International Journal of Future Generation Communication and Networking
Vol.7, No.1 (2014), pp.19-28
http://dx.doi.org/10.14257/ijfgcn.2014.7.1.02

Robustness Analyses of Internet Topology with Power-law Features

XU Ye and MA Wen-xuan

School of information science and engineering, Shenyang Ligong University, Shen yang 100159, China
xuy.mail@163.com mawenxuan1013@163.com

Abstract

For a better predicting and a trying to improve the performance of Internet, we try to study the characteristics of the Internet topology in the autonomous system. Firstly, we put focus on power-law characteristics of Internet topology and give power-law distribution comparison experiments between Internet topology and that of the small-world network. Experiments show clearly that the topology of the Internet has power-law distribution. Secondly, we focus on study the robustness of Internet topology, and experiments show that Internet is robust to random failures and fragile to target attacks. However, a reasonable allocation of network redundancy and network load can make a network strong and low-cost with abilities to be robust under target attacks.

Keywords: *autonomous system; Internet topology; power-law distribution; robustness*

1. Introduction

As technology continues to progress, Internet has become the social routine work and a n indispensable part of life in today. Internet is rapidly developing its network size, while t he topology is also changing. To extract a network structure can help identify the main fea tures of a ultra-large-scale complex topologies, which is an important prerequisite not onl y to the effective usage of Internet, but the guidance of further network construction [1].

Since Faloutsos [2] found that the Internet Autonomous System(AS) level topology nodes showing power-law degree distribution, people have a new understanding of Internet systems. Internet topology study is to explore new topics. In a random network, the node degree distribution approximately applies Poisson distribution, almost all nodes are clustered around the average node degree, and very few nodes with high degrees can be ignored [3]. Meanwhile, the power-law networks have different characteristics from random networks. For example, the existence of a high degree nodes greatly weakened the network robustness. A malicious attacker only need to attack the network nodes with highest degree could make the network paralyzed quickly [4]. "Robust yet fragile" is the most important and basic features of complex system. It is important to understand thoroughly the characteristics and regularity of the complex giant system – Internet, would be helping for development of Internet topology modeling and network technology control.

In recent years, by the Internet AS level topology structure of network topology model is called the Internet topology generator. Internet Topology Builder chronologically divided into three generations until now: the first generation for a random graph generator in the 1980, such as Waxman [5] generator; the second generation is the structure generator in the 1990 s such as Tiers [6] and Transit-stub [7]; the third generation generator is based on network node degree since 2000 such as BRITE [8] and Inet [9]. Experiments found that these Internet models only simulates Internet is a small part of features. Founding on this, we perform our experiments on a whole set of measured Internet topology [18].

ISSN: 2233-7857 IJFGCN

The research on Internet AS level topology results shows that [10-12]: in addition to po wer-law distribution, Internet topology also has many other features of complex networks such as the small-world effect, hierarchy and the rich man's club phenomena. We put focu s on the analysis of complex network characteristics of Internet AS level topology firstly i n this paper.

We try to give mathematical descriptions of the power-law distribution and its correspo nding scale conditions, by comparison studies with that of the small world networks and tr y to use the measured Internet topology data to verify the analysis to the power law behav ior. Secondly, we put focus on the robustness studies of Internet under random attacks and attempted attacks, trying to prove that it has the characteristic of the "Robust yet fragile".

2. The Topological properties of the Internet

2.1. Power-law Distribution

Power-law distribution [13] is also called scale-free distribution. A network with power law degree distribution is also known as scale-free networks. Power-law distribution is:

$$y = cx^{-r} \tag{1}$$

where *x*, *y* are positive random variables, *c*, *r* are constants greater than zero. After loga rithm computations on both sides we can get:

$$\ln y = \ln c - r \ln x \tag{2}$$

It's easy to know *lny* and *lnx* satisfy linear relations, which means that the power-law distribution is a straight line in the double logarithmic coordinates, and the slope of this line is the negative of the power-law exponent. The linear relationship is used to determine whether a given random variables satisfy the basis of a power law or not.

