Analysis of Network Vulnerability Under Joint Node and Link Attacks

Yongcheng Li 1, Shumei Liu 2, Yao Yu * 2, Ting Cao 3

1 State Key Laboratory of Complex Electromagnetic Environment Effects on Electronics and Information System (CEMEE), Luoyang, China
2 School of Computer Science and Engineering, Northeastern University, Shenyang, China
3 Shenyang International Engineering Consulting Center, China

*Corresponding author e-mail: yuyaosy@163.com

Abstract. The security problem of computer network system is becoming more and more serious. The fundamental reason is that there are security vulnerabilities in the network system. Therefore, it’s very important to identify and reduce or eliminate these vulnerabilities before they are attacked. In this paper, we are interested in joint node and link attacks and propose a vulnerability evaluation method based on the overall connectivity of the network to defense this attack. Especially, we analyze the attack cost problem from the attackers’ perspective. The purpose is to find the set of least costs for joint links and nodes, and their deletion will lead to serious network connection damage. The simulation results show that the vulnerable elements obtained from the proposed method are more suitable for the attacking idea of the malicious persons in joint node and link attack. It is easy to find that the proposed method has more realistic protection significance.

1. Introduction

Analysis of network vulnerability plays a vital role in the risk evaluation for network security. To avoid risks and take proactive measures, it is necessary to evaluate network performance of vulnerability to determine the serious of devastating attack threats.

A great deal of works have been done on evaluating network performance of vulnerability, but most of these works pay attention to use centrality dimension, such as degree and betweenness, to determine vulnerable nodes or even links [1, 2]. However, these methods only consider the relative importance of a few nodes or links, and thus they cannot expose the tremendous harm of attacking simultaneously. Another works focus on the problems of removal optimizing several global graph methods to nodes and links, such as network diameter, clustering coefficient, etc [3, 4]. Unfortunately, these methods do not apply well when the connectivity of network is high-priority. Recently, pairwise connectivity has been used as an useful method to analysis the effect of the attacks [5, 7-10].

The pairwise connectivity was first proposed in [6] as an useful method. Arulselvan et al later proposed the critical node/link problems. T. N. Minh and M. T. Thai et al first put the evaluating network vulnerability methods as optimization problems in [5] and [7], namely $\beta$-edge disruptor and $\beta$-vertex disruptor, the purpose is to search a minimum set of vulnerable elements. However, these methods merely to study the vulnerability of nodes or links, and ignore grave damage to the network...
caused by joint nodes and links attack schemes. Then T.N.Dinh et al considered the cost of attack and proposed a new optimization method for the joint node and link attack problem — $\beta$ -disruptor [10], the purpose is to search a set of minimum costs for links and nodes which deletion would degrade the pairwise connectivity greatly. However, this method ignores the situation that the multi-group sets attack cost are the same when the network connectivity degradation condition is satisfied; And multiple parameters are introduced in the algorithm, which is not conducive to the selection of parameter values.

Based on the above analysis, this paper provides a more comprehensive evaluation on network vulnerability and presents the scheme vulnerability analysis of joint links and nodes attacks based on connectivity (JNLC). The main work and contributions of this paper are as following:

- The mapping function is defined in our scheme, which avoids the introduction of other parameters except $\beta$ and also ensures the accuracy of the algorithm analysis results.
- The goal of this scheme is to identify a set of minimum costs for nodes and links which deletion would degrade the connectivity of network greatly. Considering that the attack costs of several sets may be the same, this scheme improves and strengthens the algorithm, we select the set that have the greatest degree of damage to the network as the result when the costs of several sets are equal.

The rest of the paper is as following: In section 2, we describe definition and algorithm process; In section 3, we analyze the simulation results of the proposed JNLC scheme and the other three comparison schemes; The conclusion is presented in Section 4.

2. Vulnerability Analysis of Joint Node and Link Attacks Based on Connectivity (JNLC)

Based on the previous work, this paper proposes a node-link joint analysis scheme based on connectivity (JNLC). It is intended to determine a set of limit costs for links and nodes which deletion would degrade the pairwise connectivity greatly, then we refine the results in the algorithm to make the analysis more accurate.

