International Journal of Security and Its Applications
Vol.9, No.11 (2015), pp.157-186
http://dx.doi.org/10.14257/ijsia.2015.9.11.17

# The Invulnerability Studies on Data Center Network

Kai Peng[1] and Binbin Huang[2]

[1]*College of Engineering, Huaqiao University, Quanzhou, Fujian, China*
[2]*School of Computer Science and Technology, Hangzhou Dianzi University, Hangzhou, Zhejiang, China*
*pkbupt@gmail.com*;
*huangbinbin@hdu.edu.cn*

***Abstract***

*Data center network (DCN) as the core of the cloud platform receives a widespread concern attention. Recently, the main study of these new architectures is limited to load balancing or improvement of architectures while the security study of DCN is still in its preliminary, especially for the vulnerability study. In our previous researches, we mainly concern about the invulnerability study from the protection of important nodes and vita edges. Differ from the previous one, in this paper; we engaged in the invulnerability studies from the perspective of network attack. Taking typical instances of DCN for example, based on invulnerability measurement of the average shortest path distance, we analysis the invulnerability of DCN by choosing deliberate attack and random attack. Experimental results show that for most architectures of DCN, the deliberate attacks of degree get the same result with the deliberate attacks of betweenness, especially, the deliberate attacks of degree are often harmful than betweenness attacks when attack a few nodes. However, from the perspective of random attacks, random attacks of betweenness are more harmful than degree attacks. The main contribution can be summarized as follows. We firstly engaged in the invulnerability research of DCN from the perspective of network attack and then conclude the network invulnerability of DCN by amount of experiments. The result in this paper can be widely used for the protection of DCN.*

***Keywords****: DCN, Invulnerability, Attack, Degree, Betweenness*

## 1. Introduction

Data center network (DCN) as the core of the cloud platform [1-2] receives widespread concern from both industry and academia research, a good many network structures [3-7] have been proposed for these extensive data centers. In general, all existing DCN architectures can be classified into two types, hierarchy network architecture and the recursive one. In recent years, the main study of assessment of these new architectures is limited to load balancing or improvement of architectures as the demand of new services however a few of existing research concerned about the security of the DCN, especially for the vulnerability studies for these new architectures. Network invulnerability is generally defined as the decline in the value of the overall performance of the network failure, which means the entire network can continue to work when the network is under the specific attack or service failure mode [8]. In our previous researches, we fill this void by conducting an experimental evaluation of these architectures from the node importance [9] and edge importance [10], so that we can improve the capability of network protection for vita nodes. Differ the previous ones, in this paper, we engaged in the invulnerability research of DCN for the perspective of network attack. Research on network vulnerability can make us better know how to effectively protect network. Taking typical instances of the hierarchy network architecture (Tree and Fat-tree [3]) and the recursive network architecture (BCube [6] and FiConn [7]) for examples, based on invulnerability

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2015 SERSC

measurement of the average shortest path distance, we analysis the invulnerability of DCN by choosing deliberate attack and random attack. According to the result by designing a large number of comparative experiments, we conclude that for most architectures of DCN, the deliberate attacks of degree got the same result with the deliberate attacks of betweenness, especially, the deliberate attacks of degree are often more harmful than betweenness attacks when attack a few nodes. However, from the perspective of random attacks, betweenness attacks are much better than that of degree attacks.

The main contribution in this paper can be summarized as follows. We firstly engaged in the invulnerability research of DCN for the perspective of network attack and then conclude the network invulnerability of DCN by amount of experiments on current typical instances of DCN. The result in this paper can be widely used for the protection of DCN.

The remainder of this paper is as follows. In Section 2, we introduce the invulnerability measurement. Attack strategies are described in Section 3. Followed by Section 4; we present the algorithm model and the simulation results. Finally, we conclude the paper in Section 5.

## 2. Invulnerability Measurement

In this section, we introduce the network invulnerability measure. Firstly, we give the definition of network invulnerability and then show the corresponding formula of DCN.

Network invulnerability is generally defined as the decline in the value of the overall performance of the network failure, which means the entire network can continue to work when the network is under the specific attack or service failure mode [8].

Let an undirected graph G represents the data center network, where v and w represent any two nodes in G.

As observed in [8], we can use the average shortest path distance ( L ) for the measurement of network invulnerability and the expression can be given as follow.

$$L =< d < v, w >>= \frac{1}{N(N-1)} \sum_{v \in V} \sum_{w \neq v \in V} d(v, w) \quad (1)$$

Where, $d(v, w)$ represents the shortest distance between node v and node w, N represents the total number of nodes in given network. $d(v, w)$ means that the nodes in DCN need to minimize the cost of transmission. Thus it can be used to measure the invulnerability of DCN. The more the increase of the average shortest path distance, the faster the decline of the overall performance of the network. That means the network get worse invulnerability.

## 3. Attack Strategy

The degree and betweenness as the two important indicators are widely used for the invulnerability research. In this paper, we will use these two indicators for the invulnerability research of DCN [11-12]. Based on the deliberate attack and random attack, we will design specific algorithm by choosing degree random attack and degree deliberate attack, betweenness random attack as well as betweenness deliberate attack. In Section 3.1, we give the definition and corresponding formula of degree, followed by section 3.2; we describe the definition and formula of betweenness.

### 3.1. Degree

According to graph theory [13], in an undirected graph G, the number of edges incident to the vertex of G is counted as degree. The degree of a vertex is denoted as $d_v$

 Copyright ⓒ 2015 SERSC

$$d_v = \sum_{l \in E} \sigma_l^v \tag{2}$$

Where the value of $d_v$ can be obtained by the edge and the node of V, the detail is as following expressions

$$\delta_l^v = \begin{cases} 1 & if \text{ the edge l contains node v} \\ 0 & else. \end{cases} \tag{3}$$

### 3.2 Betweenness

The betweenness of a node is shown by the expression (4) [14]. The betweenness of a vertex is denoted as $B_i$.

$$B_i = \frac{\sum_{j}^{n}\sum_{k}^{n} \frac{g_{jk}(\mathrm{i})}{g_{jk}}}{N(\mathrm{N}-1)/2} \quad j \neq k \neq i \;\; j < k \tag{4}$$

Where $g_{jk}$ is the total number of shortest paths between node of j and node of k, and $g_{jk}(\mathrm{i})$ is the number of these paths that go through node of i.

N is the total number of nodes. Be careful for that the calculation of betweenness of a node scales may be adjusted by dividing through by the number of pairs of nodes while not including node of i. The division is done by for undirected graphs, in our paper, is $\mathrm{N}(\mathrm{N}-1)/2$ and for directed graphs is $(\mathrm{N}-1)(\mathrm{N}-2)$.

As shown in Formula (4), the betweenness reflects the ability of providing the shortest route of network communication tasks of nodes. It can be used to measure the nodes' ability of controlling network resources. As betweenness fully reflect the interactive capabilities of the nodes, thus it can be widely used for determine where the heavy information load network nodes through the flow of information is. Moreover, it is also can be used to alleviate network congestion and check the cascading failure malicious attacks [15]. Thus, we can use betweenness for the invulnerable research of DCN.

