Research on Robustness of Critical information infrastructure Based on Attack-Defensive Game Model

Diyang Liu¹*, Zhen Zhang²

¹Information Technology Institute, Information Engineering University, Zhengzhou, Henan, 450000, China
²Information Technology Institute, Information Engineering University, Zhengzhou, Henan, 450000, China

*Corresponding author’s e-mail: 337935591@qq.com

Abstract. Because the traditional network robustness research ignores the confrontation process and information asymmetry conditions, this paper analyzes the impact of information asymmetry conditions on the robustness and simulates the information asymmetry conditions through a perturbation model. Based on the stackelberg game, an attack-defensive game model under asymmetric information is established, by solving the game equilibrium solution, the defensive resource allocation strategy that optimizes the network robustness is obtained. The simulation results show that when attack resources are scarce, the attacker tends to respond with a low priority attack; when the attack resources are abundant, the attacker tends to have a high priority attack response. Under the mixed defensive strategy corresponding to the equilibrium solution of the game, the optimization rate of the defender's robustness payoff compared with the expected return under the pure strategy reached 4% to 12%.

1. Introduction

Critical Information Infrastructure (CIS) refers to the information network or industrial control network that provides basic services such as networks and communications to the society or supports the normal operation of important industries such as energy and transportation. Once the CIS network is under attack and loses its ability to provide services normally, it will cause huge losses to the country [1]. The robustness of the CIS network refers to the ability of the CIS network to maintain its original topology and service functions in the event of a virus attack and other network security incidents.

The CIS network is huge and complex, so the current research on the robustness of CIS network is mainly based on complex network theory. However, the traditional network robustness optimization strategy research is still different from the attack process in the real information networks such as the Internet. First of all, the abstraction of malicious attacks is described as deleting nodes and edges, ignoring the process of attack and defensive confrontation between attacker and defender on a node. In this regard, the rigorous mathematical foundation of game theory provides a suitable framework for network dynamic attack and defensive confrontation. Ref. [2] conducts a comprehensive analysis of cost constraints, target valuation, cost-effectiveness, and defensive level in the critical infrastructure network attack-defensive game. Ref. [3] transforms the game problem into a multi-objective optimization model and uses evolutionary algorithm to solve it. Secondly, in the real network offense and defensive, the information on both sides is asymmetrical. For example, with the development of
network defensive technologies such as active defensive, deception-based defensive technologies enable the defender to break the determinism and static nature of the network system, and attackers cannot always obtain complete information about the target network through scanning and detection [4].

Based on the above analysis, under the condition of information asymmetry, this paper studies the network robustness in the Attack-defensive game from the perspective of defensive resource allocation.

2. Information perturbation model

2.1. Impact of attack information on robustness
The size of its largest connected subgraph is the number of nodes $N$ of the network. When a node suffers a malicious attack, some nodes in the network are removed from the network, the network is split into multiple connected subgraphs, and the maximum connected subgraph size of the network becomes smaller. Therefore, this paper adopts the robustness evaluation standard $R$ to measure the network robustness, which is defined as

$$R = \frac{N'}{N} \quad (1)$$

In eq.1, $N$ is the number of nodes included in the initial network, and $N'$ is the number of nodes included in the largest connected subgraph of the remaining network. Attack information refers to the network structure information used by the attacker to formulate attack strategies. Since the robustness of complex networks differs significantly under different attack strategies, attack information is very important in the process of formulating attack strategies. From the perspective of attack information, an attacker has the following three situations when formulating an attack strategy:

- When the attacker has complete and accurate network information, he can delete the most important nodes first according to some network topology characteristics. This situation corresponds to a malicious attack strategy.
- When the attacker has not obtained any network information, he can only delete nodes randomly. This situation corresponds to a random attack strategy (Random Attack, RA).
- When the defender disturbs the attack information, in this case the attacker can still formulate a malicious attack strategy based on the existing attack information, and the attack effect is between random attack and malicious attack.

