Reliability evaluation of command information system under different attack modes

Guohui Jia¹, Jie Zhou¹ and Junyi Li²

¹ Information and Communication Institute, National University of Defense Technology, Wuhan, China
² Communications Division, China Electronics Technology Group Corporation (CETC) 20th institute, Xian, China

E-mail: zhoujie8912@163.com

Abstract. Based on the basic structure of the typical command information system network, the model has been divided into physical layer and information layer. According to the whole network efficiency and reliability, five functional characteristics quantity are selected as the reliability evaluation indexes when the system is attacked randomly or deliberately. With the model we established, reliability changes of the constructed system are compared of different attack modes. The results provide evidence that the system reliability change obviously in different attack modes which should be special focused in practical application.

1. Introduction
Command information system (CIS) is a computer-based military information system [1-3], which has the functions of command and control, reconnaissance and early warning, communication, attack and other operational information support. It has become the basic support and important pivot of system operations. The improvement of the degree of network, on the one hand, has multiplied the effectiveness of the command information system. However, at the same time, it also makes the system face more serious failure risk [4]. Therefore, it is of great significance to study the failure characteristics of command information system under different attack modes for improving the reliability of the system itself and maintaining the competitive advantage in the system confrontation. At present, there are few researches on the reliability evaluation of command information system, most of which use the complex network invulnerability to measure the robustness based on the underlying network communication structure [5-6], but the combination with the actual application field is not close enough. In order to provide a theoretical support for the system practical application, the method of command information system reliability evaluation should be studied to ensure the system in guaranteed functionality.

Based on the analysis of the structure characteristics of command information system, this paper divided the system function into physical layer and information layer, establish the system reliability evaluation model with several specific indexes, and evaluates the system reliability with a certain command system as an example considering the influence of different attack modes.

2. Basic structure of command information system
Command information system is composed of reconnaissance intelligence system, fire attack system, command and control system, integrated support system, and integrated with a variety of
Communication networks, functional networks and business systems. It is an important support for system operations under the information condition. Because there are many kinds of relationships among the elements of CIS, such as information communication, command and control, cooperative support and so on. It is necessary to construct a multi-layer network model to describe the elements and relationships in CIS from different perspectives. And because information communication is the basis of the system of the combat elements, command and control, cooperative support and other relationships are based on communication, around the combat task and business relationship and further abstracted logical connection. Therefore, CIS can be regarded as a network model composed of physical layer network and logical layer network coupling.

![Figure 1. The physical layer and information layer of CIS](image)

### 2.1. The physical layer of CIS
The physical layer network GP is an undirected weighted network expressed as. It represents the set of entity nodes, corresponding to entity combat units, such as radar, fighter, anti-aircraft cluster, etc. Represents the set of edges, corresponding to the communication links between entity nodes, such as wireless communication links, satellite communication links, etc. Represents the set of edge weights, which is used to represent the number of types of communication links between nodes.

### 2.2. The information layer of CIS
The physical layer network GL is also an undirected weighted network, expressed as. Among them is the function node set, which is obtained from the physical layer entity node mapping. The set of representation edges corresponds to the information interaction between function nodes, such as command information interaction, collaborative information interaction, etc. It represents the set of edge weights and the amount of information interaction between nodes under a certain task.

### 3. Reliability modelling of CIS
#### 3.1. Reliability indexes construction

##### 3.1.1 Physical unit stability
Define the physical unit stability index as $B_1$, which reflects the ability to withstand the external threat attack of the physical layer unit of the command information system. This index is generated by a variety of protection attributes of the entity node. It can be measured directly by the attack intensity and duration of the attack.

Assume that the node is destroyed at any time, then the attack duration is

$$t^{Vi} = t_s - t_0 \quad (1)$$
3.1.2 Connection retention ability

The connection retention capability $B_2$ reflects the connectivity, accessibility and integrity retention capability of the functional network structure of the system. The connection relationship of command information system refers to the information relationship established on the basis of communication connection, which is directly related to the connection state between function node pairs.

It is assumed that in 0-$t$ time, the $(V_i, V_j)$ means functional node pairs that has been established connection relationship, the relationship can be expressed as $e_{V,V}$, then the probability of remains connected can be expressed as

$$H_{e_{V,V}}(t) = e^{-\int_0^t f(s) ds}$$

(3)

The probability of disconnection is expressed by $f(s)$, it can be expressed by the time taken by the node to change the connection relationship after the system is attacked

$$H_{e_{V,V}}(t) = e^{-\theta,s}$$

(4)

Where $\theta$ is the adjustment coefficient, $t_s$ is the time required for the information reachability to fall to the threshold, and the larger $t$ can get the better system structure retention ability. Then $B_2$ can be expressed as:

$$B_2 = \prod_{V_i, V_j \in \mathcal{V}} \left[H_{e_{V,V}}(t)\right]$$

(5)

3.1.3 System sensitivity

The system sensitivity $B_3$ reflects the change of combat information support ability and the number of information function chains in the available function network after the command information system is attacked. The lower the sensitivity $F(t)$ of the system to the attack, the stronger the system function tolerance.