## 4. Algorithm Model and Experimental Results Analysis

This section is the main part in this paper. In Section 4.1, we introduce the algorithm model, followed by Section 4.2; we describe the experimental results and the corresponding analysis.

### 4.1. Algorithm Model

(1) Degree (betweenness) deliberate attack algorithm

1. Let the adjacency matrix storage topology of network and calculate the degree (betweenness) of each node according to the adjacency matrix;
2. Delete one node each time when two or more nodes got the same value, choose one node by random algorithm, and then compute the average shortest distance;
3. Repeat Step 2, when the attack rate of node (the removed node accounted for summary nodes) got the value of 1 or the average shortest path distance got the value of 0, output the result (attack ratio and the average shortest path distance).

Copyright ⓒ 2015 SERSC

(2) Degrees (betweenness) random attack algorithm

Remove one node and corresponding edges and then calculate the average shortest distance by random algorithm; when the attack rate of node (the removed node accounted for summary nodes) got the value of 1 or the average shortest path distance got the value of 0, find out the best case of random attack and worst one by 20 times. Especially, once two or more nodes got the same value of degree (betweenness), choose one node by random algorithm.

### 4.2. Experimental Results and Analysis

This section mainly contains three sub parts. In Section 4.2.1.we mainly describe the degree attack simulation and the corresponding result discussion, the betweenness attack simulation and the corresponding result discussion are introduced in Section 4.2.2.And then, we describe the degree attack and betweenness attack comparative experiments in Section 4.2.3.

#### 4.2.1. The Degree Attack Simulation

In this Section, we will introduce degree attack simulation and discussion of four different architectures.

(1)The degree attack simulation of Tree
There are fourteen nodes in Tree, as shown in Figure 1-1; we can see the degree and betweenness. In this paper, we design four groups for tree experiment.

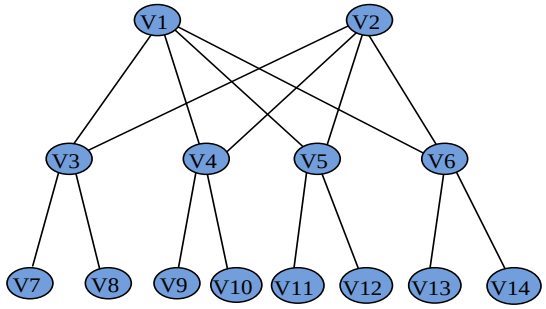



**Figure 1-1.Tree Architecture Been Marked**

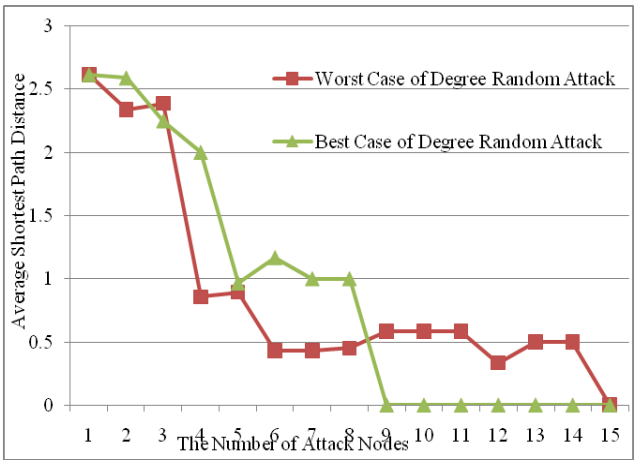
**Table 1-1.Degree and Betweenness of Tree**

| Node | Degree | Betweenness |
|---|---|---|
| V1 | 4.0000 | 0.1837 |
| V2 | 4.0000 | 0.1837 |
| V3 | 4.0000 | 0.1582 |
| V4 | 4.0000 | 0.1582 |
| V5 | 4.0000 | 0.1582 |
| V6 | 4.0000 | 0.1582 |
| V7 | 1.0000 | 0 |
| V8 | 1.0000 | 0 |
| V9 | 1.0000 | 0 |
| V10 | 1.0000 | 0 |
| V11 | 1.0000 | 0 |
| V12 | 1.0000 | 0 |
| V13 | 1.0000 | 0 |
| V14 | 1.0000 | 0 |

 Copyright ⓒ 2015 SERSC

Group 1: Comparative experiments of random attack

As shown in Figure 1-2(a), we can see that we only need to attack seven nodes (the attack rate will be 47%) in the ideal situation, the entire network will be destroyed while in the worst one, we should attack thirteen nodes (the attack rate will be 86%).

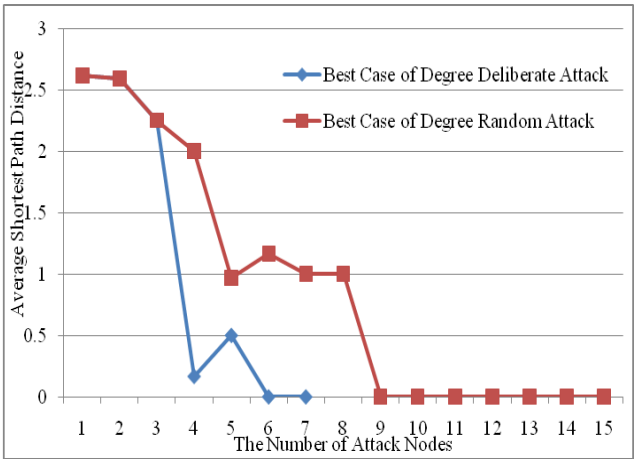



(a)

**Figure 1-2. The Degree Random Attack Experiments of Tree**

Group2: Comparative experiments of random attack and deliberate attacks of degrees

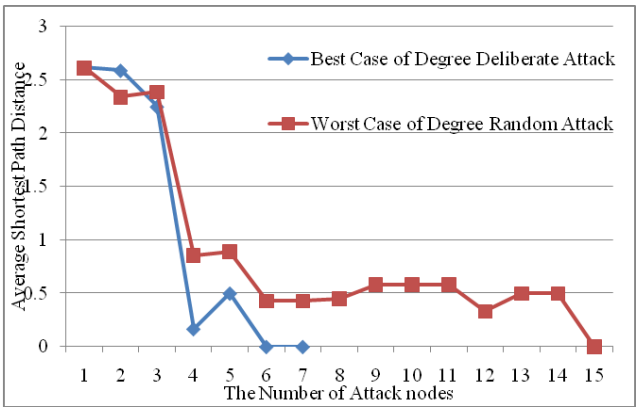
For Tree, the best deliberate attack of degree and the worst random attack of degree got nearly the same result, thus we only need to design two-group experiment.1)The average degree of deliberate attacks and best-case degree of random attack; 2) The average degree of deliberate attack and the worst degree of random attack comparison. The experimental results are shown in Figure 1-2(b) and Figure 1-2(c).




