On the Simulation of the Network Topology Generator and Robustness of the Constructed Network

Li Baoqiang, Tian Shurong, Si Shoukui and Ma Cuiling

***Abstract*—Being motivated by recent rapid developments in the theory of complex networks, we constructed one kind network topology generator and studied the network's robustness, with the use of Matlab and Pajek software. In this thesis, we describe an updated Autonomous System (AS)-level network topology generator. We show that generates topologies with characteristics more faithful to network topologies of comparable sizes. This thesis has three parts. The first is the introduction of complex networks, which make it better to accurately simulate network and study the network topology. The second, we present a topology generator that is based on AS connectivity in the network through programming by Matlab and show that it generates topologies that best approximate the actual AS network topology. The third is the investigating of the network's robustness under random attacks that remove part of nodes in the network completly, we also examine the robustness of networks under intentional attack.**

I. INTRODUCTION

In recent years research in large-scale networks has seen a rapid development in various disciplines, inspired by the discovery of two features shared by many real-world networks: small-world and scale-free. Large, complex networks are conspicuous in science and everyday life and have attracted a great deal of interest [1–3].The development of complex networks makes simulation more similar to the real-network, which can be used to investigating topology properties of the real-network.

Intranet is a typical complex network, for the purposes of different forecasts and improvements of Intranet performance, it is very important to establish an appropriate model of intranet topology. An Autonomous System (AS) is a network under a single administrative authority. ASs connect to each other through border routers, so the Intranet can be considered as consisting of interconnected ASs. Within each AS, the network could be further divided into sub-networks connected by internal routers. Hence, the Intranet can either be modeled as a graph where each node represents a router, or as a graph where each node represents an AS. In recent years, there is a network topology model, which also known as Internet topology generator, proposed for the structure of AS-level Internet topology. Topology generator on the Internet since the research in general can be divided into three generations in chronological order: The first is the random map generator in 80th years on behalf of the 20th century, one of the most commonly used models for generating Internet networks algorithmically is due to Waxman; The second is the structure generators took the 90th years of the 20th century, Tiers and Transit-stub is two obvious hierarchy designs based on the topology generator; Since 2000, the third generation generators based on network node degree got out, for BRITE example.

With the rapid development of the Intranet network, there has much interest in the resilience of Intranet network to random attacks or to intentional attacks on the highest degree nodes. Many real-world networks are scale-free and robust to random attacks but vulnerable to intentional attacks. It is important for us to know the optimal scale free network guideline to improve networks which are optimally robust against both types of attacks. Although many papers have designed the optimal network topology, such as the two-peak and three-peak optimal complex network, but we can not convert its topology to the theoretical optimization directly disobeying its evolutionary principle. On the contrary, we should study the optimal Intranet network guideline to improve the existed Intranet network robustness.

Ⅱ. THE CONSROCTION OF THE NETWORK MODEL

In order to reflect the Intranet's topological properties, we rise up this generate mainly based on two ways to add new nodes.

A. *Data sets*

Networks can be viewed as a collection of routing domains. Each routing domains is a group of nodes(routers, switches and hosts). Each routing domain in the network can be classified as either a stub domain or a transit domain. A stub domain carries only traffic that originates or terminates in the domain. Transit domains do not have this restriction. The purpose of transit domains is to interconnect stub domains efficiently; Without them, every pair of stub domains would need to be directly connected to each other. Stub domains generally correspond to campus networks or other collections of interconnected LANs, while transit domains are almost always wide networks. A transit domain consist of a set of backbone.

ASs connect to each other through border routers, so the network can be considered as consisting of interconnected ASs. AS connectivity is characterized in by the eigenvalues of the network's connectivity matrix. The connectivity matrix of a graph is a square matrix $A=(a_{ij})$, where $a_{ij}=1$ if nodes i is connected to node j, 0 otherwise. A node is not considered connected to itself. As an example, we can represent the edges for the graph in Fig.1 using the following adjacency matrix in Fig.2.

Li Baoqiang is a student in the second students' brigade of Naval Aeronautical and Astronautical University(e-mail: libaoqiang1989@126.com).

Tian Shurong, Si Shoukui and Ma Cuiling are with the Department of Basic Sciences of Naval Aeronautical and Astronautical University.