There are several new forms of power-law distribution mostly used in analysis of comp lex networks:

1) frequency-degree power-law distribution

It's shown as:

$$p_v \propto d_v^R \tag{3}$$

where p_v is the frequency of a node *v*; d_v^R is the node value of *v*.

2) degree-rank power-law distribution

It's shown as:

$$d_v \propto r_v^R \tag{4}$$

where d_v is the node value of *v*; r_v^R is sort of node *v*, which means the node degree is descendingly sorted (ranked).

3) eigenvalue-rank power-law distribution

It's shown as:

$$\lambda_i \propto i \tag{5}$$

where λ_i is eigenvalue of the topology matrix; *i* is the label sequence of the corresponding eigenvalue in descending order.

4) CCDF(d)-degree power-law distribution

It's shown as:

$$D_d \propto d^D \tag{6}$$

where D_d is the degree complementary cumulative distribution function refers to the cu

mulative value of node degree more than d; D_d is the degree.

2.2. Small World Properties

In a network, the distance between two nodes i and j d_{ij} is defined as the number of edges connecting the two nodes in the shortest path. The maximum distance between any two nodes in a network is called the network diameter [14], recorded as $D, D = \max_{i,j} d_{ij}$.

Average path length l of a network is defined as the average of the distances between any two nodes:

$$L = \frac{1}{\frac{1}{2}N(N+1)} \sum_{i \geq j} d_{ij} \tag{7}$$

where N is the number of nodes in the network. The average path length of the network is also known as the characteristic path length.

AS level Internet presents "Small-World" feature [15, 16]. Compared with the same size of random graph, Internet has a shorter path length and larger clustering coefficient.

2.3. Hierarchy Structure

Internet can be considered as a interconnected system composed of a large number of AS systems, in which each AS system can be viewed as Stub domain or Transit domain. Stub domain hosts only those originated or terminated traffics within the domain, but the transit domain does not have this limitation. The Transit domain is designed to effectively connected Stub domains. A Stub domain is usually used in the campus network or other interconnected LANs. Transit domain is commonly used in WANs or MANs. It is viewed as a service provider and a typical regional or national level ISP or backbone network [17].

2.4. Rich-club Phenomenon

A few nodes in the Internet have many edges and they are also called "Rich Nodes". Ri ch nodes tend to connect with each other to constitute a "Rich-Club" [18].

We can use the rich-club connectivity Φ (R/N) to describe this phenomenon, it represen ts the edges E of the top r nodes with highest degree over the all possible edges of these r nodes, as is:

$$\phi(r/N) = \frac{E}{r(r-1)/2} = \frac{2E}{r(r-1)} \tag{8}$$

If φ (r/N) = 1, then the top r rich node composes of a rich clubs that is a fully connected subgraph.

3. The Internet Topology Analysis of the Power-law

Degree - rank power law and the CCDF (d) - degree power law of measured Internet ar e studied in this paper.

3.1. Degree-rank Power-law Distribution

In order to review the power-law distribution of the Internet, we make power law distri bution comparative experiments on a measured Internet topology with 500 nodes and a ge

nerated small world network (degree value is 4) with 500 nodes. The results of degree-ran k power-law distribution is shown below, in which the x-axis is descending rank, the y-axi s is the power exponent.