When the command information system carries out the task, the function network set is $G_f(t) = \{V(t), E(t)\}$ and the evolved from the function network function is defined as $G_F = G_F = \{G_{F_1}, G_{F_2}, \cdots, G_{F_m}\}$. If the number of information function chains in the function network changes (the number changed from $N_{F_i}$ to $N_{F_i}'$) after the system is attacked,

$$F(t) = \frac{\sum_{i=1}^{m} |N_{F_i} - N_{F_i}'|}{\sum_{i=1}^{m} N_{F_i}}$$

(6)

Define $\eta$ as the adjust coefficient, the system function tolerance $B_3$ can be expressed as

$$B_3 = e^{-\eta \int_0^t e^{F(t)}}$$

(7)

3.1.4 Backup unit replacement capability
The backup unit replacement capability $B_4$ measures the ability of system redundant backup resources to quickly inherit the functions of damaged units. The unit replacement includes the process of configuration unit functional parameters, identity security authentication, no difference integration, etc.

If there are $m$ units to be configured in the system and the unit configuration time is $\Delta t_i$, then the system backup unit configuration time $T_C$ is

$$T_C = \sum_{i=1}^{m} \Delta t_i \quad (8)$$

Set the time when the backup unit successfully accesses the system as $T_i$, the $T_i$ is the random variable in the time period $(t_0, t_e)$. When the unit completes the configuration, the intervention request will be sent to the system. When the information system successfully intervenes in the backup unit within the unit time of adjusting time $t$, the number of backup units within the unit time is $r(t)$, and the intervention success rate of the backup unit within the unit time is

$$R_c = P[T_i \leq t] = 1 - P[T_i > t] = 1 - e^{-\mu t} \quad (9)$$

Define $\mu$ as regulation parameter, $B_4$ can be expressed as:

$$B_4 = R_c \cdot e^{-\mu t_c} \quad (10)$$

### 3.1.5 System response effectiveness

System response effectiveness $B_5$ reflects the efficiency of information system response to threat risk, which can be obtained by measuring the average response time of the system. System response time refers to the time interval between the threat perception and response measures taken by the command information system. The average response time of the system to perceive $n$ threats in time period $T_A$ is

$$\bar{t} = \frac{1}{n} \sum_{i=1}^{n} (t_i^* - t_i^0) \quad (11)$$

$t_i^0$ is the time of system perceived threats, $t_i^*$ is the threat response time, the system response effectiveness is:

$$B_5 = \exp[-k(\bar{t} + t^*)] \quad (12)$$

$k > 0$ is the adjustment coefficient, $t^*$ is the network delay time.

### 3.2. Reliability modeling based on index combination

In the reliability evaluation of information system, we need to consider the relationship between the physical layer indexes and the information layer indexes. In order to combine the reliability evaluation index, considering the non-homogeneous characteristics of index types, we adopt the non-linear aggregation method of weighted product and weighted sum to evaluate the reliability of command information system as a whole. The cooperative indexes are relatively equal and independent, which is suitable for the weighting and aggregation method of aggregating the complementary and cooperative indexes.

Here, $B_1$ and $B_2$ are set as cooperative indicators, which are represented by weighting and aggregation $B_4 \oplus B_2$. There is a strong correlation between dependent indexes, and each index has an indispensable importance to superior indexes, which is suitable for the weighted product aggregation method considering complete characteristics. Here, $B_3$, $B_4$, and $B_5$ are set as cooperative indexes, which are expressed by weighting and aggregation $B_3 \bigodot B_4 \bigodot B_5$. With the different indexes, we can get the reliability model as

$$R = \mu_1 B_1 + \mu_2 B_2 + \mu_3 B_3 \cdot \mu_4 B_4 \cdot \mu_5 B_5 \quad (13)$$
\[ \mu_1 + \mu_2 + \mu_3 + \mu_4 + \mu_5 = 1 \]  \hspace{1cm} (14)

4. Evaluation of reliability in different attack modes of CIS

It is assumed that the elements of networked command information system of joint air defense in a certain area are as follows:

**Table 1.** The unit composition of a certain CIS

| System element                      | Node type                        | Node label |
|-------------------------------------|----------------------------------|------------|
| scout unit                          | node type                        | node label |
| radar unit                          | information acquisition node     | \( V_I \)  |
| search unit                         |                                  | \( V_J \)  |
| search information processing       | information processing node      | \( V_P \)  |
| radar information processing        |                                  | \( V_P \)  |
| Regional command and control        | command decision node            | \( V_D \)  |
| radar command and control           |                                  | \( V_D \)  |
| union command and control           |                                  | \( V_D \)  |
| fire launch                         | Implement node                   | \( V_A \)  |
| electronic countermeasure           |                                  | \( V_A \)  |
| weapon interception                 |                                  | \( V_A \)  |

