Relations of Network Characteristics and Protection Strategies against Attacks

Yihjia Tsai, Chen-Han Yao, Wen-Fa Huang, You-Shan Lin, Chin-Hou Chou
Department of Computer Science and Information Engineering
Tamkang University
151 Ying-chuan Road, Tamsui, Taipei
TAIWAN
{eplusplus, jj1011, huangwenfa, outrag} @gmail.com, chou2729@hotmail.com

Abstract

The real-world networks are large and complex entities and there are many studies on mathematical models in simulating real-network structure. This paper proposed a platform to simulate protection strategies against attacks in order to gain better understanding of the relation between network characteristics and information security [1] [2]. We set up several attack and protection strategies in three network models. The attacker carries out attack and the defender uses limited resources to improve the defenses of network. For a given cost of attacks, we will analyze the impacts of network characteristics and show their effectiveness of protection.

Keywords：*Cluster Coefficient, Betweenness, Scale-Free network, Small-World network*

1. Introduction

Random network model is frequently used to study real-network, however, the real-network contains complex structures and characteristics that are not sufficiently expressed by random network model. Thus we use three network models to represent real-network. The network attackers and defenders have different strategies. The attacker will apply strategies to minimize the attack cost. The defender has limited resources, and allocate minimal resources [3] [4] in achieving the effect of protection.

In this paper three models are used to represents different characteristics of network. Resources will be allocated in the nodes, edge do not contain any weight. The action of attack will spend an equal amount of cost as the protection resources in the nodes in order to occupy or pass through the nodes.

2. Network Characteristics

The degree of node i is denoted by d_i, and the set of adjacent nodes of i is represented by N_i. Absolute value of a set equals to the number of elements in the set, thus $d_i =| N_i |$. Let C_i be the clustering coefficient of node i. $C_i = 2E_i / d_i(d_i - 1)$, E_i is the total number of connections between nodes in N_i. The maximum value of E_i is $d_i*(d_i-1)/2$, thus C_i is a ratio between 0 and 1. If E_i is written as $E_i = \sum_{j\in N_i} | N_j \cap N_i | /2$, then C_i can be rewritten as $C_i = \sum_{j\in N_i} | N_j \cap N_i | / d_i(d_i - 1)$

The betweenness value of nodes represents the importance of each node in the network. The value show the frequency of node i in the list of shortest paths between any two given nodes. Define β_i as the betweenness value of node i $\beta_i = \sum_{\substack{s\neq i\neq t\in V \\ s\neq t}} \sigma_{st}(i) / \sigma_{st}$, σ_{st} is the number of shortest path from node s to node t. $\sigma_{st}(i)$ is the number of shortest path from node s to node t passing through node i. β_i is thus a value between 0 and 1.

3. Network Models

Three well known network models used in this study are the random network [5] , scale-free network [6] and small-world network [7]. Random network is constructed by randomly connect any two nodes. Scale-free network contains a few nodes with high degree, and the other nodes have low degree. This characteristic remains unchanged despite of the network size. Node degrees of the majority of nodes in small-world network are rather alike. Small-world network has a higher average clustering coefficient and shorter path distance between any two nodes than scale-free network.

We assume that resources are allocated in the node, and the total defending resources are equal to attack cost. We further assume that the attacker knows the network structure and calculates attacking path in advance.

978-1-4244-5228-6/09/$26.00 c2009 IEEE

4. Attack & Protection Strategies

Two attack strategies are studied in this paper, uniform attack strategy (UAS) and non-uniform attack strategy (NAS). Uniform attack strategy (UAS) chooses the path of attack with uniform probability. Non-uniform attack strategy (NAS) selects the path of attack taking into consideration network characteristics. Each node in the network, its importance was different, so the attack path will have two properties: (1) attack more nodes, (2) choose the most important nodes to attack. This attack can be more effect of the path by a greater impact.

Four resource allocation strategies are used: uniform distribution; degree distribution; clustering coefficient distribution and betweenness distribution.