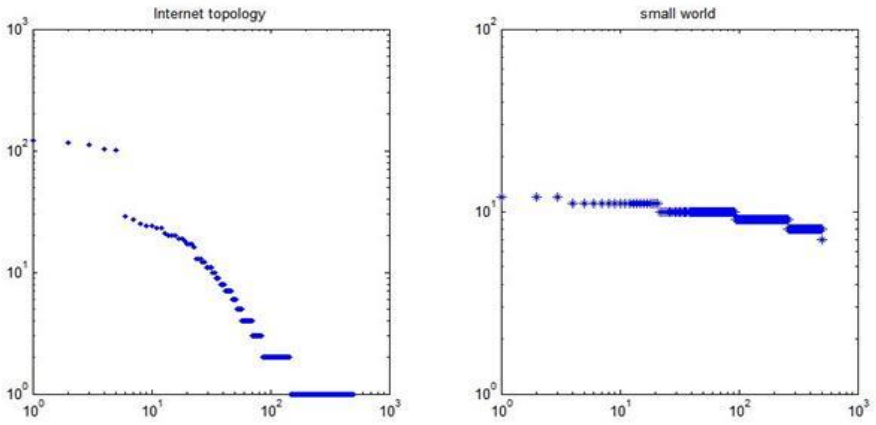

Figure 1. Degree-rank Power-law Distribution Comparison of Two Networks

It can be seen from the figure that the distribution of Internet topology shows clear linear type, and corresponding linear mathematical model can be fitted to determine its power law exponent (the gradient). For the small-world network result, we can see the power-law does not show linear type. The degree-rank power law is like a line parallel to the horizontal axis (the gradient nearly equals to 0) which means there is no power-law distribution.

The Internet topology graph, however, is not so much satisfactory since it's not a straight line. The reason may lies in that the size of the measured Internet is relatively small.

3.2. CCDF(d)-degree Power-law Distribution

In order to investigate the Internet CCDF (d)-degree power-law distribution, we make CCDF(d)-degree power-law distribution experiments to compare the measured 500-node I nternettopology and a same size small-world networks (degree 4) of. Results are as follow s, where the x-axis is the cumulative distribution function of compensation degree, the y-a xis is the value:

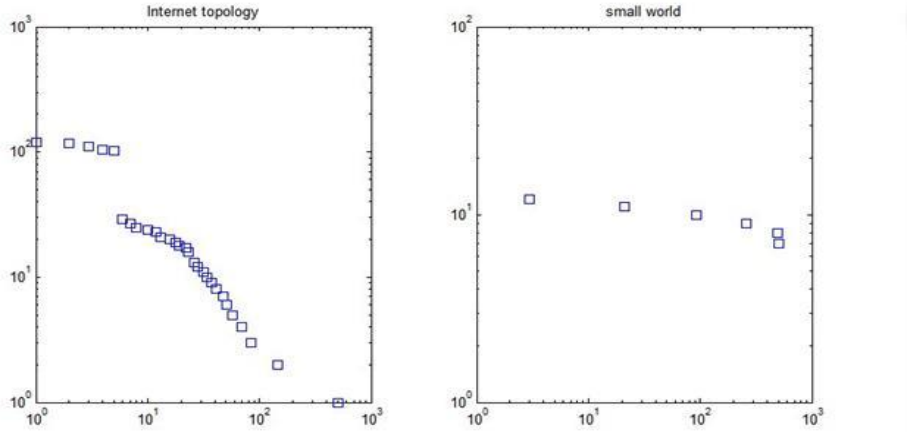

Figure 2. CCDF(d)-degree Power-law Distribution Comparison of Two Networks

Similar to the Figure 1, the main part of the Internet topology result can be seen to have a linear distribution.While in the small-world network result, the power-law distribution is a few points representing horizontal status so that a conclusion could be made that there is no power-law distribution in it.

Through the upper two experiments, we could find that there is a power law distributio n feature in Internet topology. Furthermore, in a part of Internet topology with the maximu m and minimum degree, the power law distribution is not so much clear than the other par ts. When the Internet nodes is small, the power-law distribution is not obvious, but still sh ows power-law distribution tendency.

4. Robustness Analysis of Internet Topology

4.1. Robustness

After the small world effect and scale-free properties discovered and studied in complex networks, studies of a property of robustness are getting more and more attentions. Robustness is used to represent the ability to maintain its functions or properties when the system is disturbed especially from outside interference or damage. In complex networks it reflects the ability of a network structure to resist the destructions.

