Research on optimal control model of complex networks security risk

Jizhen Li1,2*, Baofeng Ren1, Tiantian Zhang1, Chaowei Li1, Zihao Liu1

1 State Key Laboratory of Astronautic Dynamic, China Xi’an Satellite Control Center, Xi’an, Shanxi, 710043, China
2 Information and Navigation College, Air Force Engineering University, Xi’an, Shanxi, 710077, China
*Corresponding author’s e-mail: lijizhen1986@126.com

Abstract. To solve the problems such as the security risk control and the optimization of the complex networks, an optimal control model of complex networks security risk based on discrete glowworm swarm optimization with key strategy adjustment is proposed. The basic framework of this model is built based on four functional modules including detection and evaluation, strategy selection, control optimization and performance feedback. The optimal evaluation criterions of the security control strategy are constituted of factors such as control cost, benefit reward and negative effect. The discrete glowworm swarm optimization algorithm with key strategy adjustment is proposed to search for the optimal control strategy of complex network security risk. The concept of control parameter is introduced, whose feedback and adjustment make the optimal control model get evolutionary. Finally, the model and the algorithm are tested for network security risk optimal control in the Nearest Neighbor coupled with network, Erdos-Renyi random graph network, Watts-Strogatz small world network and Barabasi-Albert power law network, separately. The availability of the model and the superiority of the algorithm are validated and the effect of the change for the attack strategy to the security risk optimal control model is analyzed by simulations.

1. Introduction

With the development of computer networks, networks security risk control is gradually developed [1] and has been an important part of networks security management. Networks security risk control means taking appropriate safety control measures, regulating and controlling the security properties of the network data and information, to reduce the probability of risk events and loss degree of risk, and protect the data information value and control security specification of the network [2]. In recent years, the research on complex networks has gradually emerged [3]. Security risk control is also the focus of the research on complex networks[4], among which the structure and behavior control is the core of complex networks security control.

Up to now, few related studies have been seen. As for the foreign research: in 1970s, the U.S. published the earliest computer security control report and opened the preface of networks security management and control research; in 2001, in the process of planning the architecture of the Global Command and Control System(GCCS), an important part of the Global Information Grid(GIG), the U.S. military put forward the solution to enhance the system security and the ability to survive; in 2002, the American National Institute of Standards and Technology (NIST) put forward a security risk mitigation and control method based on the cost-benefit analysis; in 2006, the U.S. issued the USA...
Network Security and Information Assurance Research Plan and put forward guidance on networks security control; in 2011, NIST released Guidelines for Information Security Risk Management to further provide guidance on networks security control and so on. Relevant domestic research started late: On the basis of the research of P²DR model, Liu Jingxue put forward SCP²DR² model, which constituted a dynamic and compete security cycle; Fan Hong and Feng Dengue and others of Chinese Academy of Sciences proposed information security risk management framework including six processes such as risk control. Building an integrated networks security control system and achieving the optimal control of networks security have become an urgent need to improve networks security[5].

The optimal control of complex networks security refers to selecting the optimal one among many security control strategies to achieve the goal of optimal control of networks security [6]. Aiming at the above problems, related studies are carried out as follows in this paper: Firstly, the optimal control model of complex networks security risk is established; Secondly, the host-based and networks-based security defense control strategies are formulated and selected; Thirdly, the optimization evaluation criterion of security defense control strategy is constructed. Fourthly, Discrete Glowworm Swarm Optimization with Key Strategy Adjustment (KSA-DGSO) is proposed and used to obtain the optimal security control strategy. Finally, to verify the effectiveness of the optimal control model of the complex networks security risk and the superiority of KSA-DGSO algorithm, the proposed model and algorithm are tested under four typical complex networks conditions: The nearest neighbor coupled with NC network, random ER network, small-world WS network and scale-free BA network.