2.1. Models and Definition

The general network model is abstracted as a graph $G = (V, E)$, where $V$ is the set of all nodes and $E$ is the set of all links. In addition, we construct the auxiliary model $G' = (V', E')$ on the basis of the general network model, each node $i$ in $G$ is divided into two new nodes $i^+, i^-$, and the link $(i^+, i^-)$ in $G'$ corresponds to the node $i$ in $G$, link $(j^+, j^-)$ corresponds to the link $(j, i)$ in $G$, as follows:

$$
G' = (V', E') = (V^+ \cup V^-), E' = \{(i^+, i^-) \mid i \in V \} \cup \{(j^+, j^-) \mid (j, i) \in E \}
$$

where $V^+ = \{i^+ \mid i \in V, i \neq j \}$, $V^- = \{i^- \mid i \in V, i \neq j \}$, $E' = \{(i^+, i^-) \cup \{(j^+, j^-) \mid (j, i) \in E \}$

**Definition 1** (attack cost $c$): Attack cost is the cost of destroying network elements (nodes or communication links). For the nodes and links we are abstracted with $a, b$ quantified, respectively, i.e.

$$
c(i^+, i^-) = a, c(j^+, j^-) = b.
$$

It is worth noting that in the simulation phase, set $a > b$. Due to delete either $i$ or $j$ creates more disruption than delete the link $(i, j)$, it will focus on protecting nodes in the basic protection. So the attack costs of nodes are usually higher than links.

**Definition 2** (connectivity): Use $u_{ij}$ to denote the connection relation between nodes $i$ and $j$ in the algorithm embodied as follows:

$$
u_{ij} = \begin{cases} 
1 & \text{If there exist paths between node } i \text{ and } j \\
0 & \text{If there is no path between node } i \text{ and } j
\end{cases}
$$
The pairwise connectivity of $G$ is represented by $P(G)$, as shown in (1).

$$P(G) = \sum_{u \in V} u_0$$  \hspace{1cm} (1)

**Definition 3** (mapping function $f$): This paper constructs the auxiliary graph $G'$, so that all the links in $G'$ represent the nodes and links in $G$, which can make the algorithm only analyze the links in $G'$ to get results. In order not to introduce other parameters except $\beta$, but also make the results more accurate, we must use a function to express the relationship between $G$ and $G'$, as show in (2):

$$f(G') = G$$  \hspace{1cm} (2)

In this way, we can map the set $S'$ in $G'$ back to $G$ to get the corresponding nodes and links, i.e. $f(S') = S$. The specific rules of the mapping function are described in detail in the next algorithmic process.

2.2. JNLC scheme algorithm process

The overall idea of the JNLC scheme is divided into two points:

(1) The result of the algorithm analysis is a set of least costs for links and nodes;

(2) Destroying the analysis results can degrades the pairwise connectivity to $\beta$ times of the original graph.

**The algorithm description:**

Input: graph model $G$, node attack cost $a$, link attack cost $b$, connectivity threshold $\beta$.

Output: vulnerable elements set $S$, residual network graph $G \setminus S$.

Algorithm Pseudo Code:

1. Define variable $S', S'' = \emptyset$
2. Input original graph $G$
3. For node $i \rightarrow (i^+, i^-)$, for link $(i, j) \rightarrow (j^+, j^-)$, get the auxiliary graph $G'$
4. Construct the mapping function $f$, so that $f(S') = S$
5. Define the cost of each link in $G'$
6. Construct the cost function $C(S') = \sum_{(i^+, i^-) \in S'} a \cdot c(i^+, i^-) + b \cdot c(i^+, j^-)$
7. Construct the connectivity function $P(\cdot)$
8. $S'_1, S'_2 \in G'$
9. \hspace{1cm} if $P(G \setminus S'_1) \leq \beta \binom{n}{2}$ and $P(G \setminus S'_2) \leq \beta \binom{n}{2}$
10. \hspace{2cm} if $C(S'_1) > C(S'_2)$
11. \hspace{3cm} $S' = S'_1$
12. \hspace{2cm} else if $C(S'_1) = C(S'_2)$
13. \hspace{3cm} if $P(G \setminus S'_1) > P(G \setminus S'_2)$
14. \hspace{4cm} $S' = S'_1$
15. \hspace{3cm} else $S' = S'_2$
16. $S = f(S')$
17. Output the vulnerable element set $S$
18. Get the residual network graph $G \setminus S$