2.2. Information perturbation model
This paper uses a deception network to build a model to simulate the information asymmetry conditions and generates a deception network for the attacker based on the initial network [5]. The real network owned by the defender is $G_{true} = G$ and the deception network $G_{false}$ owned by the attacker. The perturbation parameter $\alpha$ is used to measure the perturbation intensity of the attack information by the defender. $k_i^{true}$ is the degree of node $i$ in the initial network, $k_{max}$ is the upper limit of the degree of node $i$ that can be changed randomly and $k_{min}$ is the lower limit of the degree of node $i$ that can be changed randomly, $M$ is the maximum node degree in the network and $m$ is the minimum node degree in the network. Because too much deviation from the true node degree will reduce the probability of attackers using perturbed topology, this paper sets $0 \leq \alpha \leq 0.5$. $\Delta k$ is the variable range of the node degree, then there is:

$$k_{max} = k_i^{true} + (M - k_i^{true}) \times \alpha \quad (2)$$
$$k_{min} = k_i^{true} - (k_i^{true} - m) \times \alpha \quad (3)$$
$$\Delta k = (M - m) \times \alpha \quad (4)$$

The expected value of the degree of node $i$ in the network $G_{false}$ can be expressed as:
$k_i^{\text{False}} = (1-\alpha) \cdot k_i^{\text{True}} + \frac{(M+m) \cdot \alpha}{2}$ (5)

Since the target network is controlled by the defender, the defender has the initial network structure information and the deception network structure information, the attacker only has the deception network structure information. At this time, the information of the attacker and the defender is asymmetric.

3. Attack-defensive game model

3.1. The set of game strategies

The strategy and cost quantification of attackers and defenders are the basis for establishing attack and defensive game models and finding the optimal defensive strategy. We first give a pure strategy definition:

**Definition 1:** Pure strategy[6]: Given a vector $P = (p_H, p_L)^T$, $p_H \in (0,1)$, $p_L \in (0,1)$, $p_H + p_L = 1$, $p_H, p_L$ respectively indicate that the attacker or the defender chooses one of the high degree strategy or the low degree strategy.

The pure strategy sets of the attacker and the defender are $S_A = \{\text{HDA}, \text{LDA}\}$, $S_D = \{\text{HDD}, \text{LDD}\}$, indicates high degree attack strategy (HDA), low degree attack strategy (LDA), high degree defensive strategy (High Degree Node Attack) and low degree defensive (HDD) and low degree defensive strategy (LDD). Taking into account the uncertainty of the behavior of both sides in the attack and defensive process, the mixed strategy of both sides must be considered. Give the mixed strategy definition:

**Definition 2:** Mixed strategy[6]: Given a vector $Q = (q_H, q_L)^T$, $0 < q_H < 1$, $0 < q_L < 1$, $q_H + q_L = 1$, $q_H, q_L$ respectively indicate that the attacker or the defender chooses one of the high degree strategy or the low degree strategy.

3.2. Cost quantification

Below we will analyze the attack and defensive costs of attackers and defenders in the game and quantify them. Given the following definitions:

**Definition 3:** Node Defensive Resource, represents the defensive resource allocated by the defender to a node, expressed as $r_i^D = r_i^D k_i^F$, $r_i^D$ is the defensive resource parameter.

**Definition 4:** Total Defensive Resource, represents all defensive resources in the target network, expressed as $T^D = \sum_{i=1}^{N} r_i^D$.

**Definition 5:** Available Defensive Resource, represents the defensive resources that the defender can allocate, expressed as $R^D = \theta^D T^D$.

**Definition 6:** Node Attack Resource, represents the attack resource allocated by the attacker to a node, expressed as $r_i^A = r_i^A k_i^F$, $r_i^A$ is the attack resource parameter.

**Definition 7:** Total Attack Resource, represents all attack resource in the target network, expressed as $T^A = \sum_{i=1}^{N} r_i^A$.

**Definition 8:** Available Attack Resource, represents the attack resource that the attacker can allocate, expressed as $R^A = \theta^A T^A$.

**Definition 9:** Attack success rate, based on the node's defensive resource and attack resource settings, the attack success rate is quantitatively expressed as:
3.3. Cost quantification

In this paper, the payoff function is defined by the network robustness evaluation index. When the defensive strategy is \( s_d \) and the attack strategy is \( s_a \), the defender’s payoff function is:

\[
f_d(s_d, s_a) = \frac{N'(G_{true})}{N}
\]  

\( N'(G_{true}) \) represents the scale of the largest connected component of the real network at the end of the attack, \( 0 < f_d < 1 \). the attacker’s payoff function is:

\[
f_a(s_d, s_a) = \frac{N'(G_{false})}{N}
\]  

\( N'(G_{false}) \) represents the scale of the largest connected component of the real network at the end of the attack, \( 0 < f_a < 1 \).

In order to prevent attackers from mastering the defensive strategy, the defensive strategy is usually a mixed strategy. This article considers a hybrid defensive strategy composed of two pure strategies, HDD and LDD. In the game model, the attacker, as a follower, chooses the attack strategy that maximizes the benefits based on the strategy of the defender. This specific attack decision is also called the best pure strategy response in game theory terms[7]. Therefore, when the defender is a mixed strategy and the attacker is a pure strategy, the payoff matrix is shown in Table 1.

