to 4 for decreasing *Avg* strategy's ratio. Because, 60% and 90%

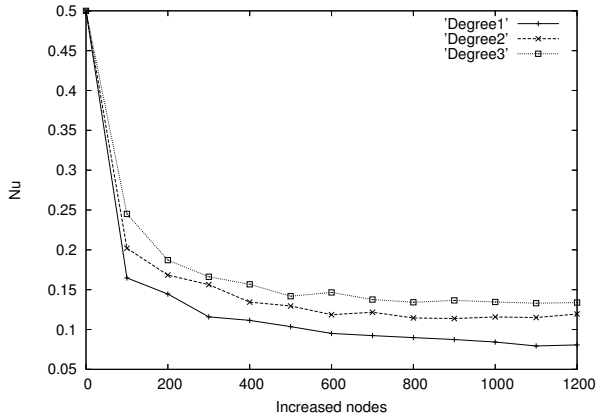

Fig. 13. ν vs. increased nodes in the 2-node graph using *Max* strategy

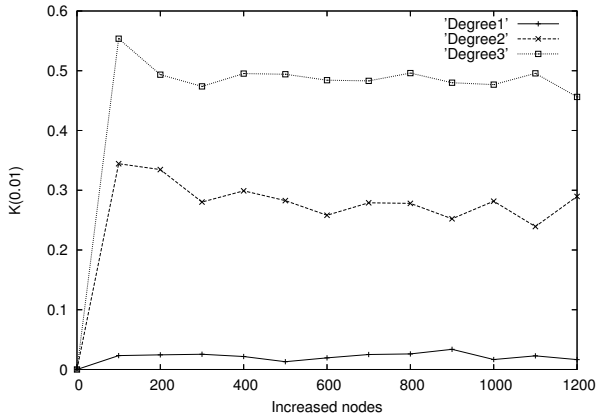

Fig. 14. $K(0.01)$ vs. increased nodes in the 2-node graph using *Max* strategy

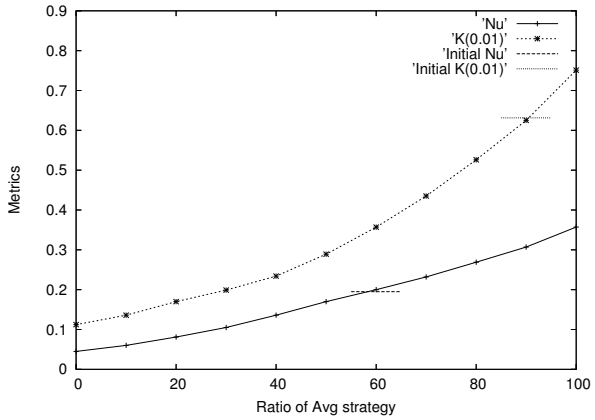

Fig. 15. Metrics transition in 200-node power-law graph with $d_{new} = 1$ using *Max* strategy and *Avg* strategy

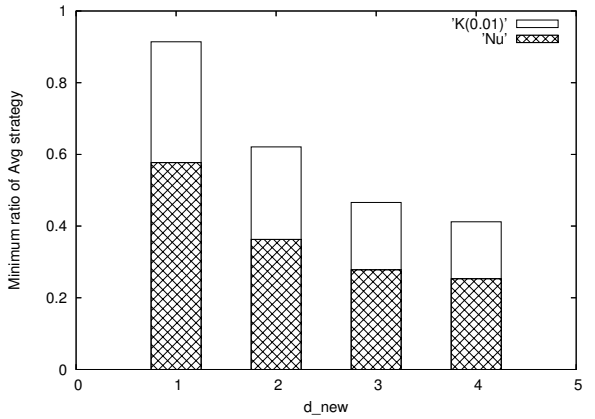

Fig. 16. d_{new} vs. minimum ratio of *Avg* strategy for increasing metrics in 200-node power-law graph

of ASs are enforced to change their evolving strategies for increasing attack resiliency, which means it is very hard to be applied to the practical situation. The experimental results in Fig. 16 shows that increasing d_{new} reduces the minimum ratio of *Avg* strategy for attack resiliency. 60% of newly generated nodes should obey *Avg* strategy to increase both ν and $K(0.001)$ with $d_{new} = 2$, 47% with $d_{new} = 3$ and 42% with $d_{new} = 4$. Therefore, both using *Avg* strategy and increasing d_{new} for newly generated nodes can practically make power-law networks more resilient to attacks. As shown in Fig. 16, 20–40% of adapting *Avg* strategy can be considered as a practical range of deployment.

V. CONCLUSION AND FUTURE RESEARCH

In this paper we have presented the resiliency metrics and evolving strategies of network topology. *Max* strategy, which obeys power-law, showed the worst attack resiliency in all experimental environments. *Avg* strategy is the best strategy for $K(\alpha)$ and *Min* strategy for ν. Therefore, it is required to expand nodes by *non-max* strategies better than *Max* strategy for network resiliency. We can also know that transition of ν and $K(\alpha)$ is mostly influenced by evolving strategies, not by the shape of a base graph. Another finding is that both using *Avg* strategy and increasing d_{new} can increase attack resiliency of power-law graphs like the Internet under practical consideration.

Our future research heads to vary the distribution of d_{new} obeying power-law $f_d \propto d^{\mathcal{O}}$ in [1], since the degree of newly generated nodes was fixed in each experiments. Another future work is considering distances between nodes and bandwidth for better network performance.

REFERENCES

[1] M. Faloutsos, P. Faloutsos and C. Faloutsos, "On power-law relationships of the Internet topology," Proc. of ACM SIGCOMM, pp.251-262, 1999.
[2] G. Siganos, M. Faloutsos, P. Faloutsos and C. Faloutsos, "Power-laws and the AS-level internet topology," *IEEE/ACM Transactions on Networking*, pp.514-524, Aug. 2003.
[3] P. Baldi, P. Frasconi and P. Smyth, Modeling the Internet and the Web, John Wiley & Sons Ltd, Aug. 2003.
[4] A. Barabasi and R. Albert, "Emergence of scaling in random networks," Science, 286:509-512, 1999.
[5] H. Lee and J. Kim, "Attack resiliency of network topologies," Proc. of PDCAT, pp.609-612, Dec. 2004.
[6] 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.
[7] R. Albert, H. Jeong and A.L.Barabasi, "Error and attack tolerance of complex networks," Nature, pp.378-382, Jul. 2000.
[8] D. Magoni, "Tearing down the internet," IEEE Journal on Selected Areas in Communications, Aug. 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. Selcuk, K. Park and H. Lee, "The Static DPF Simulator (v.2)," Tech. Rep. CSD-TR 02-008, Department of CS, Purdue University, Sep. 2002.
[11] University of Oregon Route Views Project Archive. Available at http://archive.routeviews.org/oix-route-views/.
[12] Java SE. Available at http://java.sun.com/.