Study on Evaluation Method for Network Survivability Under Intentional Nodes Attack

Jianjun Shen and Kai Li

ABSTRACT

Network survivability is an important factor to consider in network design and analysis, but evaluation of network survivability at present mainly adopts static methods, which has certain limitations. For this purpose, the article put forward an evaluation method for network survivability under dynamic condition. That is, assuming the network nodes are intentionally attacked, we evaluate its survivability by the increase of the average hops of the network. If the increase of the average hops of a network is smaller after it suffers from intentional nodes attack, then the survivability of the network is stronger. Compared with static evaluation methods, the method proposed in the paper has more practical significance. Experimental results show that the method of paper is correct.

KEYWORD: Survivability; Evaluation; Intentional Attack; Average Hops

INTRODUCTION

In recent years, as the continuous growth of Internet, World-Wide-Web, military command and control network and communication network, their scales become larger and larger, structures become more complicated, and survivability of network has become an important factor which must be considered in network design and analysis. Especially under informationization condition, as network’s role becomes stronger and stronger, it has been an important combat pattern [1] that combat sides selectively attack the core nodes or key nodes in the other side’s network, thus reach the goal to paralyze the other side’s network. For this purpose, it is a very meaningful topic to evaluate network survivability, and then design a network with higher survivability.
Researches [2][3][4] carried out in recent years show that degree distribution of many networks is obviously different from Poisson distribution. The degree distribution of many networks, such as WWW, Internet in autonomous layers, paper citation networks, can be better depicted with power-law form \( P(k) \propto k^{-\gamma} \). The decline of power-law distribution curve is much slower than Poisson exponential distribution curve.

Network with power-law degree distribution is also known as scale-free network, which has highly non-uniform degree distribution, i.e. the degree of most nodes is relatively small, while the degree of a small amount of nodes is relatively big.

Researches show that, compared with stochastic network, scale-free network has a higher robustness on random failure, but has a highly vulnerability on intentional attacks. Here, intentional attacks refer to consciously remove a very few nodes of the network with maximum importance degree, which will strongly affect the whole network’s connectivity. For scale-free network, in case 5% core nodes are attacked, the network will basically become paralyzed.

At present, in documents related to network survivability, many documents [5][6] only consider network survivability under static conditions, that is, after giving a initial network topology, they calculate the survivability of the network according to some indexes with the assuming that the network does not suffer from any attack. Obviously, these methods are defective because they do not take consideration of the situation where the network is attacked. The survivability value is meaningful only when the network is attacked. The network survivability obtained under static conditions cannot reflect the actual situation.

For this purpose, the article put forward an evaluation method for network survivability under intentional nodes attack, that is, after giving a network topology, we assuming that its nodes suffer from intentional attacks (generally, 5% core nodes are removed), and then calculate its survivability. Under the intentional nodes attack assuming, if one network’s survivability is higher than that of another network, we will reckon that the former network is more reliable.

**THE MODEL OF SURVIVABILITY EVALUATION**

Generally, network nodes will choose a shortest path for communication because the shortest path has the minimal hops. When part of the nodes does not work due to network attacking, network nodes will choose another shortest path for communication. Obviously, after the network nodes are attacked, the hops of the shortest path between nodes will increase, what’s worse, there may be no path between nodes due to disconnection. When hops increase, the reliability of network communication will decline. The path with fewer hops has a better reliability. Therefore, it is reasonable to evaluate network survivability from the hops of the shortest path. A network with strong survivability shall be the one whose hops increase of the shortest path between network nodes is smaller after the network is attacked.
The Average Hops of Whole Network

Assume that a network has N nodes, \( r_{ij} \) is the shortest path between node i and node j, and \( h_{ij} \) is the hops of the path:

\[
h_{ij} = \text{hops}(r_{ij}), \quad 1 \leq i, j \leq N, i \neq j
\]  

Therefore, the average hops of whole network \( H \) is defined as:

\[
H = \frac{1}{N(N-1)} \sum_{i=1}^{N} \sum_{j=i+1}^{N} h_{ij}
\]

Core Nodes

The article considers the network survivability under intentional nodes attack, that is, to consciously remove a very few core nodes in the network. Therefore, which nodes are core nodes in the network is a question that shall be clarified. Generally, people adopt the following two methods to judge the core nodes in a network [7].