2. Optimal control model of complex networks security risk

Research on the optimal control model of complex networks security risk will help to enhance the security and stability of complex networks [7]. To control the structural and behavioral security risks of complex networks, Firstly statistical analysis of all kinds of networks security log and security event information need to be carried out, and then the networks security risks should be evaluated in real time and accurately. Secondly, according to the requirements of security control and assessment results of security, a series of security control strategy should be formulated. Then the optimal security control strategy should be obtained through the intelligent optimization method, thus legal networks behavior will be protected more effectively, abnormal behaviors such as network attacks are contained, optimal control of complex networks security risks is obtained, and the overall networks security and stability are improved[8]. In the end, according to the implementation effect of the security control strategy, the model and related control parameters are adjusted, which makes the security optimal control model evolve continuously. Based on the requirements above, an optimal control model of complex networks security risk based on discrete glowworm swarm optimization with key strategy adjustment is proposed. The model which will be referred to as the DSCP model hereinafter includes four functional modules: Detection and evaluation module, Strategy selection module, Control optimization module and Performance feedback module.

2.1. Networks security risks detection and evaluation

Detection and evaluation module mainly includes collection and detection of the networks security data, SSUT index classification system, networks security risks assessment, and etc. Networks security risk assessment is the basis of networks security control, which is based on series of raw data representing networks security situation. This raw data needs to be detected and collected by some tools and software installed on related hosts, such as host monitoring software, vulnerability scanner, log analysis software, simple network management software and related commands. Networks security situation analysis is a long-term continuous process with sudden characteristics, to simplify the analysis, in this paper, network security situation data is sampled and analyzed by equal time interval sampling method. In addition, the conventional safety index is reclassified into: internal safety index(Safety), which emphasizes the reliability of the network system and the host itself; external security index(Security), which emphasizes the level of protection against external attacks of the network system and host; user type index(User-Type), which emphasizes user’s personalized demand
for networks security and determines the weights of influencing factors of various indexes. The index system composed of three types of security indexes such as Safety, Security and User-Type is referred to as SSUT index system [9]. The contents of SSUT index system are as shown in table 1.

### Table 1. SSUT index system

| Classes                | Name                              | ID | Influence factor |
|------------------------|-----------------------------------|----|-----------------|
| **Internal safety**    | Safety index                       |    |                 |
|                        | CPU usage                          | $S_{a1}$ | $R_1$           |
|                        | Hard disk usage                    | $S_{a2}$ | $R_2$           |
|                        | Memory usage                       | $S_{a3}$ | $R_3$           |
|                        | Support number of concurrent links | $S_{a4}$ | $R_4$           |
|                        | Number of open ports               | $S_{a5}$ | $R_5$           |
|                        | Average port traffic               | $S_{a6}$ | $R_6$           |
|                        | Number of safety equipment         | $S_{a7}$ | $R_7$           |
|                        | Number of backup devices           | $S_{a8}$ | $R_8$           |
| **External security**  | Security index                     |    |                 |
|                        | Number of vulnerabilities          | $S_{e1}$ | $T_1$           |
|                        | Average vulnerabilities risk level  | $S_{e2}$ | $T_2$           |
|                        | Patch timeliness                   | $S_{e3}$ | $T_3$           |
|                        | Patch quality                      | $S_{e4}$ | $T_4$           |
|                        | Frequency of security incidents     | $S_{e5}$ | $T_5$           |
|                        | Mean time to failure               | $S_{e6}$ | $T_6$           |

The original data collected in the networks are pre-processed, normalized and then classified according to the SSUT index system. Next the user type index User-Type is determined according to the source of the original data and different impact factors are given to each security index. Networks security situation value is calculated through the following formula:

$$ S = \sum_{i} (S_{a_i} \times R_i) + \sum_{i} (S_{e_i} \times T_i) , \text{ and } \sum_{i} R_i = 1 , \sum_{i} T_i = 1 $$

(1)

after the normalization of the original data, $S \in [0, 1]$, and the smaller $S$ value is, the higher the information system networks security is.

### 2.2 Formulation and selection of security control strategies

At present, networks security protection measures and products are numerous. However, this kind of safety protection measures and products have strong pertinence, only when the corresponding safety event occurred, it will response and stop the security incidents from further expansion. But security incidents mostly have a definite latency period, during which the networks security data information will take slight changes, which this kind of protective measures and products will be difficult to detect. When the security threat is perceived, the network may have already be harmed. Therefore, evaluating the overall situation according to the networks security data information and implementing security risk control measures according to assessment results are feasible ways to ensure the security of network.

