Simulation of Network Effect on C4ISR System Based on Complex Network Theory

Yongjie YAN & Yan ZHANG
The 28th Research Institute of China Electronics Technology Group Corporation, Nanjing, 21007

ABSTRACT: Considering the problem about the C4ISR system architecture performance change brought by cyber attack, we present a network effect of C4ISR system simulation method based on complex network theory. Firstly, analyzing the vulnerability existing operational application and the cyber attack process against C4ISR system. Secondly, we propose the concept on C4ISR system network effect, then revealing the generation mechanism of network effect. Thirdly, the model of network effect is established based on complex network statistical character. Considering the area joint air defense system as the experiment object, the network effect experiment is developed according to different attack conditions.
KEYWORD: C4ISR System; network effect; complex network; cyber attack

1 INTRODUCTION

Currently, the integrated electronic information system is coming into an integration construction and development phase, turning to net-centric flattening network mode[1]. Due to the large size of, complexity of and dependency on C4ISR system, the security concerns are escalating. Since worldwide military countries are developing the cyberspace operation capability, our army information system will face large cyber security threat[2-4].

The cyber threats against our military integrated electronic information system separately reflect three domains, that is, physical domain, information domain and cognitive domain. In the physical domain, cyber attacks on communication network infrastructure, command and control system, weapon platform are a major concern. In the information domain, cyber attacks include that injecting false target, tampering operation application data, forging false intelligence data and command order and so on. In the cognitive domain, the purpose of cyber attack is to misdirect the commander making decision through information modification.

In this paper, to reveal the phenomena and infection for C4ISR system caused by cyber attacks, we perform three primary jobs: 1) analyzing the cyber attack mechanism against C4ISR system; 2) proposing the network effect notion and establishing the mathematical model on network based complex network theory; 3) carrying out simulation experiment about network effect. Our discussion of network effect will show what infection brought by cyber attacks.

2 THE CONCEPT AND GENERATED MECHANI- SM FOR NETWORK EFFECT

2.1 *Network effect*

The network effect of C4ISR system is meaning that system performance affected when network node, communication link and system functional units are destroyed or blocked. The performance affected includes a reduction in the integrality of network topology structure, a degradation in the efficient of system accomplishing operational task. The concept of network effect can be described as follows:

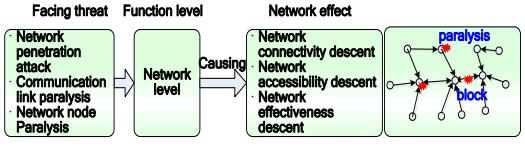


Figure 1. The concept for network effect of C4ISR system

2.2 *The generated mechanism of network effect*

According to the concept of network effect, we analyze the attack ways toward to the constituent elements of C4ISR system, such as communication unit, reconnaissance unit, command and control unit and so on. Then suggesting the attack scenario and condition in order to reveal the generated mechanism of network effect, shown in figure2.