It is assumed that the elements of networked command information system of joint air defense in a certain area are as follows:

![Figure 2. The network structure of the certain CIS](image)

4.1. Reliability evaluation in random attack mode

Taking the bearing capacity index \( B_1 \) and the replacement capacity index \( B_4 \) of backup unit as examples to explain the calculation process of the index. According to the data in the table 2, the survival time of the attacked node can be calculated. Combined with the coefficient \( \gamma \), the bearing...
capacity index $B_1$ can be obtained. Combined with the data, define the configuration time to get the backup unit of the system as $B_4$. According to the system parameters and expert opinions to get the replacement capacity index $B_4$ of the backup unit.

**Table 2. The results of random attack mode**

|       | $V_{I1}$ | $V_{P1}$ | $V_{D1}$ | $V_{A1}$ |
|-------|----------|----------|----------|----------|
| $\sigma^V$ | 4.3      | 3.6      | 2.8      | 4.8      |
| $t_0$       | 40       | 45       | 200      | 300      |
| $t_s$       | 60       | 65       | 350      | 450      |

After getting the index value, the next step is to study the index weight. The index weight is generally determined by the system design expert according to the characteristics of the system. Combined with the characteristics of this action, the index weight is determined as follows:

**Table 3. The weight value of the indexes in the reliability evaluation model**

|       | $\mu_1$ | $\mu_2$ | $\mu_3$ | $\mu_4$ | $\mu_5$ |
|-------|----------|----------|----------|----------|----------|
| weight value | 0.2      | 0.3      | 0.15     | 0.15     | 0.2      |

According to the data in the table 3, the reliability index of four nodes under random attack is calculated. The number of attacked nodes can be expanded to calculate the system reliability under different number of attacked nodes, as shown in the following figure 3.

**Figure 3. The reliability evaluation result of random attack mode**

**4.2. Reliability evaluation in deliberately attack mode**

Different from the random attack mode, the way of deliberately attack is to attack the key nodes of command information system. Here, the number of nodes is also selected as 4, and the attack situation in deliberately attack mode is shown in the table 4.

**Table 4. The results of deliberately attack mode**

|       | $V_{I3}$ | $V_{P3}$ | $V_{D3}$ | $V_{A3}$ |
|-------|----------|----------|----------|----------|
| $\sigma^V$ | 8.2      | 9.6      | 6.2      | 6.5      |
| $t_0$   | 80       | 75       | 420      | 400      |
| $t_s$   | 90       | 95       | 510      | 630      |

In order to ensure comparability, coefficient weight under random attack mode in 4.1 is adopted to define the weight of each index, and the number of node attacks is gradually increased. The reliability evaluation result under deliberately attack is shown in the figure 4.
From the reliability evaluation values of deliberately attack mode, the reliability values change rapidly with the increase of the attacked point proportion. When the proportion reaches to 25%, the reliability value is 0 which means the command information system has lost the communication capability completely. Compared with figure 3, we can find that the different attack modes have an enormous impact on the reliability of command information system which should be considered in practical application.

5. Conclusion
In this paper, the typical structure of command information system has been studied with the basic principle of complex network, a typical command information system model is established, and several kinds of indexes affecting the reliability of the system are given and the corresponding index weight values are determined. Based on different attack modes, the reliability values of the command information system are evaluated by the model. The results show that when the number of attacked nodes reaches 70% in random attack mode, the system basically loses the communication ability. However, when the number of deliberately attack nodes reaches to 25%, the whole network model basically loses the communication ability. This result can be applied for certain command information system to formulate defensive strategy under different attack modes.

References
[1] Lan Y, Mao S and Wang H. 2015 Theory and optimization of C4ISR system structure (Beijing: National Defence Industry Press)
[2] Kim D H and Motter A E 2008 Resource allocation pattern in infrastructure networks. Journal of Physics A Mathematical & Theoretical. 41 (22) 4539
[3] Lao S, Wang J and Bai L 2016 Review of the interdependent networks Journal of National University of Defense Technology 38(01) 122-8
[4] Guo C, Wang L, Li Y and et al 2012 Study on network cascading failures based on Load-capacity model Journal of Computer Research & Development 49 (12) 2529-38
[5] Hong C, Zhang J, Du W B and et al 2016 Cascading failures with local load redistribution in interdependent Watts–Strogatz networks. International Journal of Modern Physics C 27(11) 1650131
[6] Hao Y, Li C and Wei L 2018 Cascading failure model of complex networks considering overloaded nodes System Engineering and Electronics 40(10) 2282-87