The robustness of the Internet can be expressed through the network behavior under the attacks. Attacks are divided into two broad categories: one is complete random attack, that is to randomly remove a few of the nodes in the networks; the other is target attacks, that is to attack peticular nodes in the networks, especially those nodes with highest degree. Compared with random attacks, target attacks could destroy high-degree-nodes in networks and usually result in greater harms. Most of the scale-free network has good robustness against random attacks, but for target attacks, especially for high-degree-node attacks, they show fragility.

We start several robustness experiments on the measured Internet AS backbone topology against random attack and target attack respectively. Some of the parameters in simulation experiments are：

τ is scale for the attack, its value lies in interval [0,1], when τ=1 it means a complete random attack, and when τ=0 it is called complete target attack;

ω is network load, its value lies in range [0,1], when ω=1 it indicates that the network is under full load, when ω=0 it means that the network is zero loaded;

θ is network redundancy, its value lies in range [0,1], and the higher θ is, the more redu ndancy the network is, whearas the costs of network construction and maintenance increas e at the same time.

In this paper, we set G to evaluate the degree of network collapse:

$$G = \frac{N'}{N} \tag{9}$$

where, N is the number of nodes in the network simulation experiments, N' is the number of nodes of the maximum connected subgraph after the end of cascading failure in the network, G is the largest connected subgraph relative value.

4.2. Analysis of Experimental Results

4.2.1. Network Load Effect on the Robustness of the Internet: In order to study the effect of network load over the robustness of the Internet, an experiment on a 500-node Internet topology under random attacks and target attack are performed respectively.

We set τ=1 (random attack), ω=[0 0. 2 0. 4 . . . 1], θ=0 (network redundancy is zero). Experiments results are shown in Figure 3.

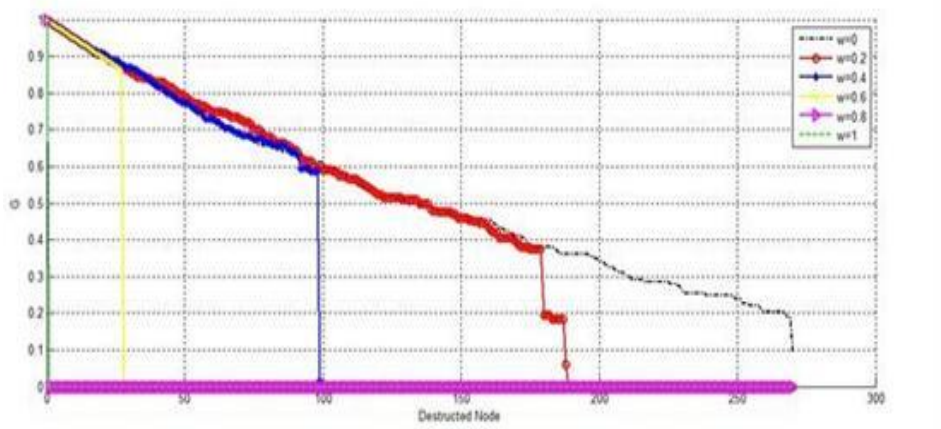

Figure 3. Random Attack on the Internet when the Network Load Changes

From the graph we can see that:

When network load ω=0.2, random attacks damage around 65% of the all nodes in the networks and the network collapse degree G reached 50%. When the percent of the dama ged nodes reaches 85%, the network was completely collapsed where the collapse degree G reached under 10%.

When network load ω=0.6, random attacks damage around 17% of the total number of nodes in the network and the network collapse degree G reached 50%. When 20% of node s are destructed, the network began to collapse completely with G reaches under 10%.

When the network load ω=0.8, random attacks damage about 4% of the total nodes in the network. The network begin to collapse completely from a quite security condition with G much greater than 0.5.

When the network load ω=1.0, the network began to collapse completely when only up to 0.1% of the nodes are attacked and damaged. The collapse is quite soon.

From the analyses we find that Internet AS backbone network shows a good robustness against random attacks. But the network is getting quite fragile when the network load is higher. Only a small increase of attacks on nodes might result in a fully collapse of the wh ole network.