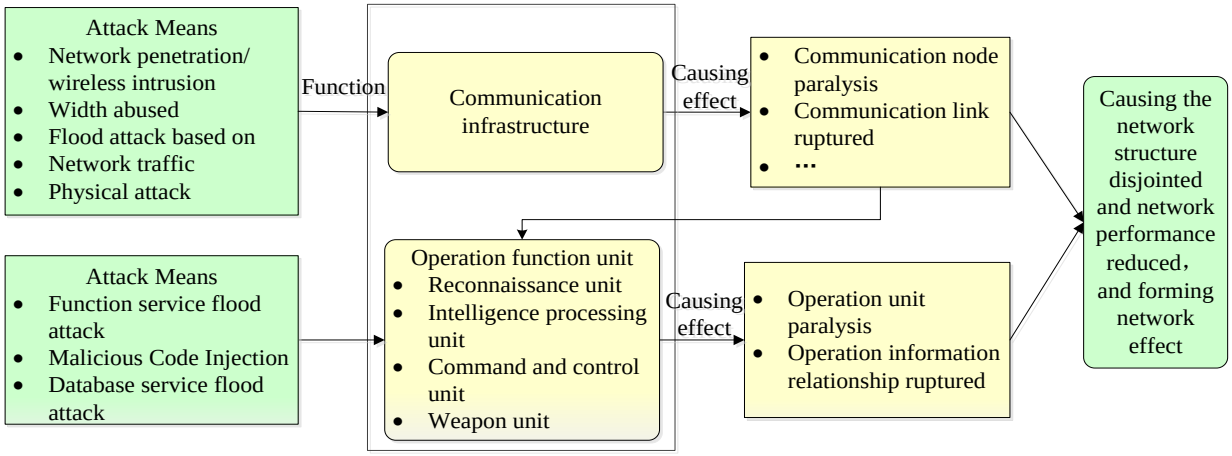


Figure 2. The generated mechanism of network effect

The communication infrastructure will face several cyber threats, including network penetration, wireless intrusion, network width abusing, traffic flood attack, virus and malicious code attack, and so on. That is due to the shortcoming of network defense measures and the vulnerability on communication protocol. Since the leak existing the OSPF or BGP route protocol, network node will be blocked and network route will be disrupted.

Also, the operation application system will face the application system penetration attack, application functional service attack, false information injection, operation order tampered and so on. Taking the intelligence processing unit for example, the intelligence processing function will be loaded and damaged under DDOS attacks, this will make the time between intelligence processing and utilizing prolong. And the bigger of attack strength, network effect of C^4ISR system is becoming more evident.

3 THE MODELING OF NETWORK EFFECT

The network effect about C^4ISR system will reflect the damaged degree of network structure， the reduction degree of system effectiveness and network communication capabilities under cyber attacks. In this research, the measurement attributes of network effect based on complex network statistical character are presented.

3.1 *The network invulnerability*

The network invulnerability is meaning that network can still maintain communication capability under the condition of network nodes and links have been deliberate attacked and random attacked. We can establish the measurement model based on network invulnerability parameters, including network connectivity, connectivity coefficient, network accessibility and efficiency.

3.2 *The model of network effect*

3.2.1 *Network connectivity*

Network connectivity is meaning that the connectivity extent about all network nodes and links, reflecting the broken extent of network structure. As the growing of network node broken, the amount of network connected component will become fewer. Then the network effect will be more evident. In this paper, we propose the following attribute parameters to measure network effect.

(1)Network structure connectivity

This index reflects the difficult degree of network structure destroyed. The definition is that least node amount required to cause network topology structure disconnected. Considering a connectivity network， we define CN_{ij} as the least node number required to separate network node i and j. And the network connectivity is defined as the minimal network cut sets denoted as CN .

$$CN = \min_{i,j}\{CN_{ij}\} \tag{1}$$

(2)The connectivity efficient of network structure

This index reflects the severity extent of network structure damaged. The compute model will be built through network connectivity component number and component node number parameters, such as follows.

$$C = \frac{1}{\omega \sum_{i=1}^{\omega}\left(\frac{N_i}{N} \times L_i\right)} \tag{2}$$

In the above, the character C is defined as network connectivity efficient, the character ω is defined as network connectivity component amount, N_i is defined as the node sum for the i th connectivity component ， N is defined as node sum， L_i is defined as the average short path for the i th connectivity component, fined as zero.

The fewer of network connectivity component and smaller of average shortest path, the better of network connectivity. When the whole network connective, then the value of C will be 1. When the

whole network node disconnected, then the value of C is 0.

(3)Network accessibility

The network accessibility $A(G)$ is defined as the average connectedness value of all network nodes, here the connectedness is meaning that the reachable path between two nodes. The calculated model about network accessibility can be expressed as follows:

$$A(G)=\frac{\sum_{i=1}^{N}A(i)}{N}$$

$$A(i)=\frac{\sum_{j=1}^{N}b_{ij-attacked}}{\sum_{j=1}^{N}\mathrm{b}_{ij-pre\_attack}} \tag{3}$$

$$b_{ij}=\begin{cases}1, node\ i\ can\ reach\ to\ node\ j\\ 0, node\ i\ cannot\ reach\ to\ node\ j\end{cases}$$

Where $A(i)$ is defined as the i th node accessibility $\mathrm{b}_{ij-pre\_attack}$ represents the connectedness of network pre-attack between node i and node j pre-attack. $b_{ij-attacked}$ represents the connectedness of network attacked between node i and j.