In addition to the traditional access control, the intrusion detection control, encryption control, disaster recovery backup control and so on, it is also urgent to try to start from the actual networks security defense control strategy [10]. According to the requirements of complex networks security control strategy and reference [11], the strategy selection module plans the security control based on structure and behavior as the host-based and networks-based security defense control strategy, and then the composite security control strategy set can be constructed. In this paper, in order to simplify the analysis, five representative subclasses were selected from the host-based and networks-based security defense control strategy for research and analysis. The detailed subclasses and descriptions are shown in table 2.
In this paper, there are three main evaluation indicators to measure the quality of network security control strategies including the control cost, the benefit reward and the negative effect. The definitions and calculation methods of each index are detailed as follows.

**Definition 1: Control cost (Cc)**. Control cost refers to the cost consumed when the security control strategy itself is operated and executed, which mainly includes the consumption of response time and computing space. For the convenience of analysis, in this paper, the cost of control strategies are divided into three levels: low, medium and high, respectively representing occupying very little, less and more resources, and the magnitude of the corresponding control costs are set to 10, 20 and 30, respectively. The table (Table 3) shows the control cost of each strategy. Therefore, the total cost of the security control strategy is \( Cc = 10 \times D_1 + 20 \times (D_1 + D_2 + D_3 + D_4 + D_5 + D_6 + D_7 + D_8 + D_9 + D_{10}) + 30 \times D_7 \).

**Definition 2. Benefit reward (Br)**. Benefit reward refers to the control efficiency of system network security when the security control strategy is implemented. Benefit reward mainly reflects the control ability and effect of security risk control strategy and is specifically reflected in the changes in network security situation before and after implementing the security control strategy. Before the implementation of security control strategy, the networks security situation value is \( S_{before} \), and after the implementation of security control strategy, the networks security situation value is \( S_{after} \). The benefit reward of the security control strategy \( Br = S_{before} - S_{after} \); the smaller \( S \) value is, the higher network security of the system is.

\( S_{before} \) and \( S_{after} \) can be calculated through the network security situation assessment method described above which is based on the SSUT index system. When \( Br > 0 \), which means \( S_{after} < S_{before} \), it shows that after the implementation of security control strategy, the networks security status and the networks security of system has been improved; when \( Br < 0 \), which means \( S_{after} > S_{before} \), it shows that after the implementation of security control strategy, the networks security status and the networks security status and the networks

### Table 2. Security defense control strategy and description

| Class                  | Strategy subclasses          | The tag | Description                                      |
|------------------------|-----------------------------|---------|--------------------------------------------------|
| Host-based security    | Close the process           | \( D_1 \) | Close suspicious or all processes                 |
| defense control        | Close the service           | \( D_2 \) | Close vulnerable software                        |
| strategy               | Close the host              | \( D_3 \) | Close the attacked host                          |
|                        | Install software patches    | \( D_4 \) | Update flawed software to the lastest version    |
|                        | System virus scan           | \( D_5 \) | Use antivirus software scanning system           |
| Network-based security | Isolate the host            | \( D_6 \) | Close the network adapter to isolate attacked    |
| defense control        | Discard suspicious          | \( D_7 \) | Use IDS or firewall to drop suspicious           |
| strategy               | Disconnect from the         | \( D_8 \) | Disconnect the information system from           |
|                        | Block the port              | \( D_9 \) | Use software to block ports                      |
|                        | Block the IP address        | \( D_{10} \) | Use software to block addresses                  |

### Table 3. Control cost (Cc) and negative effect (Ne) of control strategy

| Control strategy               | The tag | Cc level | Ne level | Ne magnitude |
|--------------------------------|---------|----------|----------|--------------|
| Close the process              | \( D_1 \) | Low      | High     | 20           |
| Close the service              | \( D_2 \) | Medium   | High     | 20           |
| Close the host                 | \( D_3 \) | Medium   | High     | 30           |
| Install software update patches| \( D_4 \) | Medium   | Low      | 10           |
| System virus scan              | \( D_5 \) | High     | Low      | 10           |
| Isolate the host               | \( D_6 \) | Medium   | Medium   | 20           |
| Discard suspicious packets     | \( D_7 \) | Medium   | Medium   | 20           |
| Disconnect from the network    | \( D_8 \) | Medium   | High     | 30           |
| Block the port                 | \( D_9 \) | Medium   | High     | 20           |
| Block the IP address           | \( D_{10} \) | Medium | High     | 20           |
security of system has been reduced; when \( Br = 0 \), which means \( S_{\text{after}} = S_{\text{before}} \), it shows that after the implementation of security control strategy, the networks security status has not changed at all.