Then we start experiments in target attacks and set τ=0 (target attacks), ω=[0 0. 2 0. 4 . . . 1], θ=0 (network redundancy is zero). Results are shown in Figure4.

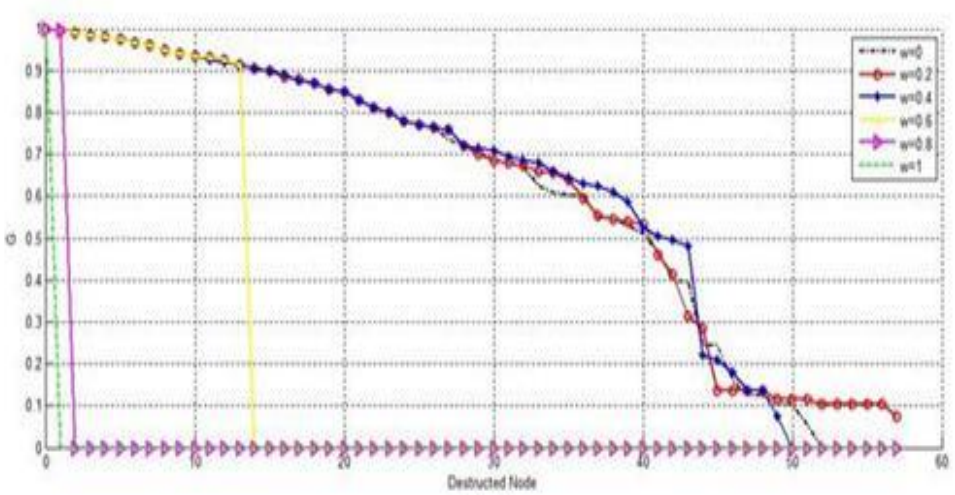

Figure 4. Target Attack on the Internet when the Network Load Changes

When set network load ω=0.2, target attacks damage only about 20% of the total numb er of nodes when the network collapse degree reached 50%. If the number of nodes reache s up to 25%, the network was completely collapsed with the collapse degree *G* getting les s than 10%.

When set network load ω=0.6, target attacks damage about 7% of all nodes when the n etwork collapse degree reaches 50%. If 8% nodes destructed, the network began to compl etely collapse with *G* getting down to 10%.

When set the network load ω=0.8, target attacks damage only 4% of the total number o f nodes when the networks begin to collapse completely.

When set the network load ω=1.0, only attack 0.05% of overall nodes, the network began to collapse completely with *G* getting very quickly down to around 0.

So, the Internet backbone network is pretty fragile to target attacks. At the same time, t he fragility level of the network doubles when the network load is getting higher. This is q uite consistent to our common-sense understanding of the network.

4.2.2. Network Redundancy Effect on the Robustness of the Internet: In order to study the effect of network redundancy over Internet robustness, experiments on 500-node Internet topology structure are performed under random attacks and target attacks respectively.

When set τ =1 (random attacks), θ=[0 0. 2 0. 4 . . . 1], ω=0. 5(set the network to be 50% workload). Results are shown in Figure 5.