(b)

**Figure 1-2 The Best Case of Degree Deliberate Attack and Best Case of Degree Random Attack**

Copyright ⓒ 2015 SERSC




(c)

**Figure 1-2(c). The Best Case of Degree Deliberate Attacks and Worst Case of Degree Random Attack**

We can see that, degree of deliberate attack only need to attack four nodes (the attack rate reach 27%) will destroy the whole network, which is much better than that of the best degree of random attack (the attack rate is 47%), and also the worst degree of random attack (the attack rate is 86%).

(2) The experiments and results analysis of Fat-tree

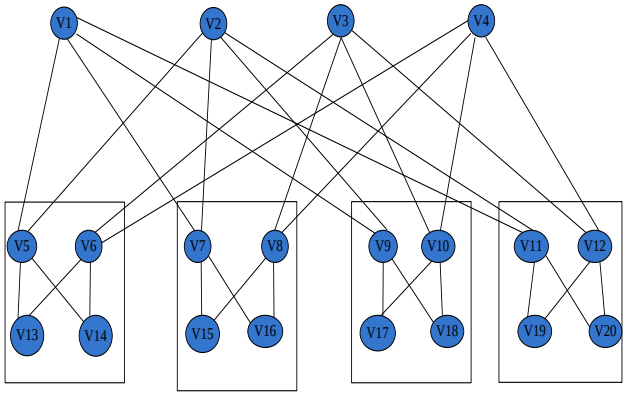



**Figure 2-1.Fat-tree Architecture Been Marked**

There are twenty nodes in Fat-tree, as shown in Figure 2-1; we can see the degree and betweenness. In this paper, we design four-group experiments for Fat-tree

**Table 1-2.Degree and Betweenness of Fat-tree**

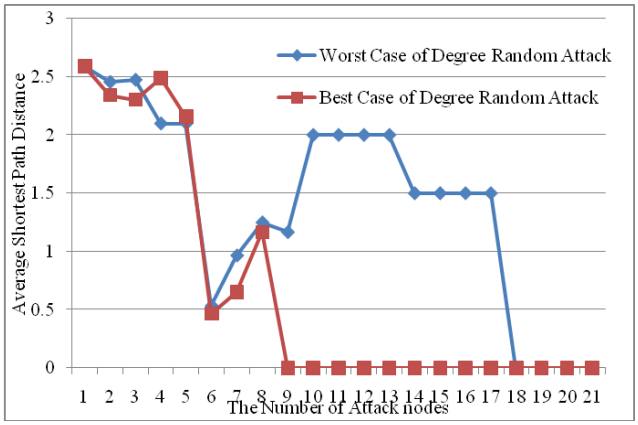
| Node | Degree | Betweenness |
|---|---|---|
| V1 | 4.0000 | 0.0795 |
| V2 | 4.0000 | 0.0795 |
| V3 | 4.0000 | 0.0795 |
| V4 | 4.0000 | 0.0795 |
| V5 | 4.0000 | 0.0704 |
| V6 | 4.0000 | 0.0704 |
| V7 | 4.0000 | 0.0704 |
| V8 | 4.0000 | 0.0704 |
| V9 | 4.0000 | 0.0704 |


Copyright ⓒ 2015 SERSC

| | | |
|---|---|---|
| V10 | 4.0000 | 0.0704 |
| V11 | 4.0000 | 0.0704 |
| V12 | 4.0000 | 0.0704 |
| V13 | 2.0000 | 0.0149 |
| V14 | 2.0000 | 0.0149 |
| V15 | 2.0000 | 0.0149 |
| V16 | 2.0000 | 0.0149 |
| V17 | 2.0000 | 0.0149 |
| V18 | 2.0000 | 0.0149 |
| V19 | 2.0000 | 0.0149 |
| V20 | 2.0000 | 0.0149 |

Group1: The random attack of degree

As shown in Figure 2-2(a), we can see that, in the ideal situation we only need to attack seven nodes (the attack rate will be 35%), the entire network will be destroyed while in the worst one, we should attack sixteen nodes(the attack rate will be 80%).

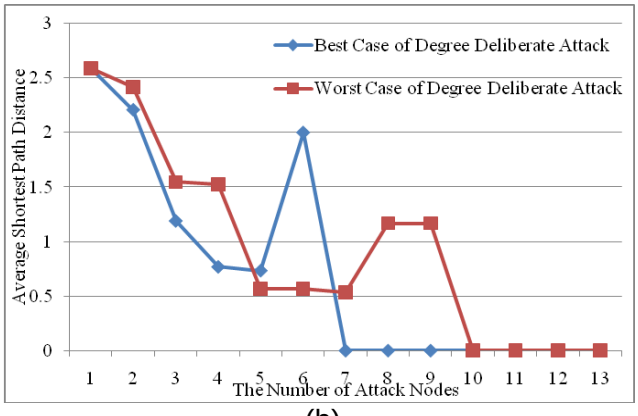



(a)

**Figure 2-2. The Degree Random Attack Experiments of Fat-tree**

Group2: Degree of deliberate attacks comparative experiments

As shown in Figure 2-2(b), we can see that, in the ideal situation, we only need to attack six nodes (the attack rate will be 30%), the entire network will be destroyed while we should attack nine nodes (the attack rate will be 45%) in the worst one. All in all, the best case of degree deliberate attacks and worst case of deliberate attacks got the close effect.

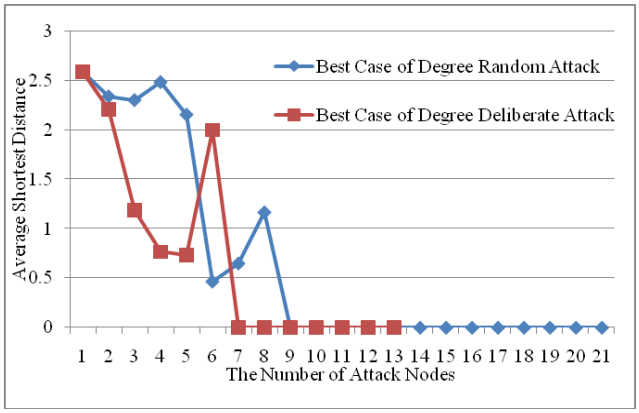



(b)

**Figure 2-2, The Degree Deliberate Attack Experiments of Fat-tree**

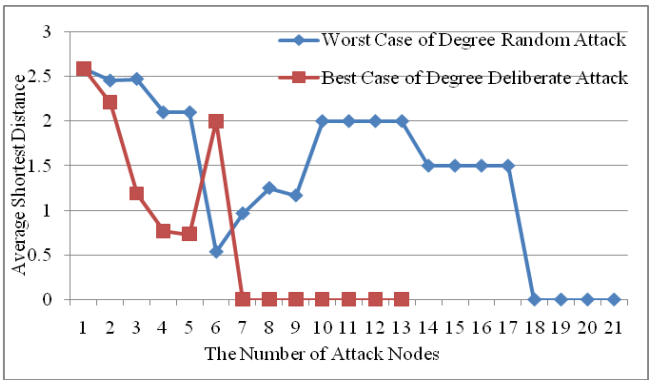
Group 3: Random attack experiment and deliberate attack experiment
For Fat-tree, we design four group experiments for the best case of degree deliberate attack and worst case of deliberate attack.