**Definition 3. Negative effect (Ne).** Negative effect refers to negative effects such as network system failure or service quality decline caused by the implementation of security control strategy. For example, disconnection of the network may cause the system to fail to provide some services for users. For the convenience of analysis, in this paper, the negative effects of control strategies are divided into three levels: low, medium and high, respectively representing very little, less and more negative effects, and the magnitude of the corresponding negative effects are set to 10, 20 and 30, respectively. The table (Table 3) shows the negative effects of each strategy. Therefore, the total negative effect of the security control strategy is \( Ne = 10 \times (D_1 + D_3) + 20 \times (D_2 + D_3 + D_6 + D_7 + D_8 + D_9) + 30 \times (D_3 + D_6) \).

### 2.4 Performance evaluation and control feedback

The performance feedback module evaluates the implementation effect of the optimal control strategy of security risk. According to the effectiveness evaluation results, the relevant parameters information of the optimal control model are constantly reset or adjusted. The dynamic feedback mechanism makes the optimal security control model continuously self-evolve, which is conducive to optimization of security control strategy and thus makes the network security keep going to the best state. The concept of control parameters is introduced here.

**Definition 4. Control parameters (Cp).** Control parameters are the dynamic feedback parameters of optimal security control model and contain two parameters: \( (Cp^t, Cp^m) \). One parameter which is denoted as \( Cp^t \) is the network security threshold. The other parameter which is denoted as \( Cp^m \) represents the number of selected strategy in optimal safety control strategies. \( Cp^t \) is the critical value which decides whether we need to introduce and implement safety control strategy under current network safety status. When the network security situation value is greater than \( Cp^t \), security control strategy need to be introduced and implemented to improve the network situation. Otherwise, it means that the current network security status is good and the security control strategy doesn’t need to be introduced and implemented. \( Cp^m \) denotes the number of selected strategies in security control strategies, and the optimal security control strategies are selected according to the optimal evaluation criteria mentioned in the section 1.3 from all the security control strategies whose number of substrategies is \( Cp^m \).

### 3. Experiment and Analysis

In this paper, the KSA-DGSO algorithm is used to search for optimal security control strategy solution. Firstly, the algorithm resets the location update mechanism according to the change of object function caused by key strategies. Then, it carries out optimal control to complex network security risks according to the optimal security control strategy. The DSCP model and the KSA-DGSO model will be separately experimented and analyzed for security risk optimal control in four representative complex networks. The Discrete Glowworm Swarm Optimization Algorithm mentioned in the reference [12] will be recorded as DGSO algorithm. In order to verify the superiority of KSA-DGSO algorithm, the KSA-DGSO algorithm and the DGSO algorithm will be compared in the experiment.

#### 3.1 Parameter Setting and Analysis

In the experiment, in order to ensure the effectiveness of experimental comparison results, the basic parameters across KSA-DGSO algorithm and DGSO algorithm should be kept the same. Krishnanand and Ghose have analyzed the relevant parameters of DGSO algorithm and obtained optimal values for reference. Among these values, luciferin volatilization factor \( \rho = 0.4 \), luciferin update rate \( \gamma = 0.6 \), dynamic decision domain update rate \( \beta = 0.08 \), initial luciferin value \( l_0 = 5 \), threshold value of neighborhood set \( n_1 = 5 \), population size \( n = 20 \), numbers of iterations \( t = 100 \) [13]. According to the section 2.3, the smaller control cost of security control strategy is, the higher reward of security control benefit becomes. Moreover, it produces few negative effects and therefore the safety control strategies are more superior. Hence, the objective function of KAS-DGSO algorithm can be expressed
as:

\[ f(x_i(t)) = Cc(x_i(t)) + \frac{1}{Br(x_i(t))} + Ne(x_i(t)) \]  