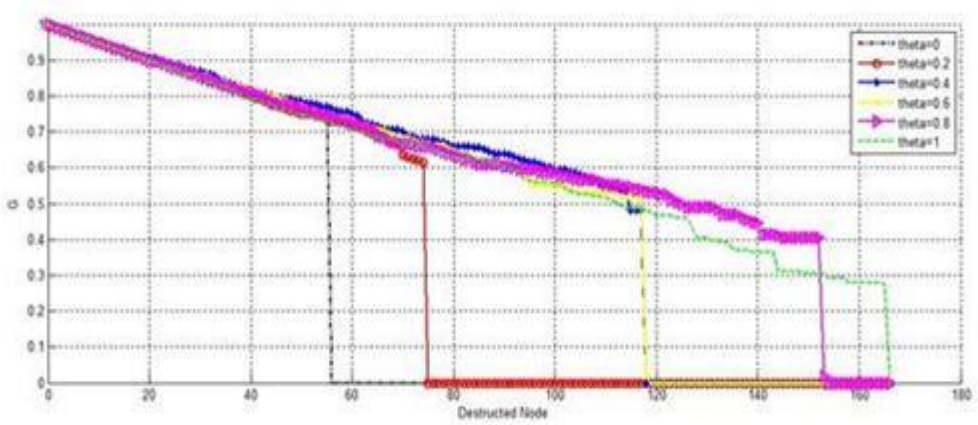

Figure 5. Random Attack on the Internet when the Network Redundancy Changes

From the figure we can see that, when we set network load θ=0.2, random attacks damage 37. 5% of nodes and the network collapse degree *G* reaches down to 50%. When the number of damaged nodes was up to 40%, the network was completely collapsed with the collapse degree G reached down to 10%.

When set network load θ=0.6, random attacks damage around 55% of the total number of nodes and the network collapse degree reached down to 50%. When the destruction node gets up to 58%, the network begin to collapse completely with G reached down to 10% very quickly.

When set the network load θ=0.8, random attack damage 60% of the networks nodes and the network collapse degree reached down to 50%. When the destruction nodes get up to 77. 5%, the network begin to collapse completely.

From the upper analyses, we find that Internet backbone network shows good robustness to random attacks. But when the network load is getting higher, only small increase of node attacks would result in a quick collapse in the network.

From the figure we find that when we set network load *w* a fixed number, a increas of

network redundancy θ would make cascading failure propagation restricted in a certain extent and the network robustness will be greatly improved.

Then we start experiments in target attacks, we set τ =0 (target attack), θ=[0 0. 2 0. 4 . . . 1], ω=0.5(set network to be 50% workload). Results are shown in Figure 6.

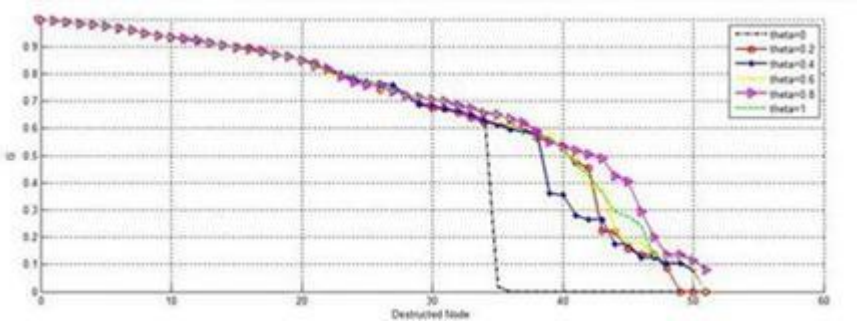

Figure 6. Target Attack on the Internet when the Network Redundancy Changes

From the figure we can see that when set network redundancy θ=0.2, target attacks damage about 20% of the total number of nodes and the network collapse degree reached down to 50%. When the number of damaged nodes reaches 23%, the network is getting completely collapsed with the collapse degree *G* reached down to 10%.

When set network load θ=0.6, target attacks damage 21% of the total number of nodes and the network collapse degree reached down to 50%. When the destructed nodes get up to 25%, the network begin to be completely collapsed with *G* reaches down to 10%.

When set the network load θ=0.8, target attacks damage around 21% of the total numbe r of nodes and the network collapse degree reached down to 50%. When the destruction g et to be 77. 5%, the network began to be completely collapsed.

Under target attacks, a increase of network redundancy can enhance network robustness largely. When the network gets into a fully connected network, network robustness would reach its best performances. However, the overall cost of network construction and maintenance would be greatly increased.

On the contrary, network load has important negative effects on network robustness compared with redundancy. The robustness of a network can also be affected by significantly when the network is overloaded.

From the experiments we could draw conclusions that a reasonable allocation of network redundancy and network load can make a network strong and low-cost with abilities to be robust under target attacks.