1) The best case of deliberate attack of degree and the best case of random attack; 2The best case of deliberate attack of degree and the worst case of random attack; 3) The worst case of deliberate attack of degree and the best case of random attack; 4) The worst case of deliberate attack of degree and the worst case of random attack. The results are shown in Figure 2-2(c), Figure 2-2(d), Figure 2-2(e) and Figure 2-2 (f).




(c)

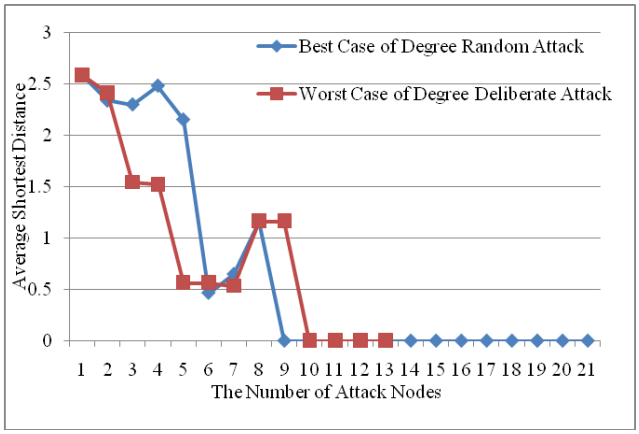
**Figure 2-2 The Best Case of Degree Random Attack and the Best Case of Degree Deliberate Attack**




(d)

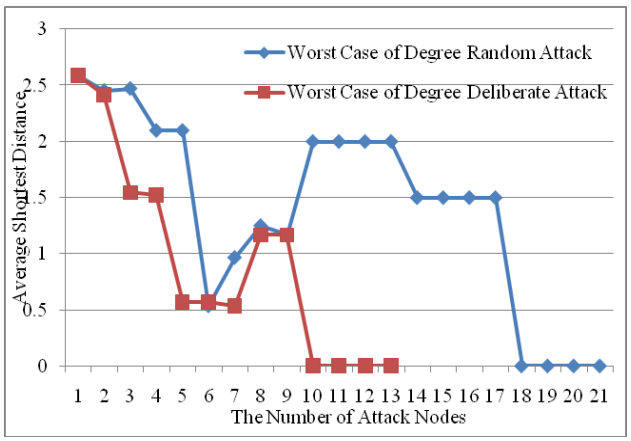
**Figure 2-2. The Worst Case of Degree Random Attack and the Best Case of Degree Deliberate Attack**


Copyright ⓒ 2015 SERSC




(e)

**Figure 2-2 The Best Case of Degree Random Attack and the Worst Case of Degree Deliberate Attack**




(f)

**Figure 2-2 . The Worst Case of Degree Random Attack and Worst Case of Degree Deliberate Attack**

We can see that the best case of deliberate attack of degree only needs to attack six nodes (the attack rate reaches 35%) will destroy the whole network, which is better than that of the best case of random attack (the attack rate is 45%); The worst case of deliberate attack of degree (the attack rate is 45%) is much better than that of the worst case of random attack (the attack rate is 80%). The worst case of deliberate attack is worse than that of random attack of degree while the best case of deliberate attack is much better than that of random attack.

(3) The experiments and results analysis of BCube

Figure 3-1 shows the network topology of BCube Architecture, which has been marked for each node. As is shown in Figure 3-1, we can get the degree and betweenness for each node. In addition, we design four group experiments for BCube.

Copyright ⓒ 2015 SERSC

**Table 1-3.Degree and Betweenness of BCube**

| Node | Degree | Betweenness |
|---|---|---|
| V1 | 4.0000 | 0.0738 |
| V2 | 4.0000 | 0.0738 |
| V3 | 4.0000 | 0.0738 |
| V4 | 4.0000 | 0.0738 |
| V5 | 4.0000 | 0.0738 |
| V6 | 4.0000 | 0.0738 |
| V7 | 4.0000 | 0.0738 |
| V8 | 4.0000 | 0.0738 |
| V9 | 2.0000 | 0.0256 |
| V10 | 2.0000 | 0.0256 |
| V11 | 2.0000 | 0.0256 |
| V12 | 2.0000 | 0.0256 |
| V13 | 2.0000 | 0.0256 |
| V14 | 2.0000 | 0.0256 |
| V15 | 2.0000 | 0.0256 |
| V16 | 2.0000 | 0.0256 |
| V17 | 2.0000 | 0.0256 |
| V18 | 2.0000 | 0.0256 |
| V19 | 2.0000 | 0.0256 |
| V20 | 2.0000 | 0.0256 |
| V21 | 2.0000 | 0.0256 |
| V22 | 2.0000 | 0.0256 |
| V23 | 2.0000 | 0.0256 |
| V24 | 2.0000 | 0.0256 |

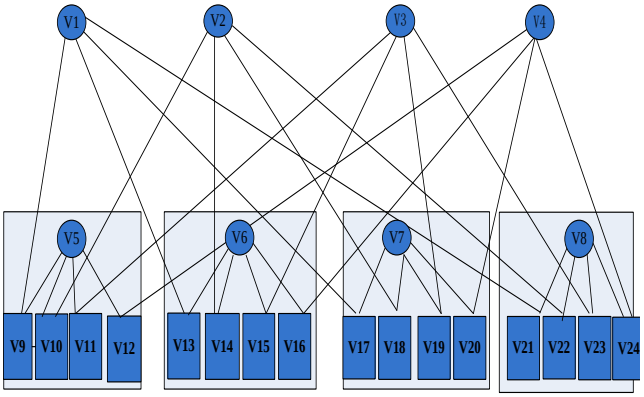
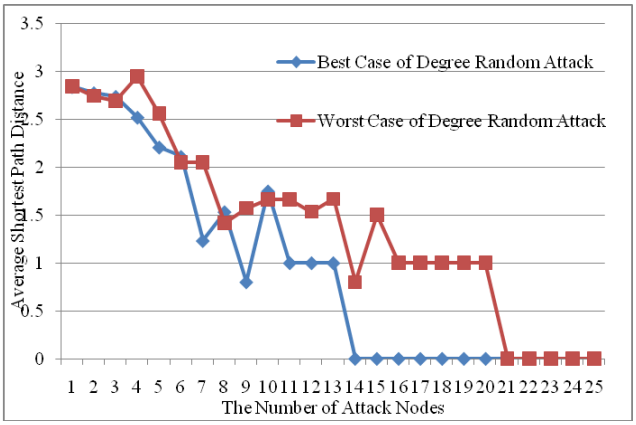



**Figure 3-1.BCube Architecture Been Marked**

Group1: The random attack of degree

As shown in Figure 3-2(a), we can see that the best case of random attack of degree only needs to attack twelve nodes (the attack rate reaches 50%) will destroy the whole network, which is better than that of the best case of random attack (the attack rate is 45%).