One is judging from the size of “degree”, i.e., the nodes with bigger degree stand a large chance to be core nodes. Another is judging from the size of “betweenness”. Betweenness refers to the path quantity passing through a certain node within all shortest paths in a network. For node i, its betweenness is defined as:

\[
b_i = \sum_{j \neq k} g_{jk}(i) / g_{jk}
\]

In the formula, \( g_{jk} \) refers to the number of shortest path between node j and node k; \( g_{jk}(i) \) refers to the number of shortest path between node j and node k passing through node i. Betweenness reflects the pivotability of a node in the network. The higher of the betweenness of a node, the more important the node is. Therefore, core node can be judged by betweenness value.

In the article, considering simplicity of realization, we adopt “degree” to judge core nodes. We assume that intentionally attacking the core nodes of a network refers to attacking the top 5% nodes in the network which are arranged according to their degree values from large to small. For a network with N nodes, assuming that the number of 5% nodes is D, the assembly of these nodes is \( s = \{n_1, n_2, \ldots, n_D\} \). In this way, when these core nodes are destroyed one by one, D kinds of conditions are one by one experienced:

\[
\begin{align*}
    s_1 &= \{n_1\} \\
    s_2 &= \{n_1, n_2\} \\
    & \vdots \\
    s_{D-1} &= \{n_1, n_2, \ldots, n_{D-1}\} \\
    s_D &= \{n_1, n_2, \ldots, n_{D-1}, n_D\}
\end{align*}
\]
The Average Hops of Whole Network after it is Attacked

Now the situation where the network is attacked is considered. After the network nodes were attacked, the network will become disconnected, as shown in Figure 1. At that time, for all connected sub-graphs, the hops of the shortest path between the internal nodes can still be calculated according to the original methods. While for nodes between disconnected sub-graphs, there is no path, therefore hops cannot be obtained. For this purpose, for all the left nodes which not include the attacked nodes, we will redefine the hops between the nodes according to the following formula:

\[ h'_{ij} = \begin{cases} \text{hops}(r_{ij}), & \text{has route} \\ C, & \text{no route} \end{cases} \]  

(4)

In the formula, \( C \) is a constant, standing for the cost, that is, under the circumstance that there is no path between node i and j, the cost C shall be paid to make the communication between them available.

![Image of networks](image)

Figure 1. The demo of disconnected sub-graphs occurring after the network is attacked.

For this purpose, when \( d (d \leq D) \) nodes in the network were attacked, that is, all nodes belong to assembly \( s_d = \{ n_1, n_2, \ldots, n_d \} \) were destroyed, at this time \( N - d \) nodes of the network are left, and the average hops of the whole network is:

\[ H_d = \frac{1}{2} \frac{1}{(N - d)(N - d - 1)} \sum_{i=1}^{N-d} \sum_{j=1, j \neq i}^{N-d} h'_{ij} \]  

(5)

The Survivability Measure Function

Now we calculate the network survivability according to the above mentioned average hops of the network after it was attacked. We assume that network nodes are destroyed one by one, that is, the assembly of the destroyed nodes is \( s_1, s_2, s_3, \ldots, s_d \). In this way, we define the survivability measure function of the network as:

\[ S = \frac{1}{D} \sum_{d=1}^{D} (H_d - H_0) = \left( \frac{1}{D} \sum_{d=1}^{D} H_d \right) - H_0 \]  

(6)
In the formula, $H_0$ stands for the average hops of initial network. After the network is attacked, its average hops generally will increase, therefore, when the network node number $N$ is relatively big, $H_d$ will be greater than $H_0$. The meaning of the above formula is that, when the network nodes are attacked one by one, the average hops of network will continuously increase. The weaker of the network’s survivability is (especially occurrence of disconnected sub-networks), the bigger the increment is. Therefore, after obtaining the value $S$, the larger $S$ is, the weaker the network’s survivability is; the smaller $S$ is, the stronger the network’s survivability is.

The above measure function hides a fact, that is, when network nodes are attacked one by one, earlier the disconnected sub-networks appear in a network, the larger the $S$ value will be, which means the weaker the network’s survivability is.

**EXPERIMENTAL RESULTS**

In order to verify the effectiveness of the evaluation method for network survivability given in the paper, experimental results on some networks are given below. Take consideration of experimental results under two conditions, one aims at special networks, and another aims at general networks. We assume that the network’s node number $N=60$, in this way, intentionally attacked node number $D$ is 3 (calculate according to 5%).