A. Uniform distribution: Refers to the average resources allocated to all nodes. If *R* is the total resources, then assigned to each node of resources for *R/n*, where *n* is the number of nodes in the network.
B. Degree distribution: Calculate the degree of each node and normalized for the rate. Then allocate resources to each node by this rate.
C. Clustering coefficient distribution: Calculate the clustering coefficient for each node, normalize and allocate resources by the rate.
D. Betweenness distribution: Calculate the betweenness of each node for the rate, and then use this rate to allocate resources on the nodes.

5. Simulation Result

5.1. UAS vs. protection strategies

In this subsection, three network models adopting uniform protection strategies are simulated. Figure 1 shows the relations between the costs of attack for three network models.

5.1.1. UAS vs. uniform distribution

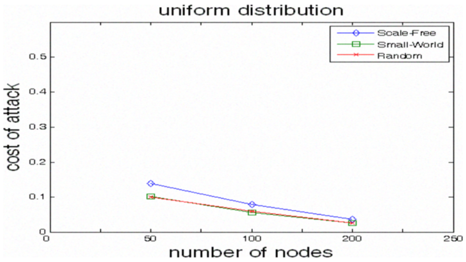

Figure 1. UAS vs. uniform distribution cost graph

For uniform distribution strategy, defender allocates most of the resources in some nodes that have lower probability to be attacked. All three network models have similar value of attack costs; this indicates that uniform protection strategy can not provide effective defenses.

5.1.2. UAS vs. degree distribution

The following three figures, Figure 2, 3 and 4, illustrate the degree distribution of the three network models with one hundred nodes.

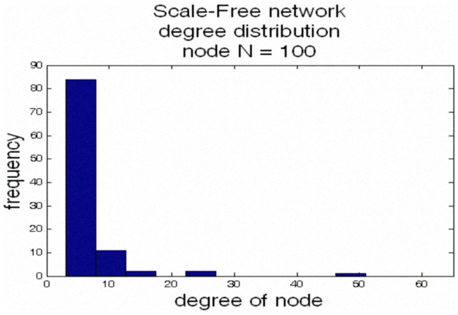

Figure 2. degree distribution in scale-free network

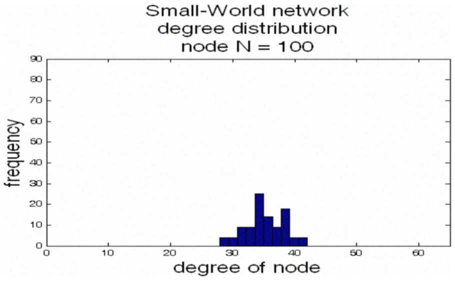

Figure 3. degree distribution in small-world network

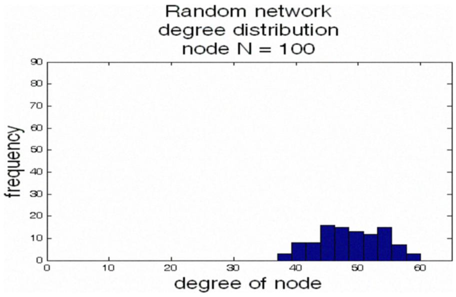

Figure 4. degree distribution in random network

From Figure 2, one prominent characteristic of the scale-free network is that only few nodes have high node degree, and the majority of nodes have low node degree. The degree distributions in the small-world network and random network are similar. Figure 5 shows the cost of UAS vs. degree distribution strategy.

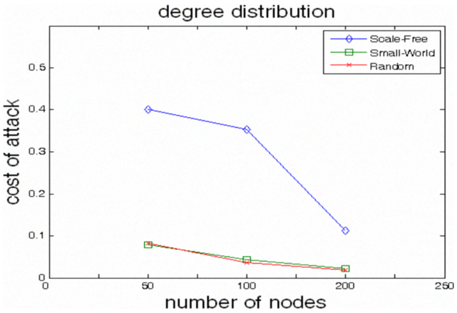

Figure 5. UAS vs. degree distribution cost graph

For degree distribution strategy, attacker pays a higher cost in the scale-free network. This is due to high degree nodes in the scale-free network. These nodes have high probability to be attacked, to increasing the attack cost; the protection strategy must allocate sufficient resources in the high degree nodes. The costs of attack are rather low for both small-world and random network models if degree distribution defending strategy is used.