Copyright ⓒ 2015 SERSC

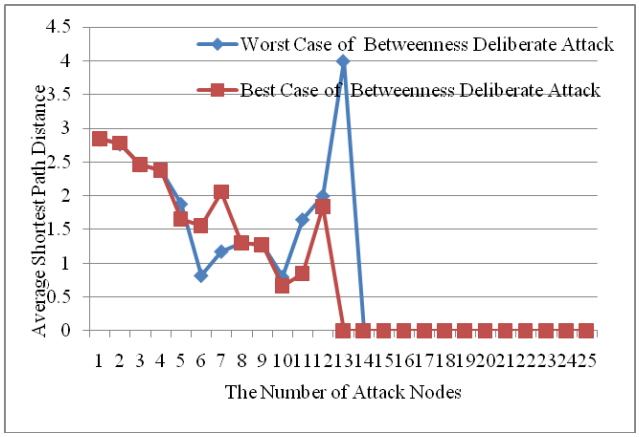



(a).

**Figure 3-2. The Degree Random Attack Experiments of BCube**

Group2: Degree of deliberate attacks comparative experiments

As shown in Figure 3-2(b), we can see that, in the ideal situation, we need to attack eleven nodes (the attack rate will be 44%), the entire network will be destroyed while we should attack twelve nodes (the attack rate will be 50%) in the worst one. All in all, the best case of degree deliberate attacks and worst case of deliberate attacks got the close effect.




(b).

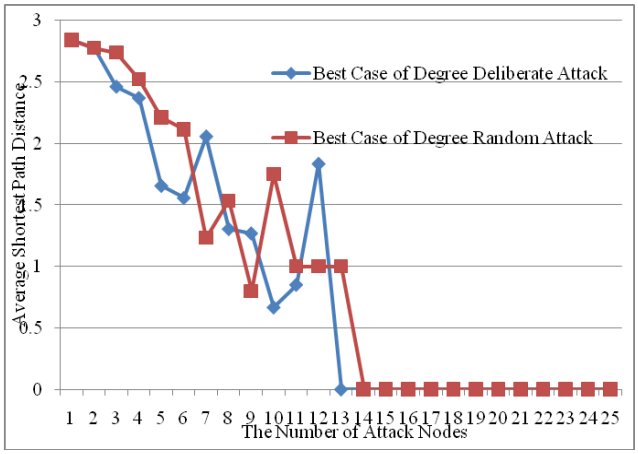
**Figure 3-2. The Degree Deliberate Attack Experiments of BCube**

Group 3: Random attack experiment and deliberate attack experiment

For BCube, we design two group experiments for the best-case degree of deliberate attack and worst case of deliberate attack.

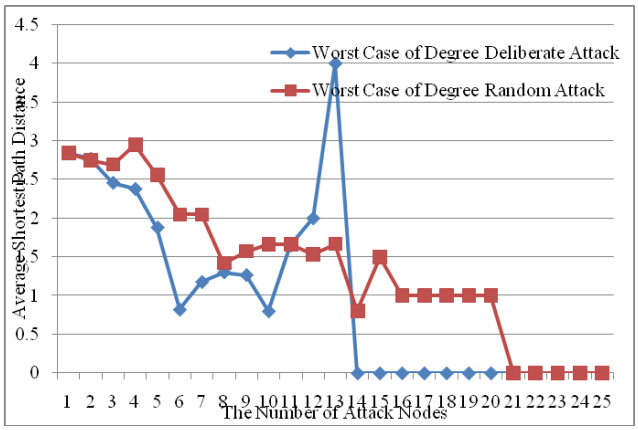
1. The best case of deliberate attack of degree and the best case of random attack; 2) The worst case of deliberate attack of degree and the worst case of random attack. The results are shown in Figure 3-2(c) and Figure 3-2(d).

Copyright ⓒ 2015 SERSC




(c).

**Figure 3-2. The Best Case of Degree Deliberate Attack and Best Case of Degree Random Attack**




(d)

**Figure 3-2 The Worst Case of Degree Deliberate Attack and Worst Case of Degree Random Attack**

We can see that the best case of deliberate attack of degree only needs to attack eleven nodes (the attack rate reaches 44%) will destroy the whole network, which is better than that of the best case of random attack (the attack rate is 50%), especially, the worst case of deliberate attack of degree (the attack rate is 50%) is much better than that of the worst case of random attack (the attack rate is 80%). All in all, the best case of deliberate attack of degree is much better than the worst case of random attack, however, the worst case of deliberate attack of degree got the close result with the best case of random attack of degree.

(4) FiConn experiment and result analysis

Figure 4-1 shows the network topology of FiConn Architecture, which has been marked for each node. As is shown in Figure 4-1, we can get the degree and betweenness for each node. In addition, we design four group experiments for FiConn.


Copyright ⓒ 2015 SERSC

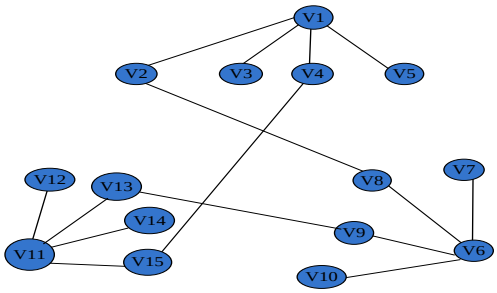


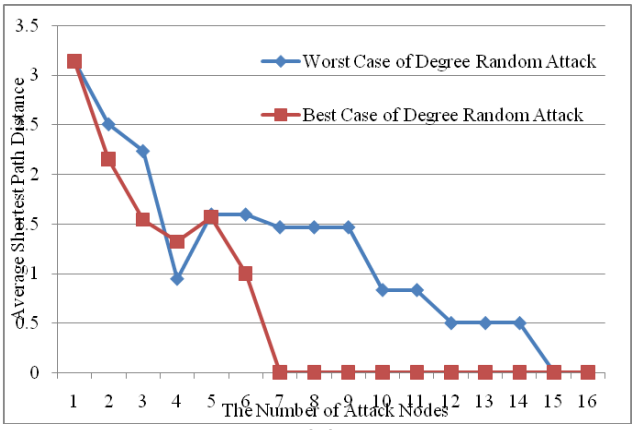

**Figure 4-1.FiConn Architecture Been Marked**

**Table 1-4.Degree and betweenness of FiConn**

| Node | Degree | Betweenness |
|---|---|---|
| V1 | 4.0000 | 0.1556 |
| V2 | 2.0000 | 0.0889 |
| V3 | 1.0000 | 0 |
| V4 | 2.0000 | 0.0889 |
| V5 | 1.0000 | 0 |
| V6 | 4.0000 | 0.1556 |
| V7 | 1.0000 | 0 |
| V8 | 2.0000 | 0.0889 |
| V9 | 2.0000 | 0.0889 |
| V10 | 1.0000 | 0 |
| V11 | 4.0000 | 0.1556 |
| V12 | 1.0000 | 0 |
| V13 | 2.0000 | 0.0889 |
| V14 | 1.0000 | 0 |
| V15 | 2.0000 | 0.0889 |

Group1: Degree random attack experiment

As shown in Figure 4-2(a), for FiConn, the best case for degree of random attack only needs to attack six nodes, which the rate of attack reaches 40%, can destroy the whole Network. However, the worst case of attack needs to attack thirteen nodes (the rate of attack is 92.8%).In summary, the former attack is much better than the latter one.