As shown in lines 4, the mapping rule for the mapping function is for each link $(d^+_1, d^-_1)$ in $G'$, if $d_1 = d_2$, then $S = S \cup \{d_1\}$, if $d_1 \neq d_2$, then $S = S \cup \{(d_1, d_2)\}$; As shown in lines 12-15, when the costs of several sets are equal, select the set that have the greatest degree of damage to the network as the result, so that it is more in line with the vulnerability analysis goal.
3. Experimental Results
In this experiment, simulation analysis is carried out at the network topology including 11 nodes and 18 links. We consider the proposed scheme JNLC and other three schemes in comparison, including the vulnerability analysis scheme based on degree-centricity (ND), the node vulnerability analysis scheme based on pairwise connectivity (NC) and the link vulnerability analysis scheme based on pairwise connectivity (LC).

The proposed JNLC scheme considers the attack cost to confirm the effectiveness of this scheme, we compare the attack cost of JNLC with other three comparison schemes. As shown in Figure 1 (a), when \( a = 3 \) and \( b = 2 \) ( \( a \) and \( b \) are the attack cost of node and link in \( G \), respectively.), the attack cost of JNLC scheme is the lowest in four schemes; Similarly, when \( a = 4 \) and \( b = 2 \), although the cost of all schemes has increased, the attack cost of JNLC scheme is still the lowest, as shown in Figure 1 (b). It easily can be seen that the set of vulnerable elements in the JNLC scheme is the most suitable for the attacker's attack target, that is, has more protection significance.

![Comparison of Attack Costs](image)

(a) When \( a = 3, b = 2 \), the attack cost of four schemes under different damage degree
(b) When \( a = 4, b = 2 \), the attack cost of four schemes under different damage degree

Fig.1 Comparison of Attack Costs

4. Conclusion
Accurate network vulnerability analysis can provide strong support for improving network security. In this paper, we evaluate the effect of attacks as far as connectivity and the attack cost problem is taken into account, the purpose is to search a set of limited cost for nodes and links which deletion will seriously damage the network connection. At the same time, the mapping function is defined in the algorithm to optimize the selection of parameters. It also considers and improves the situation when multiple sets of attack costs are the same. The experimental results show that the JNLC scheme can truly reflect the most vulnerable parts of the network and accurately predict the set that the attacker is most likely to attack.

Reference
[1] Albert R, Jeong H, Barabási A L. Error and attack tolerance of complex networks[J]. arXiv preprint cond-mat/0008064, 2000.
[2] Albert R, Albert I, Nakarado G L. Structural vulnerability of the North American power grid[J]. Physical review E, 2004, 69(2): 025103.
[3] Grubesic T H, Matisziw T C, Murray A T, et al. Comparative approaches for assessing network vulnerability[J]. International Regional Science Review, 2008, 31(1): 88-112.
[4] Murray A T, Matisziw T C, Grubesic T H. A methodological overview of network vulnerability analysis[J]. Growth and Change, 2008, 39(4): 573-592.
[5] Dinh T N, Xuan Y, Thai M T, et al. On new approaches of assessing network vulnerability: hardness and approximation[J]. IEEE/ACM Transactions on Networking, 2012, 20(2): 609-619.
[6] Matisziw T C, Murray A T. Modeling s–t path availability to support disaster vulnerability assessment of network infrastructure[J]. Computers & Operations Research, 2009, 36(1): 16-26.

[7] Dinh T N, Thai M T. Precise structural vulnerability assessment via mathematical programming[C]//MILITARY COMMUNICATIONS CONFERENCE, 2011-MILCOM 2011. IEEE, 2011: 1351-1356.

[8] Shen Y, Dinh T N, Thai M T. Adaptive algorithms for detecting critical links and nodes in dynamic networks[C]//MILITARY COMMUNICATIONS CONFERENCE, 2012-MILCOM 2012. IEEE, 2012: 1-6.

[9] Shen Y, Nguyen N P, Xuan Y, et al. On the discovery of critical links and nodes for assessing network vulnerability[J]. IEEE/ACM Transactions on Networking (TON), 2013, 21(3): 963-973.

[10] Dinh T N, Thai M T. Network under joint node and link attacks: Vulnerability assessment methods and analysis[J]. IEEE/ACM Transactions on Networking, 2015, 23(3): 1001-1011.