978-1-4577-0816-9/11/$26.00 ©2011 IEEE

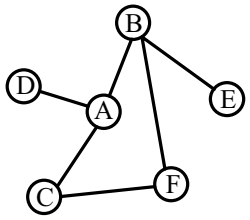

Fig.1. an example graph figure

	A	B	C	D	E	F
A	0	1	1	1	0	0
B	1	0	0	0	1	1
C	1	0	0	0	0	1
D	1	0	0	0	0	0
E	0	1	0	0	0	0
F	0	1	1	0	0	0

Fig.2. adjacency matrix which can describe the connectivity of graph in Fig.1

▪ B. *The model to construct the network*

Setting the original m_0 nodes by random, connect these nodes and use the next steps to add new nodes:

(*i*)Add one node with the propability p, by the way of degree-first attachment, and connect node i of exacted m_0 nodes with the propability

$$\Pi_{ab}(k_i)=(k_i+1)/\sum_j(k_j+1),$$

here k_i is the connectivity of node i.

(*ii*)Add one node with the probability $1-p$, by the way of distance-first attachment, and make the new node to connect the nearest exacted nodes by m_1 edges.

Repeate the above algorithm until we have added all the new points.

While simulating, we set $m=m_0=100$, $p=0.5$. Through simulating, we can get adjacency matrix A, and then draw Fig.3. The visualization of the simulated network diagram by Pajek software is Fig. 4.

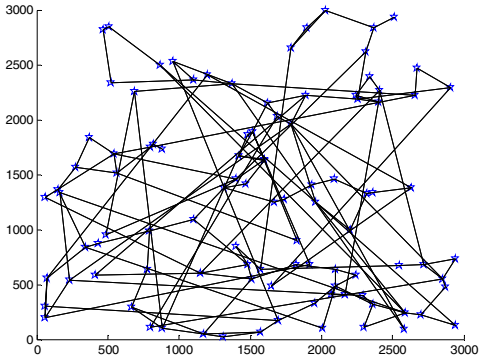

Fig.3. the Simulated Network

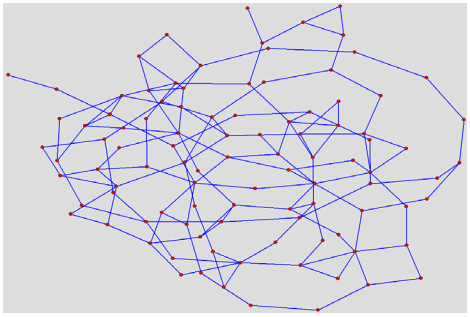
Fig.4. The visualization of the simulated network

▪ III. THE ROBUSTNESS OF THE NETWORK

Many complex networks display a surprising degree of tolerance against errors. For example, relatively simple organisms grow, persist and reproduce despite drastic pharmaceutical or environmental interventions, an error tolerance attributed to the robustness of the underlying metabolic network. Complex communication networks display a surprising degree of robustness: a small mistake may lead to the loss of the global information-carrying ability of the network. The stability of the network is often depended on the cut edge.

The cut edge is an edge in the graph without which the connected graph would separate into disconnected subgraphs. The two endpoints of the cut edge is called cut point: cut point is a vertex, if you delete it, at least two separate plans will be split into sub-plans. Therefore, to find the cut edge of the network and add new edge between the cut points can effectively improve the robustness of the network and increase network stability. Here we use breadth-first search (BFS) algorithm to find the cut edge of the simulated network.

▪ A. *How BFS works*

BFS is an uninformed search method that aims to expand and examine all nodes of a graph or combination of sequences by systematically searching through every solution. In other words, it exhaustively searches the entire graph or sequence without considering the goal until it finds it. It does not use a heuristic algorithm.

From the standpoint of the algorithm, all child nodes obtained by expanding a node are added to a FIFO (i.e., First In, First Out) queue. In typical implementations, nodes that have not yet been examined for their neighbors are placed in some container (such as a queue or linked list) called "open" and then once examined are placed in the container "closed".

▪ B. *Algorithm*

(*i*)Enqueue the root node, here it is the original node;

(*ii*)Dequeue a node and examine it. If the element sought is found in this node, quit the search and return a result. Otherwise enqueue any successors (the direct child nodes) that have not yet been discovered.

(*iii*)If the queue is empty, every node on the graph has been examined – quit the search and return "not found".

(*iv*)If the queue is not empty, repeat from Step 2.

Note: Using a stack instead of a queue would turn this algorithm into a depth-first search.

Using this algorithm and programming with Matlab, then we can get the cut edge and cut point of the simulated network.