3.2.2 *Network efficient*

The network efficient is represented as the attack impact against on network transport performance between different nodes. Transport efficient is related to the shortest distance between nodes (i, j) denoted as ε_{ij}. Let d_{ij} represent the shortest distance between node i and j, the relationship between ε_{ij} and d_{ij} can be expressed as $\varepsilon_{ij}=1/d_{ij}$. Once there are no reachable path then $\varepsilon_{ij}=0$.The overall network efficient can be represented as follows.

$$e(G)=\frac{1}{N(N-1)}\sum_{i,j\in G}\varepsilon_{ij}=\frac{1}{N(N-1)}\sum_{i,j\in G}\frac{1}{d_{ij}} \tag{4}$$

As the number of network node and link broken is increasing during attack process, network transport efficient will incessant reduce. It indicates that the network effect will become more evident as the damaged extent of network structure enhancing.

3.2.3 *The model of network effect*

According to the representation model on network effect, we separately consider intelligence processed network, command and control network, and weapon control network as attack objects, lately establishing the network effect calculated model.

Assume that the initial network will be damaged under condition of random attack or deliberate attack pattern. Defining the remnant network as the damaged network, denoted as G', G represents the initial network. Let the initial network efficient is $e(G)$, and the damaged network efficient is $e(G')$, the network effect for the network efficient measurement index can be calculated as follows:

$$\Delta e=e(G)-e(G')=$$
$$\frac{1}{N(N-1)}\sum_{i,j\in G}\frac{1}{d_{ij}}-\frac{1}{N(N-1)}\sum_{i,j\in G'}\frac{1}{d_{ij}'} \tag{5}$$

In the formula, N represents the number of network node, $e(G)$ represents the network efficient under no attack conditions. When one node 'i' is broken, then all the other nodes connected with i will be invalidation, $d_{ij}^{'}$ is defined as the shortest path between the node i and j. According to the above definition, network effect model is separately established based on measurement indexes.

Calculated model of network effect based on network connectivity

$$\Delta CN=CN-CN'=\min_{i,j\in G}\left\{CN_{ij}\right\}-\min_{i,j\in G'}\left\{CN_{ij}^{'}\right\} \tag{6}$$

Calculated model of network effect based on network connectivity coefficient

$$\Delta C=C-C'=\frac{1}{\omega\sum_{i=1}^{\omega}\left(\frac{N_i}{N}\times L_i\right)}-\frac{1}{\omega'\sum_{i=1}^{\omega'}\left(\frac{N_i^{'}}{N}\times L_i^{'}\right)} \tag{7}$$

Calculated model of network effect based on network accessibility index

$$A(G)=\frac{\sum_{i=1}^{N}A(i)}{N} \tag{8}$$

Calculated model of network effect based on network efficient index

$$\Delta e=e(G)-e(G')$$
$$=\frac{1}{N(N-1)}\sum_{i,j\in G}\frac{1}{d_{ij}}-\frac{1}{N(N-1)}\sum_{i,j\in G'}\frac{1}{d_{ij}'} \tag{9}$$

4 NETWORK EFFECT SIMULATION

We establish the simulation frame of networked effect. The principle can be described as follows:

4.1 *Checking the important attack node*

The operation processing flow of C^4ISR system can be divided into three phases, which are the intelligence processing phase, operation command and control phase, weapon control phase. Since the operation task running process is advancing, the importance of C^4ISR system's components will be alterable. So the important attack node will not be changeless.