(a)

**Figure 4-2. The Degree Random Attack Experiments of FiConn**

Group 2: Degree deliberate attacks comparative experiments

As shown in Figure 4-2(b), for FiConn, the best case for degree of deliberate attack only needs to attack five nodes, which the rate of attack reaches 33%, can destroy the whole network. However, the worst case of attack needs to attack six nodes (the rate of attack is 40%).In summary the best case for degree of deliberate attack got the close result with the worst one.

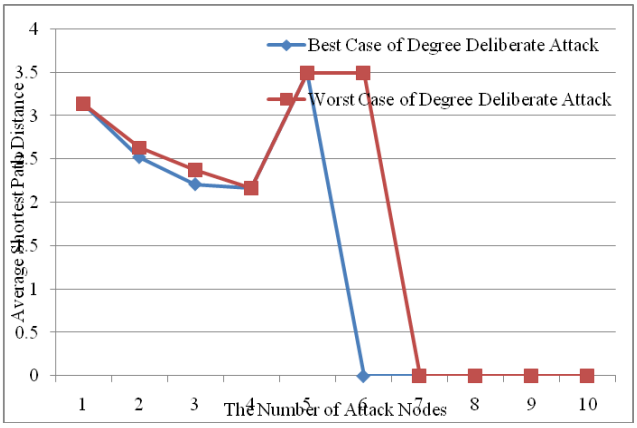
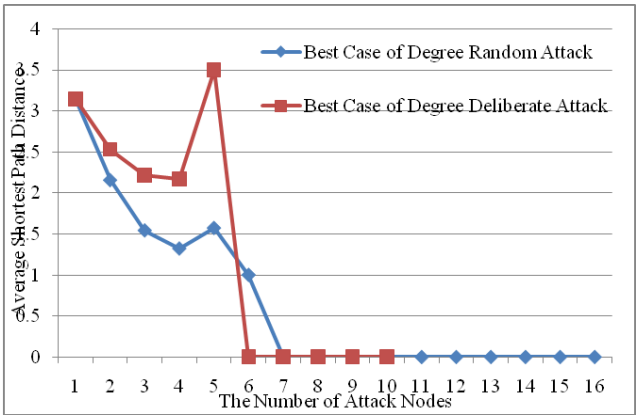



**Figure 4-2(b).The Degree Deliberate Attack Experiments of FiConn**

Group 3: Degree of random attack and degree of deliberate attack

For FiConn, the best deliberate attack of degree and the worst random attack of degree got nearly the same effect, thus we only need to design two-group experiment.

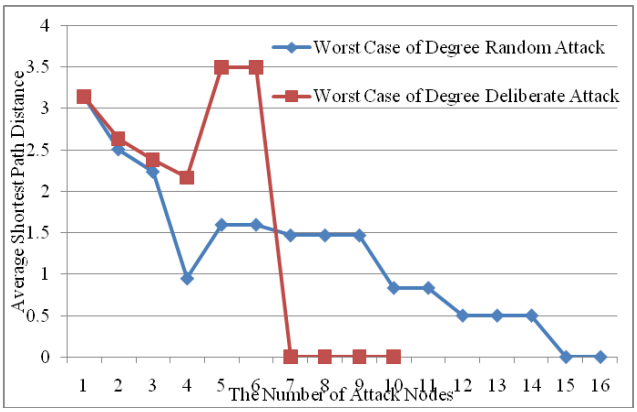
1) The average degree of deliberate attacks and best-case degree of random attack;
2) The average degree of deliberate attack and the worst degree of random attack comparison.




(c)

**Figure 4-2. The Best Case of Degree Random Attack and the Best Case of Degree Deliberate Attack**


Copyright ⓒ 2015 SERSC




(d)

**Figure 4-2. The Worst Case of Degree Random Attack and the Worst Case of Degree Deliberate Attack**

As shown in Figure 4-2(c) and Figure 4-2(d), we can see that the best case of deliberate attack of degree only needs to attack five nodes (the attack rate reaches 33%) will destroy the whole network, which is better than that of the best case of random attack (the attack rate is 40%), especially, the worst case of deliberate attack of degree (the attack rate is 40%)is much better than that of the worst case of random attack (the attack rate is 92.8%). In addition, the best case of deliberate attack of degree is much better than that of worst case of random attack while the worst case of deliberate attack of degree got the close result with best case of random attack.

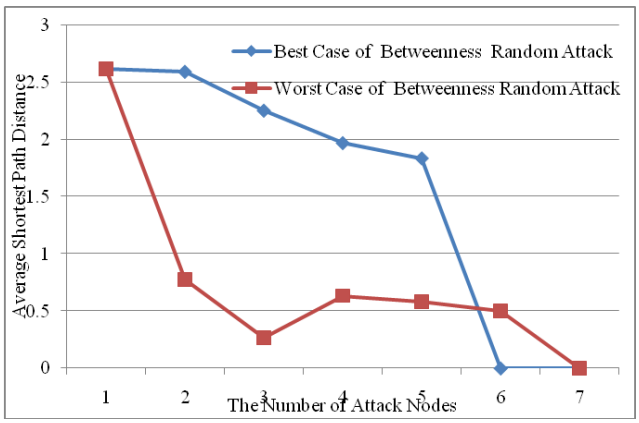
### 4.2.2. The Betweenness Attack Simulation

In this section, we will introduce betweenness attack simulation and discussion of four different architectures.

（1）The tree experiment and result analysis

Group1: The random attack of betweenness

As shown in Figure 5-1(a), for Tree, the best case of random attack of betweenness only needs to attack five nodes (the attack rate reaches 36%) to destroy the whole network while the worst case need to attack six nodes (the attack rate is 43%). Actually, they got nearly the same result.



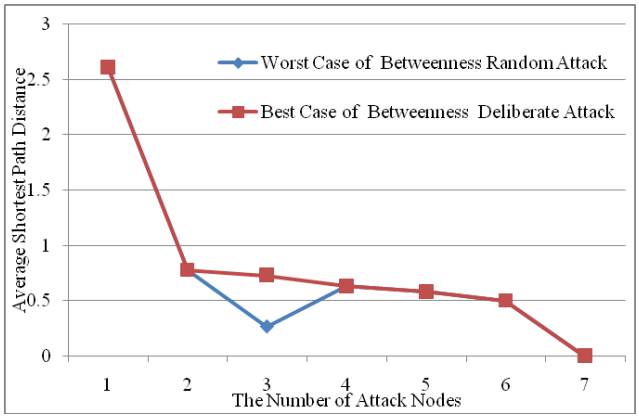

**(a)**

**Figure 5-1. The Betweenness Random Attack Experiments of Tree**

Group2: Betweenness deliberate attack experiments

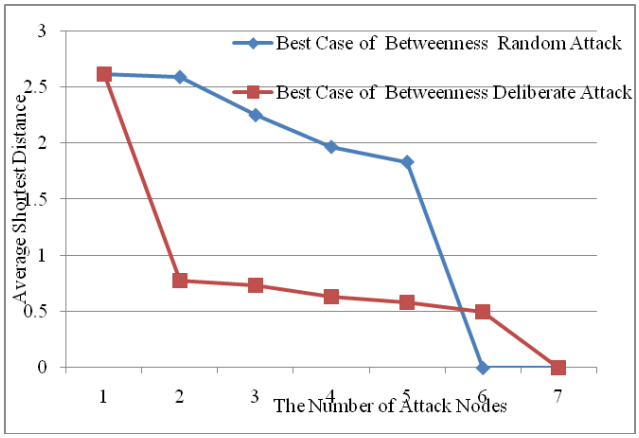
As the best case of betweenness deliberate attacks and the worst one got the close result, thus there only design two group experiments.