In this function, glowworm individual \( x_i(t) \) denotes a safety control strategy solution. Furthermore, the execution sequence of selected strategies in safety control strategies may have an impact on safety control efficiency. In order to research the optimal control of security risks accurately and scientifically, the execution sequence of the selected strategies in safety control strategies should be taken into account. In this paper, the execution sequence of the selected strategies is identified by the number subscript. For example, the glowworm individual \( x_i(t) = (13,0,0,11,15,0,12,0,0,14) \) means that the execution sequence of the selected strategies is installing software update patches, abandoning suspicious data packages, closing the process, interrupting the IP address and system virus scanning in sequence. In this paper, only the impact that the execution sequence of selected strategies may affect the benefit return \( Br \) is taken into account, and the impact on the control cost \( Cc \) and the negative effect \( Ne \) are ignored.

The set of control parameters \( (Cps, Cpm) \) has a decisive influence on DSCP model. After the experiment, it can be concluded that the control effect becomes excellent when \( (Cps, Cpm) = (0.85, 5) \).

3.2 The impact of complex network structure on security risk control.

To verify what control effects the DSCP model can produce in different complex network structure, four complex network models are generated to carry out the experiments on optimal control of security risk. The parameters of complex network are set according to the reference [14] and the related parameter settings are kept the same in all experiments. In order to observe the changes of the complex network security risk optimal control performance with the number of iterations, some concepts as follows need to be defined.

**Definition 5.** Fitness-Time curve (F-T curve). F-T curve is a two-dimensional curve which describes the objective function value of security control strategy \( f(x_i(t)) \) varies with the iterations. The ideal curve describes that the value of function \( f(x_i(t)) \) decreases with the number of iteration increasing, and it will drop to a minimum before number of iterations reaches its maximum and the minimum value will be maintained until the number of iterations reaches the maximum \( T \). Moreover, the security risk control strategy corresponding to the minimum value of function \( f(x_i(t)) \) is the optimal security risk control strategy.

After adopting DGSO algorithm and KSA-DGSO algorithm respectively for simulation experiment of complex network security risk optimal control and introducing and implementing a series of security control strategies at a certain time under four complex network structures, four Fitness-Time curves can be obtained. To observe the Fitness-Time curves under different complex network structures and different optimization algorithms better, the initial security control strategies in different simulations are set to be the same, which means that the initial \( f(x_i(t)) \) values are kept the same. The results of experiment are shown as figure 1.

![Fitness-Time curve in different complex network structures](image)

**Fig 1.** The comparison figure of the Fitness-Time curve in different complex network structures.

From figure 1, it can be found that the Fitness-Time curves are different in these four typical complex network structures, but the tendencies that the Fitness-Time curve value decreases with the iteration number increasing is the same on the whole. Also, the KSA-DGSO algorithm is superior to
DGSO algorithm in the aspect of iteration efficiency and the optimal value of $f(x_i(t))$. After 100 iterations, the optimal value of $f(x_i(t))$ (denoted as $F_{-T'}$), optimal iteration number (denoted as $T'$) and the optimal security control strategy solution (denoted as $x(T')$) under four complex network structures and different optimization algorithms are shown in the following table 4.

Table 4. The $F_{-T'}, T', x(T')$ value in different complex networks and optimization algorithms

| Complex network type | Optimization algorithm | $F_{-T'}$ value | $T'$ value | $x(T')$ |
|----------------------|------------------------|----------------|------------|---------|
| NC                   | DGSO                   | 210.3          | 86         | $(0,1,0,1,0,1,0,0,1,0)$ |
|                      | KSA-DGSO               | 205.1          | 75         | $(1,0,0,1,1,0,0,1,0,1,0)$ |
| ER                   | DGSO                   | 207.7          | 88         | $(0,1,0,1,0,1,0,0,1,0)$ |
|                      | KSA-DGSO               | 203.5          | 79         | $(0,0,1,1,1,1,0,0,0,0,0)$ |
| WS                   | DGSO                   | 215.2          | 80         | $(1,0,0,1,1,0,0,1,0,1,0)$ |
|                      | KSA-DGSO               | 210.2          | 73         | $(0,1,0,1,1,0,1,1,0,1,0)$ |
| BA                   | DGSO                   | 206.9          | 79         | $(1,0,1,1,1,1,1,1,0,0,0,0)$ |
|                      | KSA-DGSO               | 199.8          | 71         | $(1,0,1,1,1,1,0,0,0,0,0,1)$ |