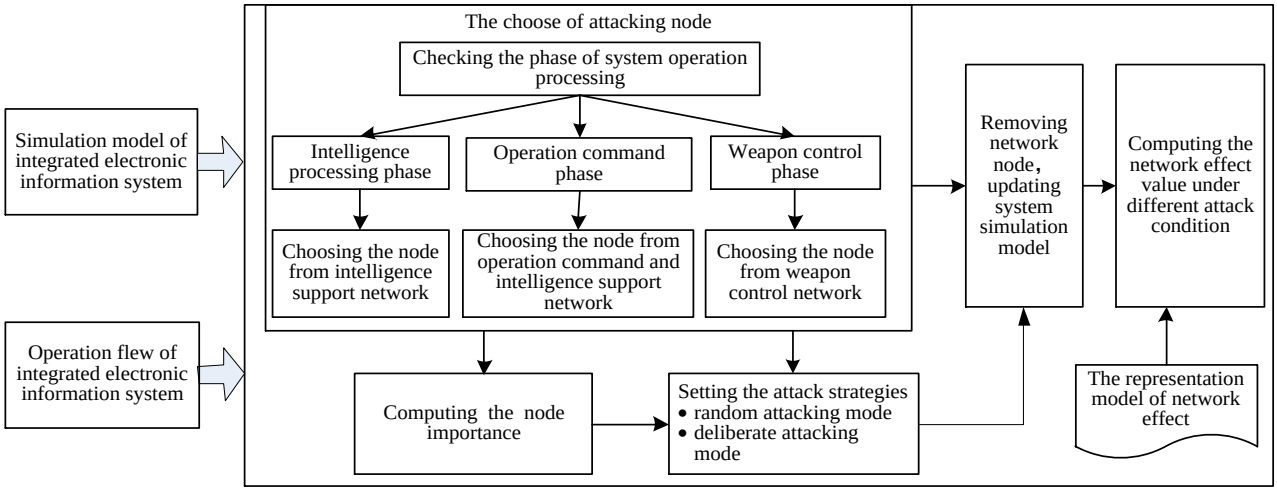


Figure 3. The simulation frame of network effect

In this paper, the important attack node will be selected through operation processing phase.

(1) In the intelligence acquirement and processing phase. We will priority choose reconnaissance unit and intelligence processing unit as the most important attack object.

(2) In the command and control phase. Intelligence analyzing and combat command decision-making will become the core operation task. So we will priority choose intelligence processing unit and command and control unit as the most important attack object.

(3) In the weapon control phase. Cooperative combat will become the main operation task, so we will priority choose weapon unit as the most important attack object.

Considering the above four types attack object, we propose node betweenness to fix on attack node. Network node betweenness refers as the node amount, which pass to the whole shortest path between different network nodes. Node betweenness can reflect important content during the process of system information transporting. The bigger node betweenness's value, the more shortest path passing to this node.

4.2 *Setting the attack mode and attack strategy*

Considering the actual combat environment, the attacker can achieve communication protocol, network topology, system vulnerability information through network detecting, network monitoring, communication reconnaissance, radar detection means. However, the security protection mechanism of C^4ISR system will make attacker difficult achieve the whole network topology information.

Assume that the communication network scale is N, the node number within known network topology area is N_1, the node number within unknown network topology area is N_2. The attack network node amount is $N \cdot f$, f represents remove rate.

The attack strategies proposed in this paper is described as follows：1) firstly adopting deliberate attacking mode to select attack node based on node's importance from the known network topology area; 2) secondly, adopting random attack mode to select attack node from the unknown network topology area.

4.3 *The simulation of network effect*

According to the above attack strategies and network effect model, respectively computing the value of network connectivity and network accessibility under different attack dense through removing different number of nodes. Then calculating the difference about the two parameters under attack condition and unattack condition in order to realize the simulation of network effect.

5 SIMULATION EXPERIMENT

5.1 Experiment condition

Taking one region combat command and control information system for example, carrying out the simulation experiment about system network effect. The constituent elements of system include four types: reconnaissance unit (34), intelligence processing unit(5), command and control unit(5), weapon unit(8).

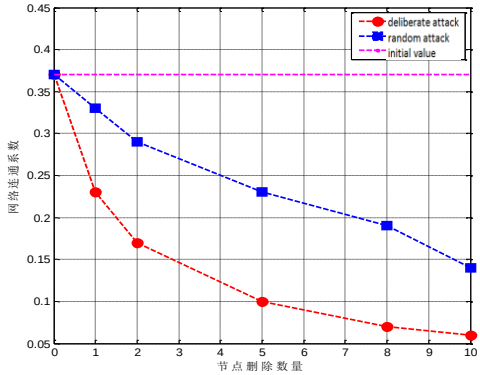
5.2 Experiment result

Setting different attack condition to calculate the value of network effect measured by network connectivity and network accessibility.