1) The deliberate attack of betweenness and the best case of random attack of betweenness comparative experiment;
2) The deliberate attack of betweenness and the worst case of random attack of betweenness comparative experiment.




(b)

**Figure 5-1. The Betweenness Deliberate Attack Experiments of Tree**




(c)

**Figure 5-1. The Best Case of Betweenness Random Attack and the Best Case of Betweenness Deliberate Attack**

As shown in Figure 5-1(b) and Figure 5-1(c), we can see that the deliberate attack of betweenness needs to attack six nodes (the attack rate reaches 43%) will destroy the whole network, which is worse than that of the best case of random attack (the attack rate is 36%), and get the same result with the worst case of random attack.

(2） Fat-tree experiment and result analysis

Group1: Betweenness random attack experiments

For Fat-tree, as the degree and the betweenness get the same attack range, thus the betweenness random attack experimental will get the same result with the former one.


Copyright ⓒ 2015 SERSC

Group 2: Betweenness deliberate attack experiments

The best case of betweenness deliberate attack and the worst case of betweenness deliberate attack. As shown in Figure 5-2, we can see that the best case of deliberate attack of degree only needs to attack eight nodes (the attack rate reaches 40%) will destroy the whole network, while the worst case need to attack at least eleven nodes (the attack rate is 55%).

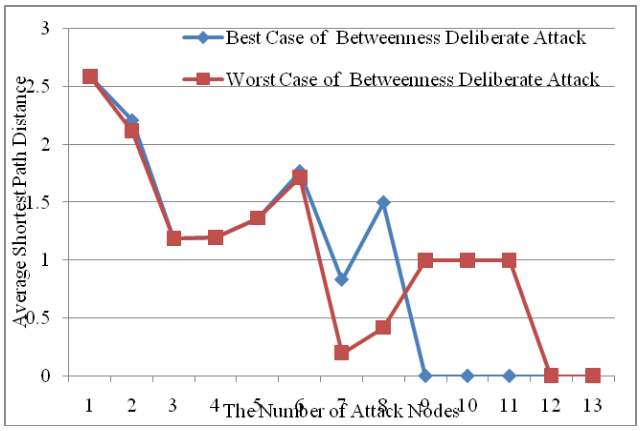



**Figure 5-2.The Betweenness Deliberate Attack Experiments of Fat-tree**

(3) The betweenness attack experiments of BCube

For BCube, as the degree and the betweenness get the same attack range, thus the betweenness random attack experimental will get the same result with the former one. Thus, there will be no more experiment here.

### 4.2.3. Degree attack and betweenness attack comparative experiments

In this section, as the degree and betweenness of nodes in BCube and FiConn got the same value, thus we only need to design experiments for Tree and Fat-tree. For each architecture, we will design two group experiments. 1) The best case of degree deliberate attack and the best case of betweenness; 2) The worst case of degree random attack and the worst case of betweenness random attack.

(1) The Tree comparative experiments

As the worst case of degree deliberate attack and the best case of degree deliberate attack got the close result, and also the betweenness deliberate attack, thus we only need to design one group experiment.

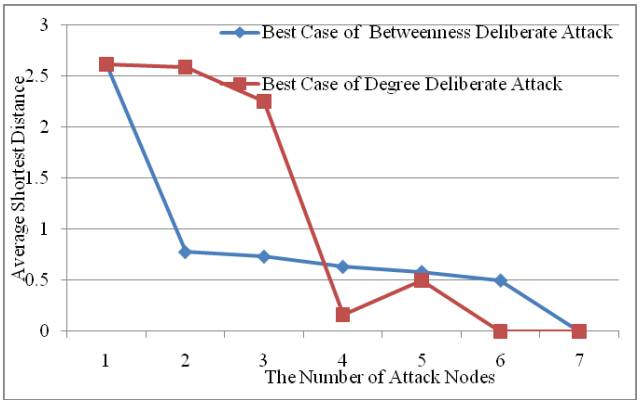


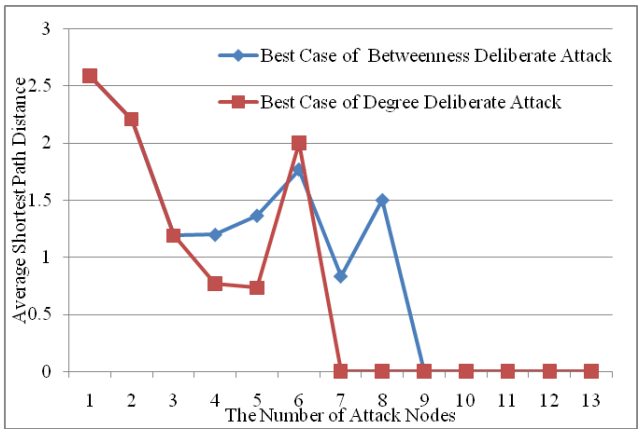

**Figure 6-1.The Best Case of Betweenness Deliberate Attack and the Best Case of Degree Deliberate Attack of Tree**

As shown in Figure 6-1, the betweenness deliberate attack need to attack six nodes while the degree deliberate attack only needs to attack five nodes to destroy the whole network. All in all, for tree, the degree deliberate attack is much better than the former.

(2) The Fat-tree comparative experiments

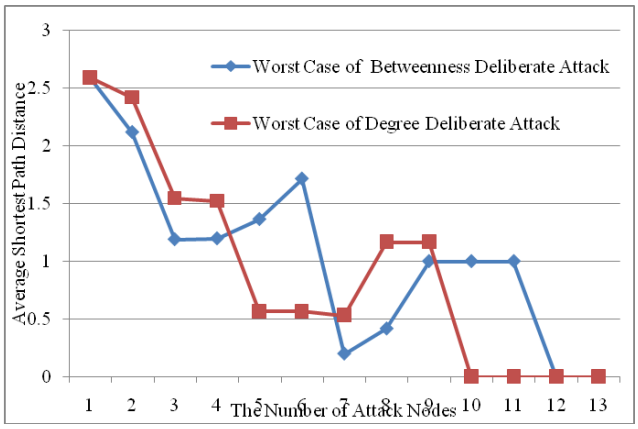
For Fat-tree, we design two group experiments.