For example, the optimal security control strategy solution according to KSA-DGSO algorithm is $x(75)=(1,0,0,0,1,1,0,0,0,1,0,1)$ in NC network, which means that the optimal security control strategy solution is obtained at the 75th iteration and the execution sequence of sub-strategies is installing software update patches, system virus scanning, blocking IP address, disconnecting the network and closing process. The optimal $F_{-T'}$ value is 205.1. From the experiment results above, it can be found that the states of security and stability under different networks have been improved obviously, the $f(x_i(t))$ value decreases continually with the increasing of number of iterations and reach the $F_{-T'}$ value in the end. The optimal security control strategy solution is obtained and the effectiveness of the DSCP model is also verified. Also, the $F_{-T'}$ value of KSA-DGSO algorithm is lower than DFSO algorithm about 2.56% and the $T'$ value reduces by 10.51% averagely, which confirm the superiority of the KSA-DGSO algorithm.

According to the optimal security control strategy solution, the selection of sub-strategies is counted and analyzed, which can further optimize the allocation of network security resources. The number of all the selected sub-strategies in $x(T')$ in Table 4 are counted and the result is shown in figure 2, in which $N$ is the time of times the kth sub-policy has been selected. From figure 2, it can be seen that there are more times to install software update patches and do the system virus scanning. Therefore, both security measures in the process of network system security building and designing should be reinforced stressfully, and the security work of complex network security protection basic facilities can also be further reinforced.

Figure 2. The time of selected control sub-policy

3.3 The impact of attack strategy on security risk optimal control
There are two types of attack strategy: random attack and intended attack. The random attack means attacking one random node in network and the intended attack means attacking key nodes in network.
The calculated attack mainly includes three types of attack: node-degree priority attack, node interval priority attack and edge interval priority attack. The node priority attack means attacking the node of biggest value priority. The node interval priority attack means attacking the node which passes the most shortest paths. The edge interval priority attack means attacking the both end nodes of the edge which passes the most shortest path [15]. In this section, in order to confirm the impact of attack strategy on security risk optimal control, DOS denial service attack or Root getting administrator privilege attack on complex network under four attack strategies including random attack, node priority attack, node interval-priority attack and edge interval priority attack are performed. Performing attack may do damage to the complex network, so some definitions need to be defined as follows.

**Definition 6 Attack damage degree (Add)** Attack damage degree means the degree of caused damage after performing DOS attack or Root attack under different attack strategies, which is relevant to the sum of all the attacked nodes’ degrees. Attack damage can be calculated as \( Add = \phi \sum_{i=1}^{L} \text{degree}_i \).

In the formula, \( \phi \) is the coefficient of attack damage. When the DOS attack is performed, \( \phi = 2 \); when the Root attack is performed, \( \phi = 10 \) [10]. \( L \) denotes the number of attacked nodes and \( \text{degree}_i \) denotes the degree of the \( i \)th attacked node. Therefore, the security control strategy optimizing control objective function is adjusted as follows:

\[
f(x(t)) = Cc(x(t)) + \frac{1}{Br(x(t))} + Ne(x(t)) + \phi \sum_{i=1}^{L} \text{degree}_i
\]

In addition, the topological structure of complex network contains uniform network and non-uniform network. In uniform network, the degree of nodes is almost the same, such as ER network, WS network, whose degree distribution obeys exponential distribution. In non-uniform network, the degree of nodes distributes non-uniformly, only the degrees of few nodes are large while the degrees of other nodes are small. For example, the degree distribution of BA network obeys power-law distribution. The internet is the typical BA network with power exponent \( r = 2.5 \). Therefore, in this section, the optimal control test is only carried out under BA network with control parameters \((Cp^r, Cp^m) = (0.85, 5)\), and the optimization algorithm is also the comparison of DGSO algorithm and KSA-DGSO algorithm. Table 5 shows the \( F-T' \) value and the \( T' \) value in each experiment.