5.1.3. UAS vs. clustering coefficient distribution

The following three figures, Figure 6, 7 and 8, show the clustering coefficient distribution of the three network models with one hundred nodes.

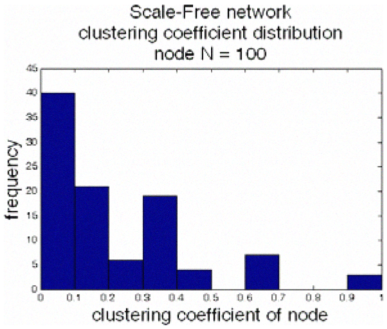

Figure 6. clustering coefficient distribution in scale-free network, average clustering coefficient is 0.2213

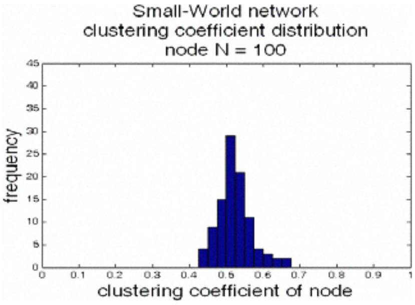

Figure 7. clustering coefficient distribution in small-world network, average clustering coefficient is 0.5229

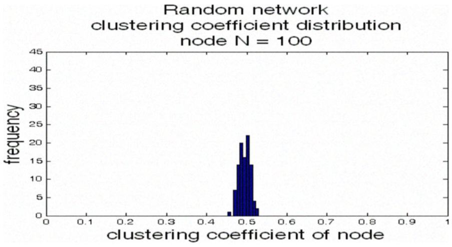

Figure 8. clustering coefficient distribution in random network, average clustering coefficient is 0.4941

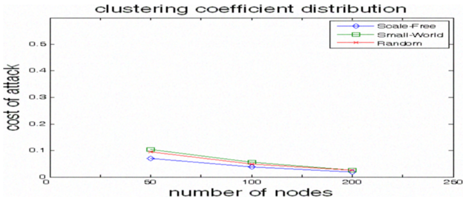

Figure 9. UAS vs. clustering coefficient distribution cost graph

Figure 9 illustrates the costs of attack for three network models. All three network models exhibit rather low value of attack costs. Even though scale-free and small-world network models have rather different average clustering coefficient, the overall effectiveness in distributing protection resources according to clustering coefficients is rather low for all three network models.

5.1.4. UAS vs. betweenness distribution

The following three figures, Figure 10, 11, and 12, are the betweenness distribution of three networks with one hundred nodes.

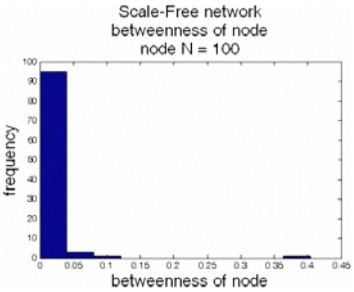

Figure 10. betweenness distribution in scale-free network

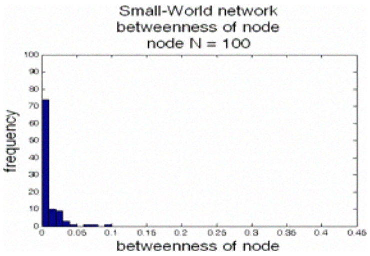

Figure 11. betweenness distribution in small-world network

From Figure 10, 11 and 12, these three betweenness distributions for three network modes are similar. The relationship between betweenness distribution and network structure are not significant.