(1)Network connectivity coefficient

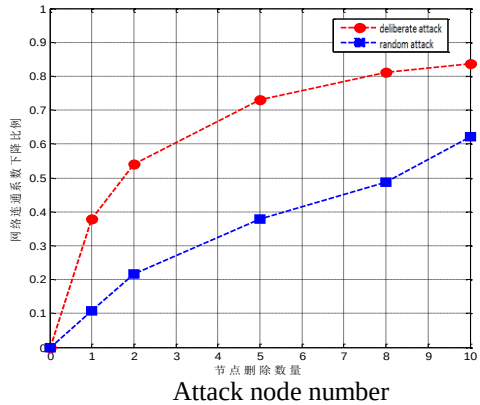
Considering the random attack and deliberate attack based on node degree, choosing system node to be attacked and calculating the reduce content for network connectivity coefficient both pre-attack and

attacked. Figure 4 and figure 5 show the change curve between network connectivity coefficient and attacked node number.



Attack node number

Figure 4. The relationship between the network connectivity and attacking node number

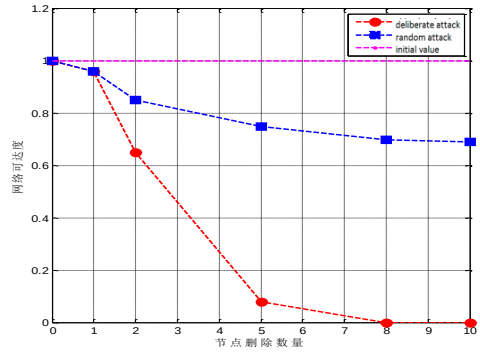


Attack node number

Figure 5. The relationship between network connectivity coefficient reducing rate and attacking node number

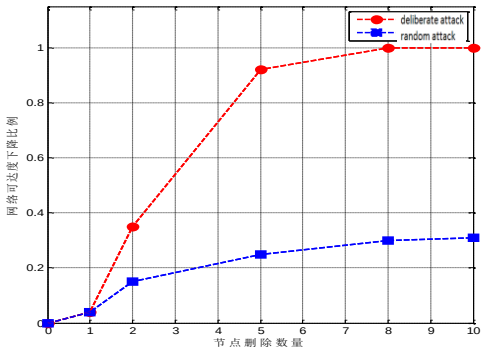
(2)Network accessibility

Similarly, Considering the above two attack patterns，calculating the reduce content for network accessibility both pre-attack and attacked. Figure 6 and figure 7 show the change curve between network accessibility and attacked node number.



Attack node number

Figure 6. The relationship between network accessibility and attacking node number



Attack node number

Figure 7. The relationship between network accessibility coefficient reducing rate and attacking node number

Through the above experiment, we can conclude that the network effect simulation approach proposed will efficiency reflect the network effect transformation trend under the condition of cyber offense. And network effect can be quality measured through network connectivity, network accessibility, network transport efficient.

6 CONCLUSION

The mechanism of network effect for C^4ISR information system generated is proposed from the cyber offensive and defense view in this paper. And the effect modeling is established and simulation analyzed based on complex network theory. This approach will bring an important mean to quantify analyze the effect content about the cyber attack threat to military information system. In the future research, we will focus on the defense frame and mechanism about C^4ISR information system under the condition of cyber offensive activity.

REFERENCES

[1] Zhang Gangning & Yi Kan, etc. Service-Oriented Architecture and Realization Methods of Netwrok-Centric C^4ISR System. Command Information System and Technology, 2013, 4(6):42-47.

[2] FAN Ai-feng & CHENG Qi-yue. Analyzing Threat and Challenge in Cyberspace. Fire Control & Command Control, 2013, 38(4):1-4.

[3] Zhou Guangxia & Sun Xin. Study on Cyberspace Operations. Command Information System and Technology, 2012, 3(2): 6-10.

[4] ZHANG Lu & HONG Liang. Research of Cyberspace Countermeasure Based on Information Technology. Computer Technology and Development, 2014, 24(6): 208- 210.

[5] WANG Xin & YAO Pei-yang, etc. Research on Command Information System Invulnerability in Network-Centric Warfare. Computer Engineering, 2011, 37(5):97-100.

[6] WANG Chang-chun & CHEN Jun-liang, etc. Modeling and simulation of combat systems paralysis based on complex network. Journal of System Simulation, 2012, 24(7): 1491- 1495.