| Attack Strategy          | Optimization Algorithm | Dos attack   | Root attack   |
|-------------------------|------------------------|--------------|--------------|
|                         |                        | \( F-T' \) value | \( T' \) value | \( F-T' \) value | \( T' \) value |
| Random attack           | DGSO                   | 219.4        | 83           | 270.3        | 88           |
|                         | KSA-DGSO               | 210.9        | 74           | 258.7        | 76           |
| Node priority attack    | DGSO                   | 241.7        | 85           | 359.6        | 90           |
|                         | KSA-DGSO               | 228.5        | 75           | 337.9        | 78           |
| Node interval-priority  | DGSO                   | 261.4        | 89           | 427.3        | 94           |
| attack                  | KSA-DGSO               | 238.5        | 80           | 398.2        | 85           |
| Edge-betweenness        | DGSO                   | 225.4        | 86           | 317.6        | 89           |
| priority attack         | KSA-DGSO               | 219.7        | 79           | 304.4        | 81           |

From the information in Table 5, it can be found that the \( F-T' \) value of KSA-DGSO algorithm is lower about 4.97% than it of DGSO algorithm and the \( T' \) value reduces about 10.19% averagely when implementing DOS attack. On the contrary, the \( F-T' \) value of KSA-DGSO algorithm is lower about 5.23% than it of DGSO algorithm and the \( T' \) value reduces about 11.14% averagely when implementing Root attack. Therefore, it is confirmed that KAS-DGSO algorithm is superior to DGSO algorithm. In order to observe the influence of DOS and Root attacks on the optimal security control under each attack strategy more intuitively, the comparison results of experimental data in Table 5.
(Table 5) are transformed into figure 3, where Attack0, Attack1, Attack2, Attack3, Attack4 respectively represent no attack, random attack, node-degree priority attack, node interval priority attack, and edge interval priority attack.

![Figure 3](image_url)

Fig 3. The comparison figure of the $F-T'$ value and the $T'$ value in different attack strategies.

It can be seen from figure 3 that no matter using KSA-DGSO algorithm or DGSO algorithm, both $F-T'$ value and $T'$ value of Root attack are higher than those of DOS attack under the same attack strategy, indicating that Root attack has a great impact on the optimal control of BA network security risk than DOS attack. The main reason is that Root attack has a larger damage degree coefficient, resulting in a larger damage to BA network. In the case of Attack1, Attack2, Attack3, Attack4, both $F-T'$ value and $T'$ value are higher than those of Attack0, indicating that random attack, node degree, priority attack, node intermediate priority attack have greater influence on the optimal control of BA network security risk than no Attack. Specifically, it can be seen from figure 3(a) and table 5 that, under the DOS attack and KSA-DGSO algorithm, the $F-T'$ value of Attack1, Attack2, Attack3 and Attack4 is 5.56%, 14.36%, 19.37% and 9.96% higher than Attack0 respectively. The $T'$ values is 4.23%, 5.63%, 12.68%, 11.27% higher respectively.

It can also be seen from figure 3(b) and table 5 that, under the Root attack and KSA-DGSO algorithm, the $F-T'$ value of Attack1, Attack2, Attack3, Attack4 is 29.48%, 69.12%, 99.30% and 52.35% higher than Attack0, and the $T'$ values is 7.04%, 9.86%, 19.72%, 14.08% higher than Attack0.

Therefore, the $F-T'$ value comparison results lead to the conclusion that the ranking of impact degree of attack strategy on the optimal control effect of BA network security is Attack3 > Attack2 > Attack4 > Attack1 > Attack0. According to the $T'$ value comparison results, it can be concluded that the impact of Attack strategy on iteration convergence is Attack3 > Attack4 > Attack2 > Attack1 > Attack0.