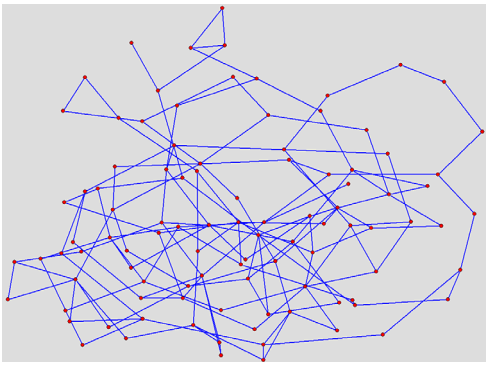

Fig.5. The reinforced network

Add new edge between cut nodes to improve the stability of the network using the following method. First, find out all cut nodes of the simulated network. Then, as the points with large degree are more stable than points with small degree, add edges between the points with smaller degree and other points in the graph. The reinforced network is as figure 5.

- C. *Random attacks and intentional attack*

Recently, there has much interest in the resilience of network to random attacks or to intentional attacks on the highest degree nodes. Studies shows it is only one case in which there was only one type of attack in a given network, that is, the network was subject to either a random attack or a targeted attack but not subject to different types of attack simultaneously. A more realistic model is the one in which a network is subjected to simultaneous targeted and random attacks. We focus on the network state after intentional and random attacks which remove fractions p^{target} and p^{rand} of the original nodes, respectively.

In the scale-free networks, the degree distribution $P(k)$ is the probability of a node with k connections to other nodes, typically decreases as a power of k. Thus with a fraction p^{random} of the nodes and their connections of the scale-free network are removed randomly, the random chosen node would have a low degree, so its removal has little effect on the network. Removal of a highly connected node could produce a large effect. We set $p^{\text{random}}=10\%$ and get Fig.6.

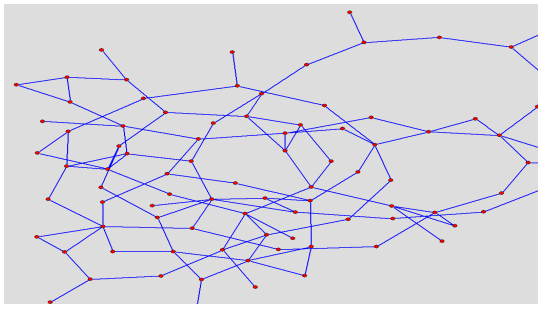

Fig. 6. $p^{\text{random}}=10\%$ of the nodes and their connections are randomly removed

If we attack the scale-free network intentionally: the removal of sites is not random, but rather sites with the highest connectivity are targeted first. The intented chosen node all have a high degree, so its removal has great effect on the network. Take out p^{target} of a decreasing order of their nodal degrees. We set $p^{\text{target}}=10\%$ and get Fig.7.

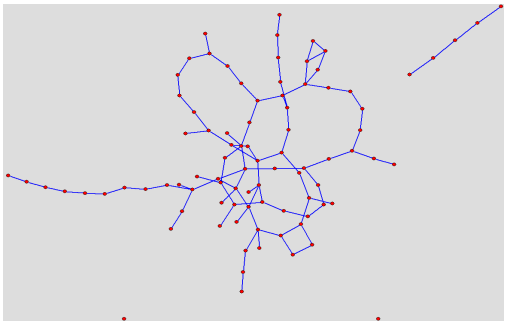

Fig.7. $p^{\text{target}}=10\%$ of a decreasing order of nodal degree

- Ⅳ. CONCLUSION

In recent years, researchers in many different areas in networking have recognized the need for a simulation that produce realistic Intranet network. In order to produce intranet network approaching to realistic network, we need a better understanding of the Intranet topology itself. In this thesis, we present a intranet topology generator that not only generates topologies with Intranet-like characteristics, but is also parsimonious in the number of parameters required. We find robustness of the Intranet network is largely depended on the cut edge of network. Then, we use BFS to find out the cut edge of network to increase the network stability through adding new edges between cut point and other point in the network. In the end, we do some test on random attacks or to intentional attacks to network and find out that random attacks have little effect on the network, while intentional attacks can largely decrease the stability of network.

REFERENCES

[1]Cheng Jin, Qian Chen, Sugih Jamin."Inet: Internet Topology Generator" .

[2]K. Calvert, M.B. Doar, and E.W. Zegura. "Modeling Internet Topology". IEEE Communications Magazine, June 1997.

[3]J. M. Carlson, John Doyle."Complexity and robustness". 2538–2545, PNAS, February 19, 2002, vol. 99, suppl.

[4] Jaime Silvela, Javier Portillo. “Breadth-First Search and Its Application to Image Processing Problems” IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 10, NO. 8, AUGUST 2001.
[5]Réka Albert, Hawoong Jeong, Albert-László Barabási. “Error and attack tolerance of complex networks” NATURE ,VOL 406 , 27 JULY 2000 .