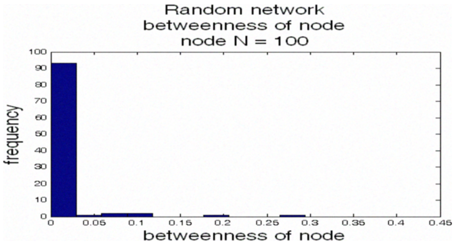

Figure 12. betweenness distribution in random network

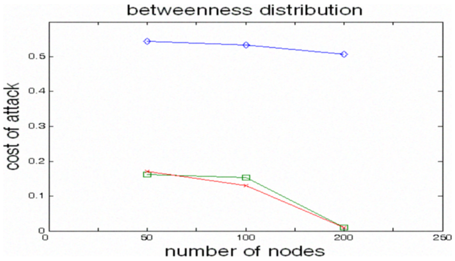

Figure 13. UAS vs. betweenness distribution cost graph

Despite the similarity in betweenness distribution for all three network models, the cost of attack for scale-free network is much higher than small-world network and random network.

5.2. NAS vs. protection strategies

In this subsection, the costs of non-uniform attack strategy with different resource allocation strategies are studied. Results are summarized in Figure 14.

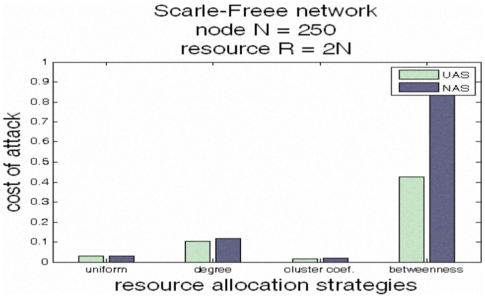

Figure 14. NAS vs. resources allocation strategies cost graph

From Figure 14 we know that the costs of attack are the highest by applying betweenness distribution defending strategy among all resource allocation strategies.

5.3. Results

From those simulation results we know that the cost of attack is rather low for random network model using all four defending strategies. This is because random network contains no apparent network structure. For scale-free network, the degree and betweenness defending strategies can effectively increase the attack cost, while adopting clustering coefficient as a defending resource allocation guide is not a good way to raise attack cost.

6. Conclusion

One result from this study is that uniform attack strategy is not an effective way for any network models. And to defend a real-world network, protection strategies based on network characteristics can offer good protections against random and non-uniform attacks. Furthermore, if the real-world network exhibits scale-free characteristics, defending strategies by allocating resources according to the degree and betweenness distribution is an effective way to increase the attack costs.

References

[1] R. J. Ellison, D. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, and N. R. Mead, "Survivable Network Systems: An Emerging Discipline," Technical Report, Carnegie Mellon University, 1997.

[2] V. R. Westmark, "A Definition for Information System Survivability," *Proceedings of the 37th IEEE Hawaii International Conference on System Sciences (HICSS'04)*, pp. 1-10, 2004.

[3] Y. S. Lin, P. H. Tsang, C. H. Chen, C. L. Tseng, Y. L. Lin, "Evaluation of Network Robustness for Given Defense Resource Allocation Strategies," *The 1st International Conference on Availability, Reliability and Security (ARES'06)*, pp. 182-189, 2006.

[4] Y. S. Lin, P. H. Tsang, Y. L. Lin, "Near Optimal Protection Strategies against Targeted Attacks on the Core Node of a Network," *The 2nd International Conference on Availability, Reliability and Security (ARES'07)*, pp. 213-222, 2007.

[5] P. Erdős and A. Rényi, "On Random Graphs," Publ. Math. Debrecen 6, pp. 290–297, 1960.

[6] R. Albert, A. L. Barabási, "Statistical Mechanics of Complex Networks," Reviews of Modern Physics, Volume 74, Issue 1, pp. 47-97, 2002.

[7] D. J. Watts, "Small Worlds: The Dynamics of Networks between Order and Randomness," *Princeton University Press*, 1999.