1) The best case of degree deliberate attack and the best case of betweenness deliberate attack;
2) The worst case of degree deliberate attack and the worst case of betweenness deliberate attack




(a)

**Figure 6-2.The Best Case of Betweenness Deliberate Attack and the Best Case of Degree Deliberate Attack**




(b)

**Figure 6-2. The Worst Case of Betweenness Deliberate Attack and the Worst Case of Degree Deliberate Attack**

As shown in Figure 6-2(a), we can see that the betweenness deliberate attack needs to attack eight nodes (the attack rate reaches 40%) to destroy the whole network while the degree deliberate attack only needs to attack six nodes (the attack rate is 30%). In addition, as shown in Figure 6-2(b), the worst case of betweenness deliberate attack needs to attack eleven nodes (the attack rate is 55%) to destroy the whole network while the worst case of degree deliberate only needs to attack nine nodes (the attack rate is 45%). All in all, for Fat-tree, the degree deliberate attack is much better than that of betweenness deliberate attack.


Copyright ⓒ 2015 SERSC

## 4. Conclusion

Data center network (DCN) as the core of the cloud platform receives a significant amount of attention while the security study of DCN is still in its preliminary, especially for the vulnerability study. Differ the previous one, in this paper, we engaged in the invulnerability research from the perspective of network attack. Taking typical instances of DCN for example, based on invulnerability measurement of the average shortest path distance, we analysis the invulnerability of DCN by choosing deliberate attack and random attack. Experimental results show that for most architectures of DCN, the deliberate attacks of degree get the same result with the deliberate attacks of betweenness, especially, the deliberate attacks of degree are often harmful than betweenness attacks when attack a few nodes. However, from the perspective of random attacks, random attacks of betweenness are much harmful than degree attacks. The main contribution can be summarized as follows. We firstly engaged in the invulnerability research of DCN from the perspective of network attack and then conclude the network invulnerability of DCN by amount of experiments. The result in this paper can be widely used for the protection of DCN. In the future, we will focus on the invulnerability from the network attack of edge.

## Acknowledgements

This work is supported by Huaqiao University Phase III fund start research projects for attracting talent in 2014 (No.14BS316), Quanzhou Science and Technology Project (No.2015Z115), the Cloud Computing Platform for Internet of Things-Fujian Scientific Research Platform for Innovation (2013H2002), the Foundation for Outstanding Young Scientist in Shandong Province (No.2014BSE28044), the Fundamental Research Funds for the Central Universities (14CX02136A).

## References

[1] Y. Zhang, A. J. Su, and G. Jiang, 'Understanding datacenter network architectures in virtualized environments: A view from multi-tier applications', J. Computer Networks, vol.55, no.9, **(2011)**, pp. 2196-2208.
[2] K.Peng, H.Zou R.Lin, and F.C.Yang, 'Small business-oriented index construction of cloud data', Proceedings of 12th In Architectures for Parallel Processing, **(2012)**, September 4-7; Fukuoka, Japan, pp.156-165
[3] M.Al-Fares, A. Loukissas, and A.Vahdat, 'A scalable, commodity data center network architecture', J. ACM SIGCOMM Computer Communication Review **(2008)**, Vol.38, No.4, pp.63-74.
[4] A.Greenberg, J. R.Hamilton, N.Jain, S. Kandula, C.Kim, P.Lahiri, and S.Sengupta, 'VL2: a scalable and flexible data center network', J. ACM SIGCOMM Computer Communication Review **(2009)**, Vol.39, No. 4, pp. 51-62.
[5] C.Guo, H.Wu, K.Tan, L.Shi, Y.Zhang, and S.Lu, 'Dcell: a scalable and fault-tolerant network structure for data centers', J.ACM SIGCOMM Computer Communication Review **(2008)**. Vol.38, No. 4, pp.75-86.
[6] C.Guo, G.Lu, D.Li, H.Wu, X.Zhang, Y.Shi, T.Chen, Y.Zhang, and S.Lu, 'BCube: a high performance, server-centric network architecture for modular data centers', J.ACM SIGCOMM Computer Communication Review **(2009)**. Vol.39, No.4, pp. 63-74.
[7] D.Li, , C.Guo, H.Wu, K.Tan, Y. Zhang, and S.Lu, 'FiConn: Using backup port for server interconnection in data centers', Proceedings of 28th Conference on Computer Communications, **(2009)**, April 19-25; Rio de Janeiro, Brazil, pp. 2276-2285.
[8] C.X.Chen, 'Study on invulnerability of emergency logistics network based on complex network', J. Application Research of Computers **(2012)**, Vol.29, No.4, pp.018.
[9] K.Peng, R.Lin, B.Huang, H.Zou, and F.Yang, 'Node Importance of Data Center Network Based on Contribution Matrix of Information Entropy', J. Journal of Networks **(2013)**, Vol.8, No.6, pp.1248-1254.
[10] K.Peng, R.Lin, B.Huang, H.Zou, and F.Yang, 'Assessment of performance in Data Center Network Based on Maximum Flow'. Proceedings of HumanCom and EMC, **(2013)**, August 22-25; Taipei, Taiwan, pp. 429-439.
[11] P.Holme, B. J Kim, C. N Yoon, and S. K.Han, 'Attack vulnerability of complex networks', J. Physical Review E **(2002),** Vol.65, No.5, pp.056109.

Copyright ⓒ 2015 SERSC 

[12] R.Albert, H.Jeong H, and A.L.Barabási, 'Error and attack tolerance of complex networks', J.Nature **(2000)**, Vol.406, No.6794, pp.378-382.
[13] L.GAO, M.H.Li, and Z.R.Di, 'The robustness of attacks on vertices and edges of food webs', J. Systems Engineering—Theory & Practice **(2005)**, Vol.7, pp.1-8.
[14] Y. Zhao, Z. Wang, and X. Guo, 'Finding most vital node by node importance contribution matrix in communication networks', J. Journal of Beijing University of Aeronautics and Astronautics**(2009)**,Vol.35, pp.1076-1079.
[15] Z.H.Wang, Y.N.Han, and H.Tang, 'Resource allocation algorithms in the reconfigurable network based on network centrality and topology potential', J. Journal of China Institute of Communications **(2012)**, vol.33, no.8, pp.10-20.

## Authors

**Kai Peng**, he received his Ph.D. degree in State Key Laboratory of Networking and Switching Technology from Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2014. He is currently an assistant professor in the College of Engineering, Huaqiao University. His research interests include wireless sensor networking, IOT, cloud computing and Big Data. *The corresponding author. Email: pkbupt@gmail.com

**Binbin Huang**, she received her Ph.D. degree in State Key Laboratory of Networking and Switching Technology from Beijing University of Posts and Telecommunications (BUPT), Beijing, China, in 2014. She is currently an assistant professor in the School of Computer Science and Technology, Hangzhou Dianzi University. Her research interests include cloud computing and Big Data.

 Copyright ⓒ 2015 SERSC