**Comparison of Special Networks’ Survivability**

This paper compares the survivability of three special networks, which are fully-connected network, star network and ring network, as shown in Figure 2. In the experimental calculation, we assume that the value of $C$ in formula (4) is $N/2$.

![Figure 2. The demo of special networks, which are fully-connected network, star network and ring network.](image)

Applying the evaluation method for survivability given in this paper, we get the following experimental results for above three networks, as shown in Table 1.

From the experimental results, we can see that the survivability of fully-connected network is strongest, and the survivability of star network is weakest, which conforms to the actual situation.
Table 1. The experimental result of special networks’ survivability.

| Attacked Nodes | $H_d$ | Attacked Nodes | $H_d$ | Attacked Nodes | $H_d$ |
|----------------|-------|----------------|-------|----------------|-------|
| \{n_1\}        | 1     | \{n_1\}       | 30    | \{n_1\}       | 20    |
| \{n_1,n_2\}    | 1     | \{n_1,n_2\}   | 30    | \{n_1,n_3\}   | 20    |
| \{n_1,n_2,n_3\}| 1     | \{n_1,n_2,n_3\}| 30    | \{n_1,n_2,n_3,n_4\} | 22 |

$S = 0$ $S = 28$ $S = 6$

Comparison of General Networks’ Survivability

Here, we compare the survivability of two networks with general topological structure, which are shown in Figure 3. In the experimental calculation, we assume the value of $C$ in formula (4) is $N/4$.

![Figure 3: The demo of two general networks for survivability comparison.](image)

Applying the evaluation method for survivability given in this paper, we obtain the following experimental results for above two networks, as shown in Table 2.

From the experimental results, we can see that the survivability of network b is better than that of network a. Observing the topological structures of two networks intuitively, because network b has one more links than network a, so the survivability of network b is supposed to be stronger than that of network a. Therefore, the experimental results are correct.

Table 2. The experimental result of general networks’ survivability.

| Network a | Network b |
|-----------|-----------|
| Attacked Nodes | $H_d$ | Attacked Nodes | $H_d$ |
| \{n_1\}        | 8.1     | \{n_1\}       | 6.1    |
| \{n_1,n_{46}\} | 11.2    | \{n_1,n_{46}\} | 10     |
| \{n_1,n_{46},n_{31}\} | 13.3 | \{n_1,n_{46},n_{31}\} | 11.4 |

$S = 8.1$ $S = 7.4$
CONCLUSION AND FURTHER WORK

Aiming at the deficiency of static evaluation methods for network survivability, the paper put forward a dynamic evaluation method for network survivability. The paper firstly introduces the concept of network average hops, and then assumes that when the network suffers from intentional attacks, the invalidation of partial network nodes will result in the increase of network average hops. Obviously, the increment of average hops for the network with weak survivability will be larger, especially under the condition that disconnected sub-networks appear after the network was attacked, the increment of average hops will be more notably. Therefore, the survivability measure function and evaluation method proposed in the paper are reasonable, and the experimental results also prove the correctness of the method. As the assumption that the network being attacked is considered by the method mentioned in the paper, it has a high value of practical application. In the future, the author will carry out researches on the situations where the network suffers from virus infection and network edges are attacked, aiming to improve network’s reliability better.

REFERENCES

1. Jianjun Shen. Research on Operation Simulative Training in Information Age [C]. Applied Mechanics and Materials Vols. 411-414, 2013: 2860-2864.
2. Barabási A.L., Bonabeau E. Scale-free networks. Scientific American, May 2003: 50-59.
3. Newman M.E.J. The structure and function of complex networks. SIAM Review, 2003(45): 167-256.
4. Albert R., Barabási A.L. Statistical mechanics of complex networks. Reviews of Modern Physics, 2002(74): 47-97.
5. Rongkun Yuan, Xiangru Meng, Mingxun Li, Xiangxi Wen. Evaluation Method for Network Invulnerability Based on Node Importance. Fire Control & Command Control, 2012(37): 40-42.
6. Yuping Rao, Jingyu Lin, Deting Hou. Evaluation method for network invulnerability based on shortest route number. Journal on Communications, 2009(30): 113-117.
7. Holme P., Kim B.J., Yoon C.N., Han S.K. Attack vulnerability of complex networks. Phys. Rev. E 2002, 65: 056109.