4. Conclusions

Aimed at the problem of risk control and optimization of complex networks security, an optimal control model of complex network security risk based on detection evaluation, strategy selection, optimal control and effectiveness feedback is established. A discrete firefly swarm optimization algorithm with key strategy modification is proposed to find the optimal security control strategy solution. The DSCP model and KSA-DGSO algorithm are tested for optimal security control under four typical complex network structures to verify the effectiveness of DSCP model and the superiority of KSA-DGSO algorithm. In addition, the impact of attack strategy on DSCP model is also studied deeply. The experimental results show that: the ranking of the impact of an attack strategy on the optimal control effect of BA network security is node preemptive attack, node degree preemptive attack, edge preemptive attack and random attack from higher to lower. The order of the influence on iterative convergence from higher to lower is node intermediate priority attack, edge intermediate priority attack, node degree priority attack, random attack. KSA-DGSO algorithm is superior to DGSO algorithm under each attack strategy. To sum up, the work of this paper plays a guiding role in
promoting the study of risk control and optimization of complex network security.

References

[1] Justin Ruths, Derek Ruths. (2014) Control Profiles of Complex Networks [J]. *Science*, 343, 1373-1376.

[2] Baosen Zhang, Ram Rajagopal, David Tse. (2014) Network Risk Limiting Dispatch: Optimal Control and Price of Uncertainty [J]. *IEEE Transactions on Automatic Control*, 59(5): 2442-2456.

[3] Zhou Tao, Zhang Zike, Chen Guanrong. (2014) The Opportunities and Challenges of Complex Networks Research [J]. *Journal of University of Electronic Science and Technology of China*, 43(1): 1-5.

[4] Jun Yan, Haibo He, Yan Sun. (2014) Integrated Security Analysis on Cascading Failure in Complex Networks [J]. *IEEE Transactions on Information Forensics and Security*, 9(3): 451-462.

[5] Lee Phillip, Clark Andrew, Bushnell Linda, Poovendran Radha. (2014) A Passivity Framework for Modeling and Mitigating Wormhole Attacks on Networked Control Systems [J]. *IEEE Transactions on Automatic Control*, 59(12): 3224-3237.

[6] Li Li, Huixia Zhang, Yuanqing Xia, Hongjiu Yang. (2018) Security estimation under Denial-of-Service attack with energy constraint [J]. *Neurocomputing*, 292(31): 111-120.

[7] Guang hui, Wen wu, Xing huo, Jin hu. (2017) Complex Cyber-Physical Networks: From Cybersecurity to Security Control [J]. *Journal of Systems Science and Complexity*, 30(1): 46-47.

[8] Saurabh Amin, Galina A. Schwartz, S. Shankar Sastry. (2013) Security of interdependent and identical networked control systems [J]. *Automatica*, 49: 186-192.

[9] Li Jizhen, Meng Xiangru, Wen Xiangxi, Kang Qiaoyan. (2015) Network security situation prediction based on Gaussian Process optimized by Glowworm Swarm Optimization [J]. *Systems Engineering and Electronics*, 37(8): 1887-1893.

[10] Wen-Hsien, Chou, Yu-Wei, Lee, Kuen-Chang, Lin, Wan-Rung, Hwang, Elliott T. Y. (2013) Combining Decision Making Trial and Evaluation Laboratory with Analytic Network Process to Perform an Investigation of Information Technology Auditing and Risk Control in an Enterprise Resource Planning Environment [J]. *Systems Research and Behavioral Science*, 30(2): 176-193.

[11] Jiang Wei, Fang Binxing, Tian Zhihong, Zhang Hongli. (2009) Evaluating Network Security and Optimal Active Defense Based on Attack-Defense Game Model [J]. *Chinese Journal of Computers*, 32(4):817-827.

[12] Zhou Yongquan, Huang Zhengxin, Liu Hongxia. (2012) Discrete Glowworm Swarm Optimization Algorithm for TSP Problem [J]. *Acta Electronica Sinica*, 40(6): 1164-1170.

[13] Li Zhao, Xu Aiguo, Ban Xiaofang. (2013) Complex information system security risk propagation research based on cellular automata [J]. *Acta Physica Sinica*, 62(20): 200-203.

[14] Chen Pin-Yu, Cheng Shin-Ming. (2015) Sequential defense against random and intentional attacks in complex networks [J]. *Physical Review E-Statistical, Nonlinear, and Soft Matter Physics*, 91(2), 022805.

[15] Y Li, S Liu, Y Yu, T Cao. (2018) Analysis of network vulnerability under joint node and link attacks [C]. *Materials Science and Engineering Conference Series*, 322.