Table 1. Mixed strategy payoff matrix

| Defender | HDA | LDA |
|----------|-----|-----|
| HDD      | \( q_H f_{H,H}^d P_H^T, q_H f_{H,H}^a P_H^T \) | \( q_H f_{H,L}^d P_L^T, q_H f_{H,L}^a P_L^T \) |
| LDD      | \( q_L f_{L,H}^d P_H^T, q_L f_{L,H}^a P_H^T \) | \( q_L f_{L,L}^d P_L^T, q_L f_{L,L}^a P_L^T \) |

3.4. Attack-defensive game model

The essence of cyberspace security is attack and defensive. In the process of defensive, CIS defenders first need to decide how to allocate defensive resources to many different information resource nodes to achieve the best defensive effect, that is, the most robust network excellent. Therefore, this article describes the network attack and defensive process under asymmetric information through a game model, analyzes the robustness payoff of defenders under different attack and defensive strategies through the game model, by obtaining the equilibrium solution of the game model, the defensive resource allocation strategy that optimizes the network robustness is determined. For the above problem, we use the stackelberg game model to describe, as shown in Figure 1.

The classic stackelberg game is a two-person non-cooperative game consisting of a leader and a follower. We regard the defender as the leader and the attacker as the follower. The defender first determines his own defensive strategy, and the attack strategy is determined by the attacker based on the defensive strategy he understands. First, we make the following assumptions:

1. Both the attacker and the defender are intelligent decision makers, and the formulation of attack and defensive strategies is not random.

2. The goal of both the attacker and the defender is to maximize their own benefits. For example, the
attacker will choose the attack strategy that most damages the target network, and the defender will choose the defensive strategy that best protects the target network topology.

On the basis of the above two assumptions, we can describe the conflicting relationship between the attacker and the defender as a strategic attack and defensive game model. We define the attack and defensive game model as follows:

**Definition 11**: Attack-defensive game model is a triple \( ADG = (N, S, U) \)

1. \( N = (p_1, p_2, p_3, \ldots, p_n) \) is the participant of the game. The participants of the game in this model are the attacker and defender.

2. \( S = (s_1, s_2, s_3, \ldots, s_n) \) is the set of game strategies. The game strategy of the attacker and the defender in this model mainly refers to the allocation strategy of attack resources and defensive resources.

3. \( U = (f_1, f_2, f_3, \ldots, f_n) \) is the player’s payoff function.

### 3.5. Cost quantification

The goal of Stackelberg game optimization is to obtain strong Stackelberg Equilibrium (SSE), so that attackers cannot cause more damage to the network structure by optimizing attack strategies. SSE forces followers to always choose the strategy that is most beneficial to the leader when the benefits of multiple strategies are the same, so it can ensure the existence of equilibrium; on the other hand, the defender can calculate the attacker’s preferred strategy before implementing the mixed strategy. In this way, the defender maximizes its own robustness gains. This is the so-called first-hand advantage. Because of the first-hand advantage, the leader can choose a strategy that is infinitely close to the equilibrium solution to make followers tend to choose a strategy that is favorable to it. So as to achieve a more desired strong equilibrium, which also ensures the existence of equilibrium. In this paper, the linear programming method is used to calculate the SSE [8].

Assuming that the defender’s optimal mixed defensive strategy is \( Q^* \), and the corresponding attacker’s optimal attack strategy is \( P^* \), When the attacker’s response strategy is HDA, the equilibrium solution problem can be described as

\[
\begin{align*}
\text{max } & q_H f_{h, h}^d + q_L f_{l, h}^d \\
\text{s.t.} & (f_H^a - f_{h, h}) q_H + (f_L^a - f_{l, h}) q_L \geq 0
\end{align*}
\]

(9)

In this condition, the optimal benefit of the defender is \( f_H^a \). When the attacker’s response strategy is LDA, The equilibrium solution problem can be described as

\[
\begin{align*}
\text{max } & q_H f_{h, l}^d + q_L f_{l, l}^d \\
\text{s.t.} & (f_H^a - f_{h, l}) q_H + (f_L^a - f_{l, l}) q_L \geq 0
\end{align*}
\]

(10)
In this condition, the optimal benefit of the defender is \( L_f \). If \( f_L^* > f_H^* \), the equilibrium solution is \( P^* = P_L^*, Q^* = Q_L^* \), else the equilibrium solution is \( P^* = P_H^*, Q^* = Q_H^* \).