5. Concluding Remarks

A correct understanding of Internet topology is not only a basis for network modeling, but also the premise of fully understanding of the complex properties of Internet.

We firstly discusses the main features of complex networks, including the power-law distribution, free-scale features, small-world effect, hierarchy structure, rich club phenomenon. And then we give analyses features of the Internet AS topology resulting in conclusions that the Internet AS level topology complies with power law distribution. Finally, researches and analyses are done on robustness of Internet topology, and we find that Internet has good robustness against random attacks but fragilities against target attacks. However, a reasonable allocation of network redundancy and network load can make a network strong and low-cost with abilities to be robust under target attacks.

References

[1] R. Dai and L. Cao, "Internet an open complex giant systems", Science in China, vol. 33, no. 4, **(2003)**, pp. 289-296.
[2] M. Faloutsos and P. Faloutsos, "On power-law relationship of the Internet topology", ACM SIGCOMM Computer Communication Review, vol. 29, no. 4, **(1999)**, pp. 251-262.
[3] Y. Zhang, H. Zhang and B. Fang, "Summary of Internet topology modeling", Journal of Software, vol. 15, no. 8, **(2004)**, pp. 1220-1226.
[4] G. Zhang and G. Zhang, "Association study of Internet network", Journal of Software, vol. 17, no. 3, **(2006)**, pp. 490-497.
[5] B.-M. Waxman, "Routing of multipoint connections", IEEE Journal of Selected Areas in Communication, vol. 6, no. 9, **(1988)**, pp. 1617-1622.
[6] K. Calvert, M. Doar and E. Zegura, "Modeling Internet topology", IEEE Communication *Magazine*, vol. 35, no. 6, **(1997)**, pp. 160-163.
[7] M. P. Mahadevan, D. V. Krioukov and M. Fomenkov, "The Internet AS-level topology: Three data sources and one definitive metric", Computer Communication Review, vol. 36, no. 1, **(2006)**, pp. 17-26.
[8] Y. Zhang, H. Zhang and B. Fang, "China AS level topology measurement and analysis", Journal of computer, vol. 31, no. 4, **(2008)**, pp. 611- 619.
[9] X. Zhang, H. Zhao and L. Wang, "AS-level Internet topology analysis", Journal of communication, vol. 7, **(2008)**, pp. 50-61.
[10] Y. Xu, "Internet topology modeling based on large-area model", Publishing House of electronics industry, Beijing, **(2011)**.
[11] X. Wang, X. Li and G. Chen, "Complex Network Theory and Its Application", Tsinghua University press, Beijing, **(2006)**.
[12] S. Zhou and R. J. Mondragon, "Redundancy and robustness of the AS-level Internet topology and its models", Electron. Lett., vol. 40, **(2004)**, pp. 151-152.
[13] S. Jin and D. Bestavros, "A. Small-world Internet topologies: possible causes and implications on scalability of end-system multicast", Technical report, BUCS-TR-2002-004, **(2002)**.
[14] M. Doar, "A better model for generating test networks", Proceedings of IEEE Global Internet, London, **(1996)**, pp. 86-93.
[15] A. Medina, A. Lakhina, I. Matta and J. Byers, "BRITE: an approach to universal topology generation", Proceedings of MASCOTS, Washington, **(2001)**, pp. 346-353.
[16] J. Winick and S. Jamin, "Inet-3. 0: Internet topology generator", Technical report CSETR-456-02, Department of EECS, University of Michigan, **(2002)**.
[17] T. Bu and D. Towsley, "On distinguishing between Internet power law topology generators", Proceeding of INFOCOM, New York, vol. 2, **(2002)**, pp. 638-647.
[18] Skitter, CAIDA. http://www.caida.org/tools/measurement/skitter/.

Author

Ye Xu, received his Ph.D degree in Computer Application Technology from Northeastern University (China), 2006. Now working in Shenyang Ligong University (China), as an associate professor, a Master instructor and a Deputy Chief in Discipline Construction Department. His recent research interests include large-scale networks and complex systems, information fusion and wireless sensor networks.