4. Experiment and Analysis

4.1. Network topology

In order to verify the effectiveness of the optimal defensive strategy selection algorithm proposed in this paper for network robustness optimization, perform simulation experiments on CERNET. The simulation experiment was completed on the pycharm community edition 2019.3 platform.

CERNET is a national academic computer internet network invested and constructed by the state, managed by the ministry of education, and constructed and operated by universities such as Tsinghua University. CERNET is divided into four levels of management, namely the national network center, the regional network center and the regional main node, the provincial education and research network, and the campus network.

4.2. Effectiveness verification of robustness optimization

Under the condition that the perturbation parameter \( \alpha = 0.3 \) and the defender can call the resource parameter \( \theta_D = 0.2 \), as the attacker can call the attack resources increase, the equilibrium solution of the game model and the optimization results of the defensive benefit under the corresponding strategy are shown in Table 2.

| \( \theta_A \) | Equilibrium solution | Defender Payoff | Pure strategy Payoff | Optimization rate |
|-------------|----------------------|-----------------|---------------------|------------------|
| 0.1         | \( Q_L = [0.119, 0.801] \) | 0.941           | 0.902               | 4.14%            |
| 0.2         | \( Q_L = [0.118, 0.802] \) | 0.820           | 0.799               | 2.56%            |
| 0.3         | \( Q_L = [0.233, 0.763] \) | 0.700           | 0.675               | 3.57%            |
| 0.4         | \( Q_L = [0.246, 0.754] \) | 0.633           | 0.550               | 8.30%            |
| 0.5         | \( Q_L = [0.309, 0.691] \) | 0.449           | 0.411               | 8.46%            |
| 0.6         | \( Q_L = [0.495, 0.505] \) | 0.333           | 0.313               | 6.01%            |
| 0.7         | \( Q_L = Q_H = [0.553, 0.447] \) | 0.200           | 0.195               | 2.50%            |
| 0.8         | \( Q_L = Q_H = [0.575, 0.425] \) | 0.155           | 0.135               | 12.90%           |
| 0.9         | \( Q_L = [0.948, 0.052] \) | 0.125           | 0.105               | 12.00%           |

5. Conclusion

It can be seen from Table 1 that when the \( \theta_A < 0.7 \), the attacker tends to respond to the LDA attack. In the corresponding equilibrium solution, the defender has a great probability of choosing LDD; When \( \theta_A = 0.7 \) or \( \theta_A = 0.8 \), the attacker chooses the LDA attack to respond to the HAD attack with the same response, and in the corresponding equilibrium solution, the probability of the defender choosing HDD and LDD is also relatively close; When \( \theta_A = 0.9 \), the attacker tends to respond to HDA attacks. In the corresponding equilibrium solution, the probability of the defender choosing HDA is extremely high. Under the mixed defensive strategy corresponding to the equilibrium solution of the game, the defensive benefit of the defender is compared with the expected benefit under the pure strategy, and the optimization rate of the defensive benefit reaches 4%-12%.
Acknowledgments
This paper was supported by the National Natural Science Foundation of China (NNSF) under Grant Nos. 61802429, 61872382 and 61521003.

References
[1] Ren W, Yuan J, Jiang L, Zhao T. (2016) Technical Framework Research on Critical Information Infrastructure Cybersecurity Classified Protection. In: Proceedings of 2016 4th International Conference on Machinery, Materials and Information Technology Applications (ICMMITA 2016). 2016:1167-1171.
[2] Guan P, He M, Zhuang J, et al. (2017) Modeling a Multitarget Attacker–Defender Game with Budget Constraints. Decision Analysis, 14(2): 87-107.
[3] Zhang C, J E. (2013) Protecting critical infrastructures against intentional attacks: a two-stage game with incomplete information. Iie Transactions, 45(3): 244-258.
[4] Zhao P, Jia B Fang C, Liu Q, et al. (2017). Survey on cyber deception. Journal on Communications, 38(12): 128-143.
[5] Wu J, Tan S Y, Liu Z, et al. (2017) Enhancing structural robustness of scale-free networks by information disturbance. Entific Reports, 7(1):7559.
[6] Jiang W, Fang B X, Tian Z H, et al. (2009) Network security evaluation and optimal active defensive based on offensive and defensive game model. Chinses Journal of Computers,32(04):817-827.
[7] G. Brown, M. Carlyle, J. Salmerón, and K. Wood, (2006) Defending critical infrastructure. Interfaces 36, 530–544.
[8] V Conitzer and T Sandholm, (2006) Computing the optimal strategy to commit to. In: Proceedings of the 7th ACM Conference on Electronic Commerce (ACM, 2006), pp. 82–90.